Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Guest Editorial

Drones: Regulatory challenges to an incipient industry

David Wright[*]

Trilateral Research & Consulting LLP, London, UK

Drones are an interesting, emerging technology. The prospect of "dragonfly drones", foreseen by *The Economist* seven years ago,[1] is not at all far-fetched. The size and cost of drones are dropping inexorably. One can imagine, if not foresee, that such drones will become an accoutrement of young people today, much like an obligatory smart phone. Philip Pullman, in the *His Dark Materials* trilogy, described a world where everyone was accompanied by a daemon, a semi-magical spirit animal, a projection of the individual's animus. Drones may be the daemons (in more ways than one) of the 21st century. While one can foresee a range of practical applications for drones of varying sizes and capabilities and with varying payloads – such as monitoring pipelines or finding lost livestock or responding to the pleas for help from a hiker on a remote mountain or monitoring flooding – there is little doubt than drones will be a new source of intrusiveness of our privacy. Is it so hard to imagine a testosterone-packed teenager directing his drone to watch the object of his affection (or lust) sunbathing in the supposed privacy of her back yard?

Already the principal payload of most drones is visual surveillance. We can see potentially massive violation of privacy looming on the horizon. If such is the case, should the technology be permitted at all? Should "we" (society, our elected officials) permit the development of a technology likely to so threaten our privacy? Or, if it's impossible to stop development of the technology, is it possible to control it, to introduce a very tight regulatory regime where drones can be authorised to specific individuals or officials for authorised, socially acceptable applications?

Countervailing forces are at work. The drones industry is revving up. The industry can see the prospect of a large market. In a sluggish economy, policy-makers are not likely to curtail the development of a new industry. On the contrary, they are more likely to respond to industry pressures to remove barriers. And even if policy-makers acted in the public interest in, say, Norway to curtail the unauthorised use of drones, other countries, such as China, may be less inhibited. Should Norway cede a big new market to China? The pressures on Norwegian policy-makers, in the face of a gathering industry in China, are going to be intense. What politician could side-line an industry in his or her own country and effectively give free rein to a foreign industry?

Are drones to our privacy what guns are to our bodies? Is it possible to take action at the international level to curtail the intrusiveness of this emerging technology? Before attempting to answer such questions, we need a much better understanding of drones and their regulatory environment.

Before introducing the articles in this special issue, we need to say something about terminology: "drone" is used here and in four of the five articles. Drone aficionados – especially industry and policy-makers – don't much like the word. Perhaps it suggests something like a zombie or some thoughtless technology on a kamikaze mission. Aficionados prefer more bureaucratic terms, like unmanned aerial vehicle (UAV) or unmanned aerial system (UAS), which are the preferred terms in the US, or remotely piloted aircraft system (RPAS), the term preferred in Europe (and by ICAO). But in the interest of brevity and simplicity, and without wishing to cause undue offence, we like the term "drone".

This special issue of *Computer Law & Security Review* is timely. It comes as we (society) are just beginning to scramble up the bell curve, when the numbers of drones are set to explode, driven by the aforementioned reductions in size and price. This special issue has several articles that provide us with excellent insight into the issues surrounding drones. The span of these articles is comprehensive, covering virtually all aspects of drone issues.

Four of the papers come from Roger Clarke, one of the world's foremost privacy and surveillance experts. His first paper, "Understanding the Drone Epidemic", provides a description and analysis of drones. It describes their emergence and notes their considerable diversity. Drones can weigh more than 150 kg and be used in military applications

[*] Trilateral Research & Consulting LLP, Crown House, 72, Hammersmith Road, London W14 8TH, UK.

E-mail address: david.wright@trilateralresearch.com.

[1] *The Economist*. "Unmanned aircraft: the fly's a spy", 1 Nov 2007. http://www.economist.com/node/10059596.

0267-3649/$ – see front matter © 2014 David Wright. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2014.03.009

yet can also weigh as little 100 g with costs low enough to attract hobbyists and recreational users. Thus, in addition to the larger drones, there are micro drones and even nano drones. They may be fixed-wing aircraft or rotor-bladed craft capable of hovering outside your bedroom window. In order to settle on a satisfactory working definition of drones, the paper identifies the various attributes displayed by drones, including the dimensions of their attitude, operating envelope, attributes enabling survival, degree of autonomy, their remote control. It identifies size, altitude, range of data links and intended missions as distinguishing characteristics.

