Toulouse Business School

From the SelectedWorks of W. Gregory Voss

2013

Privacy law implications of the use of drones for security and justice purposes (Proof)

W. Gregory Voss, *Toulouse Business School*

Available at: https://works.bepress.com/gregory_voss/1/

Privacy law implications of the use of drones for security and justice purposes

W. Gregory Voss

Toulouse Business School (TBS),
Toulouse University,
20 boulevard Lascrosses, BP 7010,
31068 Toulouse Cedex 7, France
E-mail: g.voss@tbs-education.fr

Abstract: With the advent of new technologies, new means of surveillance and data collection have appeared on the radar. Drones are among the latest to be considered for domestic security purposes, both in the EU and the USA. After surveying some examples of the non-warfare use of drone for security and criminal justice purposes, this article analyses applicable privacy and data protection legislation and constitutional guarantees, on both sides of the Atlantic. This study extends to the application to drone-generated data of, inter alia, the Fourth Amendment to the US Constitution, Council of Europe instruments, and the EU Data Protection Framework, highlighting challenges to civil liberties and tensions between these and national security and justice concerns. Finally, this article looks briefly at proposals for legislative reform regarding drones at the US State and Federal levels and prospects for future legislation.

Keywords: drones; UAVs; UASs; RPAs; data protection; data protection law; privacy; privacy law; security and justice; surveillance; aviation law.

Reference to this paper should be made as follows: Voss, W.G. (xxxx) 'Privacy law implications of the use of drones for security and justice purposes', *Int. J. Liability and Scientific Enquiry*, Vol. X, No. Y, pp.000–000.

Biographical notes: W. Gregory Voss is a Professor of Business Law at Toulouse University, Toulouse Business School (TBS) in Toulouse, France. Voss is a member of IRDEIC – Research Institute in European, International and Comparative Law. He obtained a J.D. degree from the University of Michigan Law School and DESS Postgraduate degree in Droit et systèmes d'information from the Université Toulouse 1 Capitole. He is admitted as an avocat to the Bar of Toulouse and as an Attorney-at-Law to the Bar of the State of New York.

This paper is a revised and expanded version of a paper entitled 'The use of images and other data from drones for security purposes: a transatlantic viewpoint' presented at the World Social Science Forum 2013, Montreal, Canada, 13–15 October 2013.

Copyright © 200x Inderscience Enterprises Ltd.

1 Introduction

The coming of new technologies has brought along with them new possibilities for collecting and using data for the surveillance of individuals, whether by the state (e.g., NSA – PRISM Programme) or by the private sector (behavioural advertising, for example). These means have obvious impact on civil liberties and fundamental freedoms. This article focuses on the use of data from drones for security and criminal justice purposes, and takes a transatlantic view, primarily from the standpoint of the USA, the European Union and France.

1.1 Drones as a new technology for surveillance

The dictionary defines a 'drone' as: "…3: an unmanned aircraft or ship guided by remote control".[1] A synonym for our purposes is 'unmanned aerial (or air) vehicles' (UAVs), also known, together with the systems that surround them, as 'unmanned aircraft systems' (UASs)[2] (sometimes known as unmanned aerial systems), or even 'remotely piloted aircraft systems' (RPAS). RPASs, which are 'under control of a remote pilot-in-command for the entire flight under normal conditions and movements on the ground', include not only the 'drone', but also the system involved. The European RPAS Steering Group states that "RPAS belong to the wider family of Unmanned Aircraft Systems (UAS), which also comprises 'autonomous' RPAS (i.e., no human action is necessary after take-off)."[3]

Drones already exist domestically – whether in the US or in Europe – and are being used for different purposes, including as a new technology for surveillance. When incorporated into a system, drones may use GPS technology, advanced camera technology (e.g., high resolution lenses), and embedded computer systems (chips and controllers), providing them with certain advantages over previously existing surveillance methods, such as ground-level optical observation. The fact that they may be operated without personnel onboard allows them to be used when conventional aerial surveillance is too costly, or for long periods of time where personnel fatigue is an issue. In addition, the fact that they do not require onboard personnel allows them to be designed smaller, making them less obtrusive and less expensive than other forms of aircraft (i.e., airplanes and helicopters) used for surveillance. Drones may obtain personal data, such as images, in digital form, allowing for easy processing afterwards.

