Available online at www.sciencedirect.com
ScienceDirect
www.compseconline.com/publications/prodclaw.htm
Computer Law & Security Review

The regulation of civilian drones' impacts on behavioural privacy

Roger Clarke[a,b,c,*]

[a] Xamax Consultancy Pty Ltd, Canberra, Australia
[b] Australian National University, Canberra, Australia
[c] University of N.S.W., Sydney, Australia

Keywords:
RPA
RPAS
UAV
UAVS
Visual surveillance
Behavioural privacy
Experiential privacy

ABSTRACT

Surveillance technologies have burgeoned during the last several decades. To surveillance's promises and threats, drones add a new dimension, both figuratively and literally. An assessment of the impacts of drones on behavioural privacy identifies a set of specific threats that are created or exacerbated. Natural controls, organisational and industry self-regulation, co-regulation and formal laws are reviewed, both general and specific to various forms of surveillance. Serious shortfalls in the regulatory framework are identified. Remedies are suggested, together with means whereby they may come into being.

1. Introduction

This is the last in a series of four papers that together identify the disbenefits and risks arising from the use of drones, and consider the extent to which they are subject to suitable controls. The first paper provided background on the nature of drones. The second reviewed existing, critical literatures, in order to ensure that the accumulated understanding of relevant technologies is brought to bear on the assessment of drone technologies as well. The third examined regulatory frameworks relating to public safety, and showed them to be far from satisfactory, particularly in regard to the smaller categories of drones.

Surveillance applications of drones include environmental monitoring, tracking of livestock and wildlife, measurement of meteorological and geophysical phenomena, and observation of large-scale human constructions such as buildings, energy infrastructure such as electricity networks and gas and water pipelines, and road-, air- and sea-traffic. This paper, however, is concerned solely with the surveillance of people, and spaces through which people pass. It excludes consideration of the use of drones in war-zones – a topic that is already copiously addressed in the literature. Its scope is limited to civilian contexts, but up to and including para-military uses by law enforcement and national security agencies, such as border protection, observation and pursuit of criminal suspects, and the observation of civil unrest. The paper's purpose is to examine the extent to which current regulatory regimes appear to exercise controls over the use of drones to conduct such surveillance.

Most privacy discussions focus on data privacy and data protection, to the virtual exclusion of other aspects of privacy. This paper, on the other hand, has as its focus not data privacy, but behavioural privacy. It commences by considering the various dimensions of privacy, with particular emphasis on the dimension that is most directly harmed by surveillance – the privacy of personal behaviour. It then reviews the current state of play in relation to the monitoring of individuals, and identifies the ways in which drones add to the already-

[*] Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman, ACT 2611, Australia.
E-mail address: Roger.Clarke@xamax.com.au.

http://dx.doi.org/10.1016/j.clsr.2014.03.005
0267-3649/

intense intrusiveness of contemporary surveillance technologies. The current regulatory arrangements are then considered. The relatively 'soft' regulatory forms are shown to have little impact. Formal laws are then reviewed, commencing with potentially relevant causes of action of longstanding, and then human rights laws, aviation laws and privacy laws, culminating in laws relating to surveillance *per se*.

2. Privacy

The term 'privacy' is applied to a range of human interests in having private space (Warren and Brandeis, 1890; Morison, 1973; Solove, 2006). The following sections distinguish five dimensions of privacy (Clarke, 1997, 2006), narrowing the focus down to the two most directly impacted by surveillance.

2.1. Dimensions of privacy

The dimension that is most widely discussed is privacy of personal data. As data storage has become cheaper, it has become increasingly common for data-streams to be captured, and retained, and even retained indefinitely. Drones are capable of being used to capture large volumes of data. Where that data does, or may, record actions of, or involving, identifiable individuals, personal data result. Examples include drones that monitor Wifi emanations, that carry automated number-plate recognition (ANPR) capability, and that transmit real-time video of sufficient quality to enable a human operator to visually recognise an individual and associate the recording with that person. Near-future prospects include the emergence of less error-prone 'facial recognition' technologies, tracking of devices carrying RFID-chips, including motor vehicles and anklets imposed on 'open prisoners', and tracking of chips implanted in animals, including humans.

Drone activities accordingly give rise to threats to data privacy. Issues include:

- additional collection of personal data, perhaps in very large volumes
- additional storage, retention, use and disclosure of data about individuals
- use and disclosure in contexts, and for purposes, that have little or nothing to do with the original context and purpose of collection, and which accordingly invite misinterpretations
- interception of data-flows, e.g. of surveillance video transmissions (Gorman et al., 2009)
- unauthorised access to stored data
- exploitation of the data in conjunction with other data

An area of particular public concern is the generally inadequate controls over access by law enforcement agencies to increasing volumes of data. This has been accompanied by increasing attempts to collect large volumes of data, not only for retrospective investigation, and not only once the fact of a criminal act is known or reasonable grounds for suspicion exist, but also prospectively, 'just-in-case'. An example is the abuse of ANPR by various governments, to date at its most extreme in the UK, as a means of mass surveillance of road traffic (Clarke, 2009a). Another example is Internet traffic 'data retention' regimes.

Since the 1970s, data protection laws (sometimes misleadingly referred to as though they were comprehensive privacy laws) have been enacted in most countries (EPIC, 2006; Greenleaf, 2013, 2014). Moderate protections exist in Europe, and various, generally weak protections exist in other countries. The inadequacies of data protection laws have been highlighted by the exploitation of personal data by social media service-providers, and by spy agencies. The emergence of drone-based surveillance adds to an already-burning fire. The impact of drones on data privacy was the focus of a previous article in Computer Law & Security Review (Finn and Wright, 2012).

A close cousin to data privacy is privacy of personal communications, which relates to ephemeral transmissions rather than data that is of necessity stored. In most countries, this is also subject to at least some degree of legal protection.

A third dimension, privacy of the physical person, is concerned with the integrity of the individual's body. Drones may impinge on this interest to the extent that they are used to collect data such as facial images, other physical measures of the individual – commonly referred to as biometrics – and emanations from implants. Where such data is adequate to distinguish the particular physical person from all other human beings, the term 'entifier' is usefully applied to it (Clarke, 2009b). However, it is two further dimensions of privacy that are the primary concerns in this paper, because they encompass the interests that are most directly impinged upon by drone-based surveillance.

2.2. Behavioural privacy

The privacy of personal behaviour is concerned with freedom of the individual to behave as they wish, without undue observation and interference from others. The term 'behaviour' in this context encompasses the individual's activities, movements, associations and preferences. Like any other privacy interest, this is subject to a wide range of conflicts with other interests of the individual, and with interests of other individuals, groups, and society as a whole. Privacy protection is always an exercise in balance.

Overt surveillance stifles behaviours, including (and desirably) illegal behaviours, but also behaviours that are discouraged by organisations with institutional or market power. Covert surveillance, on the other hand, gives rise to the 'panoptic' effect: individuals fear that they may be subject to observation at any time, and that many behaviours might be construed by the powerful to be undesirable. This results in a form of 'self-discipline' – a 'chilling effect' on a wide range of behaviours, and the stultification of freedoms of expression and of innovation (Gandy, 1993, but the literature on 'the panoptic effect' goes back to Bentham, 1791, and has multiplied since Foucault, 1975).

The interest in behavioural privacy encompasses all aspects of human behaviour, but some aspects are particularly sensitive, such as sexual activities, religious practices and political activities. The focus is commonly on psychological needs for 'seclusion' (Warren and Brandeis, 1890; Solove, 2006). However, societies and economies depend on innovative behaviour, which tends to be stifled by observation. Similarly, a healthy