The paper identifies various drone applications that make them attractive to the military, law enforcement, businesses (big and small) and hobbyists. They can be used to search for missing persons and emergency management in the survey of fires, floods, earthquakes, etc. The major application areas are hobby and entertainment, journalism, law enforcement, community policing and attacks.

In Clarke's second paper, "What drones inherit from their ancestors", the "ancestors" refer to computing, data communications and robotics. The paper also has important sections on cyborgism and surveillance. The paper completes the foundations for the regulatory analysis that follows in the third and fourth papers. The paper explains that computing is inherent within drones, because they involve signal processing, data processing and transmitting computed commands. Clarke's review then shifts from data processing to enable decision-making to the data itself and, in particular, the concern where a single device is the sole or dominant source of data on which a decision-maker depends.

At the end of the section on computing, he draws some conclusions about computing for the design and deployment of drones. He follows a similar, but shorter approach with regard to data communications and its implications for drones. He describes them as forms of distributed robotics. Clarke says that a set of principles is needed to provide humankind protection against the harm that can arise from the uncontrolled design and application of drones (which can be regarded as airborne robots). He provides six principles. Having addressed the ancestors of drones, the author then shows how those who perform the functions of drone pilots and facilities operators can be regarded as cyborgs. He argues that not only is the cyborgisation of drone controllers through physical enhancements of relevance, but so is the psychological dimension. Here he refers to a risk of a "computer games" mentality and some degree of de-humanisation.

Next, Clarke turns to surveillance, and he argues that drones represent a substantial change to surveillance capabilities in at least three ways: they offer new angles for visual surveillance, they avoid ground-level congestion, they reduce the cost-profile. Drones are adding a further dimension to the substantial surveillance threats that already exist. He concludes that "drones greatly expand the scope for surveillance in the visual spectrum and beyond for contributing streams of content to support data surveillance. Such applications of drones threaten substantial negative impacts on personal, social, economic and political behaviour."

Clarke's third paper, co-authored with Lyria Bennett Moses, focuses on public safety related to civilian use of drones. The paper is divided into seven sections. Following the Introduction, section 2 identifies threats, for example, of drones falling out of the sky and hitting something or, worse yet, hitting something explosive or a power cable or, still worse, killing someone. The paper says there are, in theory, natural controls to such risks. Among such natural controls are economic considerations (drones are not yet as cheap as a week's supply of groceries, therefore, owners are likely to take at least some care of them), public opinion and customer attitudes. Clarke does not find such controls sufficient to keep the risks in check. Section 3 explores "Regulation and technological change", first generally and then more specifically in relation to drones. Table 1 helpfully categorises regulatory forms – i.e., formal regulation, co-regulation, industry self-regulation and organisational self-regulation, which guide Clarke's analysis of the regulatory regimes in Australia, Europe and the US. Section 4 discusses how existing laws may contribute to limiting harm from drones. He reviews general liability laws, criminal laws, laws relating to violent acts and laws relating to computing and data communications. Some of these laws might help to act as a deterrent, but they are rather too general and have too many uncertainties if they were to be the only solution to limiting the harms arising from drones.

Section 5 concerns "Regulatory arrangements directly relating to air safety". Clarke reviews air safety laws at the international level as well as those in Australia, the US and Europe. ICAO's Convention on International Civil Aviation specifically leaves the regulation of pilotless aircraft to national laws. ICAO says that "remotely pilot aircraft system (RPAS) engaged in *international* air navigation shall not be operated without appropriate authorisation from the State" (italics added). But what about those drones that don't fly across borders, only across the street to hover outside a competitor's offices? Should those drones be authorised by a regulator? Each individual drone? The burden on regulators of having to process thousands of applications would, I suspect, cause some dyspepsia. Are micro or nano-drones the same as "model aircraft" or should they be subject to similar rules? In Australia, Clarke points out, there are no requirements for model aircraft registration, pilot licensing or model aircraft airworthiness certification. Should there be? Should thousands of model aircraft ("toys") be registered with a regulator?

Clarke not only points to one regulatory gap after another, but has not seen much action by regulators to close these gaps. In the US, business has been lobbying for removal of regulatory shackles and Congress has responded by warranting more permissive drone regulations by September 2015, a deadline that seems unrealistic. In Europe, the European Aviation Safety Agency (EASA) has responsibility for civil aviation within the EU, but for government-operated drones and those lighter than 150 kg, regulation is left to the Member States. However, the European Commission is contemplating the possibility of changing that and, with several Directorates-General involved, led by DG Enterprise, the Commission seems keen for Europe to exploit the potential market, while addressing privacy and data protection gaps.