Up to now, the use of drones has been limited by aviation regulation. The US FAA Modernization and Reform Act of 2012 (FMRA)[4], a 2012 French decree regarding the use of airspace by drones[5] and the eventual implementation of the European RPAS Steering Group's Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, will lead to an increased use of drones in the US and Europe. In addition, the reduction of their use in foreign armed conflict situations (in the case of the US) may give impetus to their integration into the domestic sphere. For example, the United States Senate Committee on Armed Services recommended taking measures to incorporate UASs into the US National Airspace System (NAS) in order to further their development:

> "Large Numbers of UASs now deployed overseas may be returned to the United States as the conflict in Afghanistan and operations elsewhere wind down in coming years, and new UASs are under development. Without the ability to operate freely and routinely in the NAS, UAS development and

> training – and ultimately operational capabilities – will be severely impacted…. DOD [Department of Defense]'s leadership belatedly realized how important and difficult UAS NAS integration would be. While progress has been made in the last 5 years, the pace of development must be accelerated."[6]

This move to the domestic use of drones will likely be spurred on by industry, as well as government.[7]

According to one author, "[n]early 90 other [than the US] countries already have surveillance drones in their arsenals, and China is producing several inexpensive models for export."[8] Nonetheless, we will focus on the US, Europe and France, so let us now briefly survey the current domestic use and potential use in a near future of drones there, while noting relevant aviation regulation provisions having an impact on such use.

1.2 Aviation requirements and use of drones in the United States

The utilisation of drones in the United States today is restricted by the Federal Aviation Administration. The FAA requires that specific authorisation must be obtained in order to operate a UAS. Today the FAA issues Certificates of Waiver or Authorization (COA), for public aircraft[9], or issues special airworthiness certificates, for civil aircraft, to authorise UAS flight operations.[10] For model aircraft, there is an FAA Advisory Circular which allows their use.[11] The FAA only issues certificates in the experimental category for civil drones under 14 CFR §§21.191, 21.193, and 21.195. The civil aircraft that fit in this category are not authorised to utilise drones for commercial use (for compensation or hire), but at the time that its notice of policy on UAS was written, the FAA had authorised five certificates for the "purposes of research and development, marketing surveys, or crew training".[12]

For public use, COAs are typically issued for a year's time, but a COA is not required if the UAS is only operated "within an active Restricted, Prohibited or Warning Area airspace when operating with permission from the appropriate authority or using agency of that airspace".[13]

The FAA is currently establishing test ranges for the integration of UAS (both for public and private use) into the NAS, which are to be operational until February 2017[14], and in that connection, following public consultation, has published final privacy requirements for the test site programme.[15] These take the form of terms and conditions added in Article 3 of the other transaction agreement (OTA) for the programme and require a site operator to have publicly available privacy policies governing UAS authorised by it.[16] Such policies must comply with applicable privacy laws, including any changes to such laws.[17] In addition, the site operator must "[r]equire each UAS operator in the Test Site to have a written plan for the operator's use and retention of data collected by the UAS."[18] Although these minimal privacy requirements have the merit of existing, their scope is quite limited as they only cover the test programme.

With this information in mind, we may divide examples of current and potential uses of drones in the United States into the following categories:

- Current public aircraft uses: Customs and Border Protection agency (CBP) surveillance; law enforcement and crime prevention; local police agencies; FBI; Drug Enforcement Administration; security; training; National Guard (in preparation for use overseas); and drone testing are examples.

- Potential future public aircraft uses: e.g., search and rescue missions; and firefighting.
- Potential future civil aircraft uses: such as advertising, agriculture, journalism, and surveillance (private/commercial).

As drone technology becomes more familiar, potential new uses may be found, such as the recent announcement of the potential use of drones by Amazon for the delivery of packages to customers.[19]

1.3 Aviation requirements and examples of the use of drones in Europe including France

In Europe, where RPAS "have been used by State entities, civil or military, for security reasons"[20], the scope of the mission of the European Aviation Safety Agency (EASA) – the European aviation authority and counterpart to the US's FAA – specifically excludes "[aeronautical] products, parts and appliances, personnel and organisations [involved in the design, production and maintenance of such products, parts and appliances]" when they are "engaged in military, customs, police or similar services". Responsibility for such services, which are the basis for the use of drones for security and justice purposes, is left to the EU member states.[21]

In France, for example, an Order of August 1, 2007[22] was a first step to allowing the use of military and civil drones in segregated air space and in order to allow the taking of photographs by the police, customs, civil security, etc.[23], and this was repealed and replaced by the Order of December 21, 2009[24], which in turn was repealed and replaced by the current Order of April 11, 2012[25], the latter truly being aimed to help develop the civil use of drones in France.

With respect to the use of drones in Europe, the Washington Post cited the Guardian in 2011, for the information that [a] consortium of police departments in Britain [were] developing plans to use [drones] to monitor the roads, watch public events such as protests, and conduct covert urban surveillance.[26]

In Germany, drones have been announced for tests by the Deutsche Bahn railway company to fight against graffiti vandalism of trains.[27]

The French have used them both for public and private purposes. For private purposes their use has been especially for capturing images, such as the French production company, Elle est pas belle la vie (LPBV), did for film shots, or for visual inspection on the inaccessible and monumental Millau Viaduc project, according to Slate.fr.[28] "Drone journalism", involves the French media using drones – with their cost far below that of a helicopter – for the advantages of the multiple possible viewpoints they afford.[29] ERDF; a subsidiary of the French electricity company EDF, was said to plan to test them for use in the surveillance of electric lines in the Rhone-Alpes Region.

On the public side, firefighters in the Southwestern French department of the Landes have been using them to conduct surveillance in forests during the summer period.[30] The city of Marseilles plans to use them to do surveillance on drug dealers and improve the city's security.[31]

Although there is suspicion that the French had used drone surveillance in instances of public riots in suburban Paris in 2005[32], Thierry Delville, a man described as the 'Mister Drone' of the French National Police is said to have stated that drones were not used then – manned aircraft were – and to have indicated that small drones are destined

for special forces such as the French equivalent of SWAT teams (GIGN and RAID) to secure or conduct surveillance in crowds, but that there are fears of them accidentally falling in a crowd.[33]

Taking a look further, and with a bit of imagination, an Article 29 Working Party (an independent European Union advisory panel, which gives guidance on privacy directives to member states, which then can be used by member state data protection agencies or legislators[34]) has issued an opinion on biometric technologies which includes an example regarding surveillance (albeit private) showing a potential use of drones. In the example, a next generation shopping centre implements a video surveillance system.

The example suggests that "potential car thieves could be identified and tracked before they even touch a car" in the center's car parking facility. "If needed tele-guided aerial vehicles (drones) with cameras and other sensors could keep track of suspects until the suspicion is diverted or confirmed. Objects hidden in clothing (knives or shoplifted items) could be detected", the opinion example continues. It then points out that, "[a] similar application has been designed in the INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) project where technologies are combined to fight potential acts of terrorism and crime before it happens."[35] The sky's the limit!