Clarke considers whether a co-regulatory approach is a suitable way to address the issues raised by drones. While it has some theoretical advantages, he remains sceptical. Co-regulation reduces the resource constraints on regulators and shifts responsibility on to the shoulders of industry, but co-regulation needs to be accompanied by audit and enforcement powers and, as Clarke points out, engagement of other stakeholders, including the public. Industry self-regulation implies that industry associations impose constraints on their members, i.e., the latter are supposed to follow a code of practice. In the case of drones, a relevant such organisation is the Association for Unmanned Vehicle Systems International (AUVSI), which has more than 2700 members from more than 60 countries. However, its code of conduct is brief and more a statement of aspiration than an enforceable set of rules. Another indicator of effective self-regulation is the existence of industry standards, but Clarke does not find such standards for drones. Evidence of the efficaciousness of the last regulatory model, self-regulation, is even more scarce. Clarke concludes his paper with a warning that considerable risk exists of preventable harm arising from drone usage, mainly because countries are moving slowly in developing a regulatory policy covering the categories of drone that ICAO regards as national responsibility.

Clarke's fourth paper examines the extent to which current regulatory regimes exercise control over the use of drones for surveillance of people. It starts off with a discussion of the "dimensions" (or types) of privacy, but then notes that drones particularly impact behavioural privacy, which Clarke defines as being concerned with the freedom of the individual to behave as he or she wishes without undue observation or interference from others. Drones may also impact on privacy of personal experience, i.e., they can monitor the experiences accumulated by a person. The paper then considers the different types of surveillance and, in particular, visual surveillance, which is typically invasive of behavioural and possibly experiential privacy. Clarke points out that the visual surveillance capabilities of drones are somewhat different from other types of visual surveillance. For example, drones can observe and record people in more places than other types of surveillance. Drones may also subject people to scrutiny for longer periods. Drones give paparazzi new powers of observation. Drones will give operators greater facility to engage in voyeurism and surreptitiousness.

Clarke reviews current regulatory arrangements relevant to surveillance. He notes that, unlike the aviation industry which has operated within the framework of an international convention, no such cohesive influence exists in surveillance regulation. Practices, laws and responses to the many challenges presented by surveillance technologies vary enormously among jurisdictions. His analysis of controls over surveillance follows the same structure presented in the preceding paper, i.e., it reviews natural controls, self-, industry and co-regulatory approaches. Here natural controls include technological limitations (e.g., of image quality), physical danger (e.g., from weather and power lines), economic factors, reputation and countervailing powers (e.g., complaints, boycotts, civil disobedience). He does not see self-regulation playing any significant role in controlling surveillance by drones. Ditto regulation by industry codes of practice and co-regulation. Regarding the latter, he argues that for co-regulation to be effective, the views of industry and other stakeholders need to be taken into account within a statutory context with enforcement mechanisms. He concludes that none of the above controls makes any significant contribution to protection against unjustified, disproportionate and unsafe surveillance. The protection of behavioural privacy thus depends on formal regulation.

So Clarke goes on to consider existing generic laws, such as those dealing with trespass, torts and human rights laws, and finds that some could provide some regulatory impact on surveillance. However, aviation laws contain little or no protection against surveillance or intrusion upon privacy. And the snag with many "privacy" laws is that they are focused on data protection, rather than other types (or dimensions) of privacy such as behavioural privacy. Next, he considers surveillance laws, media and law enforcement use of surveillance devices and concludes that "the legal framework [in Australia] governing visual surveillance might be described as a patchwork quilt in which many patches are missing, and the rest are threadbare". Laws that address surveillance specifically are largely intended to authorise surveillance by law enforcement agencies; their privacy protections are weak. In order to address drone surveillance threats, Clarke says proposals need to be subjected to prior evaluation and justification, taking into account the views of stakeholders. He suggests that an effective regulatory regime is needed but elusive. If these papers get in front of regulators, they might lead to meaningful action.