1.4 Images and other data collected by drones for security purposes

Images, whether they are still or moving images (video), may be obtained from properly-equipped drones. In addition, drones may capture heat (thermic) data including thermal imaging, infrared images[36], sound data (through microphones), may intercept data travelling in the internet, cell and other telephone conversations, etc. The ability to capture different kinds of data using drones will likely further develop as new technologies see the light of day. The drone is the vehicle that enables the technologies to fly, a medium and not the actual determinant of the data that may be obtained. Obviously, these images and other data are of interest to police and other officials for security purposes, but are subject to certain constitutional provisions, and applicable data protection and privacy legislation.

2 Current constitutional provisions and data protection and privacy legislation governing the use of drones for security purposes

Data protection and privacy law are at the heart of our analysis, and this from a transatlantic view.

From an international standpoint, Article 12 of the Universal Declaration of Human Rights provides:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [37]

The way this universal concept of privacy has been translated into national or regional law has varied. The European RPAS Steering Group, "a group of key European stakeholders" mandated by European Commission DG Enterprise and DG Mobility and Transport for "the elaboration of a roadmap for the safe integration of civil RPAS into the

European aviation system starting in 2016"[38], highlighted one difference between the EU and the US in the area of privacy, in an annex to its Final Report:

> "In the US privacy is seen as a protection from government intrusion into the private life. In Europe privacy is regarded as a human right to be protected from any kind of intrusion, governmental or not."[39]

One American scholar speaks of 'significant privacy conflicts' between the US and Western Europe.[40] Citing Robert Post, he describes a divide between privacy as an aspect of dignity in Western Europe, while privacy is an aspect of liberty in the US.[41]

We will start our analysis with a study of relevant US law.

2.1 United States

In the context of security and surveillance, the Fourth Amendment to the United States Constitution is the starting point for any analysis of privacy in the context of surveillance. As one scholar stated, "… American 'privacy' law, however ingenious its elaborations, always tends to image the home as the primary defense, and the state as the primary enemy."[42]

As of writing, there has not yet been a case at the United States Supreme Court level involving drones and privacy. Nonetheless, existing principles may be analysed so as to apply them to new technologies, such as drones. Thus, to begin our analysis we will review certain other case law of the United States Supreme Court involving the State and actions nearer or farther from the 'home', in each case relating to the Fourth Amendment, which provides as follows:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[43]

This 'search and seizure' Amendment has been the subject of extensive United States Supreme Court interpretation, which has resulted in the development of various doctrines and exceptions. One such exception to the requirement is that, in order for a law enforcement officer to conduct a search or seizure, he or she must obtain a valid search warrant is the 'plain view' exception.[44] Although the Supreme Court has not yet ruled in a case involving drones, we can still see that this exemption is important with respect to drones which view people, their property and their behaviour from the air, such as did other aircraft in the following three cases involving airplanes (in two cases) and a helicopter (in a third case).

The first important case on this issue is *California v. Ciraolo*.[45] In the 5-4 *Ciraolo* decision, the Fourth Amendment was found not to have been violated by an aerial observation of marijuana plants in Ciraolo's backyard. In order to come to the judgment that it rendered, the Court had to determine whether Ciraolo has a "constitutionally protected reasonable expectation of privacy". Two tests, derived from the earlier cases of *Katz v. United States*[46] and *Smith v. Maryland*[47], were applied to come to this result: "first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"[48]

In this case, where the plants were in Ciraolo's backyard and he had built a 10-foot fence to conceal the plants from street-level, the first test was met (although the court did not have to decide the issue, as California did not challenge the lower court's finding in this direction). For the second test, the court applied a standard from its earlier decision in *Oliver v. United States*.[49] This was "whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment".[50] That is, whether the Fourth Amendment protected Ciraolo' s backyard (in the common law 'curtilage'[51] of the home) from police view at 1,000 feet altitude without a warrant. In doing so, the court drew an analogy to police officers not being required to "shield their eyes when passing by a home on public thoroughfares", and found that there was no such protection:

> "The observations by Officers Shutz and Rodriguez in this case took place within public navigable airspace, see 49 U.S.C. App. § 1304, in a physically nonintrusive manner; from this point, they were able to observe plants readily discernible to the naked eye as marijuana. That the observation from aircraft was directed at identifying the plants and the officers were trained to recognize marijuana is irrelevant. Such observation is precisely what a judicial officer needs to provide a basis for a warrant. Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. On this record, we readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable, and is not an expectation that society is prepared to honor."[52] *(citation omitted)*

Here, objects in 'plain view', albeit viewed from an airplane at 1,000 feet, were not protected from surveillance.