The fifth and final article in this special issues on drones is "Civilian Uses of Unmanned Aerial Vehicles and the Threat to the Right to Privacy" by Uri Volovelsky. Although the paper is billed as "An Israeli Case Study", it makes reference to policies and events in Europe and the US as well. It foresees a rapid expansion in the civilian use of UAVs (Volovelsky uses the US term) in the coming years and considers the implications for the right to privacy. The paper refers to some interesting cases involving drones (e.g., paparazzi used a drone to photograph Tina Turner's wedding). He quotes some statistics, e.g., that 30,000 drones are forecast to fly in US national airspace by the year 2020. He claims that Israel is the world's largest producer of UAVs for military and civilian purposes. As in Europe, Australia and the US, Israel has not yet made UAV operational permits contingent on satisfying some privacy requirements (in addition to safety measures). The prospect of protecting privacy absolutely against intrusions by drones seems illusory. Volovelsky refers to provisions about not allowing the civilian use of drones over densely inhabited areas. Fewer flights will lessen infringements of individuals' right to privacy.

The author agrees that introducing UAVs to the civilian market is a new type of threat to privacy. As in Europe, privacy in Israel is a fundamental right, enshrined in legislation. Drones are not like CCTV. In addition to video recording, drones can identify body heat, chemical substances, and concealed weapons. Drones are not like helicopters either. The latter make a lot of noise and are relatively big. Drones make no noise, are small, can fly undetected and cost a tiny fraction of a helicopter. Some drones are cheap: as little as a few hundred euros. Volovelsky refers to some of the same applications of drones as Clarke. Drones can be used in monitoring, preventing and warning of crises due to natural disasters (floods, earthquakes, fires, nuclear disasters). They can be used to monitor coastal and border areas. Journalists, film-makers and the police are all natural markets for drones. Existing technologies are being integrated into drones, e.g., drones can carry payloads for biometric data, facial recognition, for photography and video recording, night vision and see-through imaging. Drones can carry GPS receivers and be used for voyeurism as well as some worthwhile applications. As elsewhere, the Israeli CAA does not address privacy matters. Its powers to regulate safety do not extend to privacy.

The article concludes that drones will pose "an enormous challenge to the right to privacy". They will infringe that right, but will also provide advantages. The author says it is essential to have a solution enabling civilian use of drones while concurrently protecting the right to privacy. He concludes that to mitigate the risk to privacy posed by drones, policy-makers must establish a new set of statutes, rules and guidelines. Technological and social measures can help protect privacy. Privacy by design and privacy impact measures can also help. Governments must take steps to educate the public about drones. Laws are needed to spell out the obligations of drone operators, with limitations on the type of technology and, in particular, the camera lenses that can be installed on civilian drones. Law enforcement authorities should need a search warrant to use a drone. As with Google Street View, provision should be made for blurring faces and licence plates.

Volovelsky's article is well sign-posted, well-written, stuffed with some interesting factual data. It is clear in its analysis. He presents four "insights". First is that progress in drone technology is inevitable. Second is that it is problematic to have a situation where the regulation of drones is the sole responsibility of CAAs. The Israeli data protection authority (ILITA) should be consulted and play a leading role in shaping the rules and guidelines regarding use of UAVs. The third insight is that a combination of legislative-regulatory, technological and social measures is needed to limit breaches of privacy. The fourth is that the effectiveness of solutions to mitigate risks depends on the ability of states, commercial bodies and individuals to co-ordinate their operations. Governments and policy-makers should initiate public discussion with all stakeholders involved in the design, manufacture and use of drones as well as the "non-profit" sector to identify and monitor effective solutions.

This is sensible advice to conclude a special issue that gives a comprehensive overview of what is going on in the world of drones. One might assume that policy-makers have been rather somnambulant with regard to drones, but in fact, they seem to be aware that there are policy implications with which they must deal rather urgently. In Europe, the European Commission and some data protection authorities are actively addressing the situation. Reports on privacy and data protection implications are underway.[2] National DPAs and European Commission representatives have been meeting and discussing the situation. Australia has also initiated some moves towards legislation addressing the privacy implications of drones, a development which Roger Clarke has described in an e-mail to the author as "one of the more informed and sensible privacy-related documents I've seen from outside the academic and advocacy communities in quite a long time".

The policy environment and the market for drones are likely to evolve rapidly over the next year or two. Both Clarke and Volovelsky call for engagement with stakeholders, an essential ingredient in well grounded policy.

[2] Trilateral Research is conducting a study of the privacy and data protection implications of remotely piloted aircraft systems for the European Commission. The final report is expected before the end of 2014.