In a second, similar case – *Florida v. Riley*[53] – a helicopter was used to make observations with respect to the contents of a greenhouse through openings in its roof, and to conclude that marijuana plants were inside. The greenhouse was in a residential backyard and the investigating sheriff's officer made naked-eye observations from an altitude of 400 feet.

The Supreme Court followed its *Ciraolo* decision, and its premise that "the home and its curtilage are not necessarily protected from inspection that involves no physical intrusion," to arrive at a similar conclusion.[54] Public navigable airspace for fixed-wing aircraft descended as low as 500 feet, however such limit did not apply to helicopters, which "are not bound by the lower limits of the navigable airspace allowed to other aircraft".[55] (Citation omitted). The court emphasised that the helicopter was not violating the law, that it was not 'sufficiently rare' for one to be flying at such altitude so as to lend substance to Riley's claim "that he reasonably anticipated that his greenhouse would not be subject to observation from that altitude", "[a]s far as the record reveals, no intimate details connected with the use of the home or curtilage were observed", etc., and thus that no Fourth Amendment violation had occurred.[56]

In a third case involving not an individual, but a legal person, and not the police but an administrative agency, the taking of aerial photographs from within lawful navigable airspace was found permissible without an administrative warrant. This case – *Dow Chemical Company v. United States*[57] – involves the Environmental Protection Agency (EPA) hiring an aerial photographer to fly over the industrial plant complex of Dow Chemical in order to take aerial photographs using a "standard precision aerial mapping camera" to conduct an investigation under the Clean Air Act. The holding – "that the taking of aerial photographs of an industrial plan complex from navigable airspace is not a search prohibited by the Fourth Amendment"– takes into account the lessened level of

the protection of privacy accorded to an industrial complex – treated as comparable to an open field[58] – in contrast to that afforded the 'curtilage' area of the backyard of someone's home.[59]

Once again, we can see that protection of privacy is greater the closer to the 'home' that you are, and becomes weaker as you stray from man's 'castle'.[60]

Although not directly applicable to the surveillance of individuals, the *Dow Chemical Company* case is interesting for its *dictum*. Here, where an aerial mapping camera was used – whose photographs could be enlarged – the court noted that:

> "It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant. But the photographs here are not so revealing of intimate details as to raise constitutional concerns. … [t]he mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems. An electronic device to penetrate walls or windows so as to hear and record confidential discussions of chemical formulae or other trade secrets would raise very different and far more serious questions; other protections such as trade secret laws are available to protect commercial activities from private surveillance from competitors."[61] *(Citations omitted)*

The court acknowledges (without deciding the fact, which was not brought to it in this case) that, even though there are fewer concerns about privacy in the context of an industrial plant than with respect to a home, intrusion by certain technology unavailable to the public may be prohibited by the US Constitution.

What these three cases indicate is that it is permissible to carry out surveillance without a warrant, including the capture of images, from the air, so long as the law is not violated by the operation of the aircraft, helicopter, etc. However, *dictum* has indicated that the use of other technologies, such as satellites, which are generally unavailable to the public, might require a warrant. In addition, one factor to be assessed is whether or not the image data is "so revealing of intimate details as to raise constitutional concerns", although one wonders what these intimate details are meant to be.[62]

In another Supreme Court case – *Kyllo v. United States* – the use of technologically-enhanced thermal imaging of the home in order to find marijuana was disallowed. In that case, the technology was not being used from the air, but from a car in the street, and the use was considered to be a search as it provided information from within the house without a warrant.[63] The *Kyllo* case suggests that there are limits to the use of invasive new forms of technology which allow law enforcement officers to virtually pass through the walls of a home.[64]

In conclusion, under the Fourth Amendment to the United States Constitution, there seem to be no legal impediment to the use of drones for surveillance in most instances, especially when used for the capture of images, if the drones are operated legally – even without a court warrant. This or similar opinions have been adopted by various legal scholars.[65] However, we should caution, in light of the protection of the home and its curtilage area, that invasive –technologies allowing the obtaining of data from within the house would likely be disallowed, absent a valid warrant based on 'probable cause' – that is, a reasonable basis that evidence of a crime that has been committed is located at the place that the drone will survey.

But once the data from drones gets into the US law enforcement system, what happens? On the Federal level, the FBI runs an 'electronic clearinghouse of crime data', called the National Crime Information Center (NCIC). According to the FBI,

> "NCIC policy establishes a number of security measures to ensure the privacy and integrity of the data. The information passing through the network is encrypted to prevent unauthorized access. Each user of the system is authenticated to ensure proper levels of access for every transaction. To further ascertain and verify the accuracy and integrity of the data, each agency must periodically validate its records. Agencies also must undergo periodic audits to ensure data quality and adherence to all security provisions."[66]

More importantly, the FBI is subject to the Privacy Act of 1974, which sets forth procedures for the use of personally identifiable information about individuals by federal agencies.[67] The Privacy Act provides conditions for the disclosure of records regarding individuals[68], requires accounting for certain disclosures[69], allows a right of access to records by their data subject[70], and, subject to conditions, a right to request amendment.[71] In addition, requirements are set out regarding the maintenance and collection of information[72], civil remedies and criminal penalties are available in the event agencies do not comply with the legislation.[73] Nonetheless, certain investigatory material compiled for law enforcement purposes may benefit from one of the specific exemptions from certain of the foregoing requirements.[74] Finally, pursuant to the Privacy Act, the FBI established ten 'blanket' routines for permitted parties to whom information may be disclosed form the system of records, which apply, *inter alia*, to the NCIC as well as to the FBI Central Records System.[75]

Privacy protections may apply at the state and local level, as well, although other than our discussion of recent state legislative initiatives targeting drones, these are outside the scope of this article.

We will now investigate Council of Europe and European Union privacy law, insofar as they affect the operation of drones for security purposes. We will follow that discussion with one regarding protection in France, before turning to a new section on United States protection.

2.2 Council of Europe

European privacy protection arises on different levels. We start our discussion with two conventions of the Council of Europe – an organisation to which the member states of the EU belong, but which includes other nations in Europe, including the Russian Federation and Turkey.[76]

One source of protection is the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), whose purpose "… is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him…."[77] Convention 108 requires parties to the Convention to implement the data protection principles of Convention 108 in domestic law, including those relating to data quality and data security, the requirement of appropriate safeguards for 'special data', information requirements, data rectification and erasure provisions and remedies.[78]

Convention 108 applies generally to both public and private authorities. However, derogations from these principles and requirements (except for those in Article 7 related

to data security) are allowed in the interests of "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences".[79] These are some of the sorts of interests which are involved in the use of drones for security purposes. Nonetheless, one part of Convention 108 which is interesting for the purposes of our subject is the requirement of taking, "[a]ppropriate security measures … for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."[80]

Another instrument leading to privacy protection – whose ratification is a prerequisite for joining the Council of Europe – is the Convention for the Protection of Human Rights and Fundamental Freedoms, known as the "European Convention on Human Rights" (ECHR).[81] Article 8 of the ECHR provides as follows:

> "Article 8. Right to Respect for Private Life and Family
>
> 1 Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[82]

Once again, national security, public safety and the prevention of crime – purposes for the use of drones discussed in this article – are carved out, in this case in Article 8(2) of the ECHR, reproduced above. However, in order to fit within the carve out, certain conditions must be met under the case law of the European Court of Human Rights (ECtHR): a right protected by Article 8 must be involved (interfered with); the relevant action under Article 8(2) must be "in accordance with the law" (that it be based on domestic law and that this basis accord with the rule of law (regarding accessibility and foreseeability for citizens); and such action must be "necessary in a democratic society".[83]

Although this author is aware of no ECtHR case involving the use of drones for domestic surveillance, an application of these concepts involving surveillance using new technologies (GPS) indicates that the above conditions may be met, without too much difficulty, indicating that ECHR member states may have a relatively large lee way in the implementation of such surveillance. This analysis would presumably apply to the use of drones for surveillance, as well.

In the case of *Uzun v. Germany*[84], the ECtHR (Fifth Section) reviewed allegations that observation of him by GPS and the resulting use of data violated his rights under Article 8 of the ECHR.[85] The ECtHR noted that "GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life."[86]

In *Uzun*, the ECtHR, when evaluating whether the action was "in accordance with the law" under Article 8(2) of the ECHR, noted that where, as is the case here, the surveillance was carried out with regard to movements in public places, there is less of an interference with his public life than with, for example, interception of telephone conversations. Moreover, the ECtHR which noted that the surveillance has a basis in German statute law (Code of Criminal Procedure)[87], observed that the Public Prosecutor

had ordered the surveillance and that there were adequate opportunities for judicial review of the legality of such measures. The ECtHR considered that this first requirement of Article 8(2) had been met.[88]

The ECtHR next dealt with the requirement that the action be "necessary in a democratic society." Here, necessity corresponds to a 'pressing social need', proportionate to the 'legitimate aim pursued'. In the circumstances, where a terrorist group claimed responsibility for several counts of attempted murder and evaded means of visual surveillance, the ECtHR found that the action met this second requirement of Article 8(2) and thus, that there was no violation of Article 8 of the ECHR.[89]

In sum, these two Council of Europe instruments provide some privacy guarantees for citizens (respect for fundamental rights, implementation of data protection principles, respect for home, etc.), although in the context of the use of drones and resulting data for security purposes, certain exclusions may apply.

According to the European RPAS Steering Group, the focus of the ECtHR has been more on the protection of individuals from the dissemination of personal information (or what we may call information privacy), than from the collection of the information itself (or location privacy), which contrasts with US Fourth Amendment cases discussed above. This information privacy orientation is that of the EU Directives and Regulations on the processing of personal data.[90]

2.3 European Union

At the EU level, several legal instruments provide guarantees with respect to privacy and data protection, which might apply in case of the use of drones (and that data that result from their use) for security and justice purposes. We will look at these one by one.

The main instrument that exists today with respect to data processing in the EU is the Data Protection Directive of 1995 (DP Directive).[91] However the DP Directive specifically excludes "processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."[92] Thus, another instrument must be relied upon with respect to such processing of data obtained through the use of drones for security and justice purposes.

The Council Framework Decision 2008/977/JHA (Framework Decision) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[93] was adopted under Article 34(2)(b) of the version of the Treaty on European Union in effect prior to the final adoption of the Treaty of Lisbon, and has as its purpose, to "ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters".[94] However, the decision applies to cross-border processing of data[95] and not to purely national member state data processing by police and judicial authorities. Thus, an analysis of whether or not the framework decision applies will hinge upon whether there is cross-border criminal cooperation between different member states or not.

In addition, Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), which came into effect after the final adoption of the Treaty of Lisbon, provides, simply, that "[e]veryone has the right to the protection of personal data concerning them."[96] The European Parliament and Council were called upon to lay down rules to protect individuals from the actions of EU institutions, bodies, offices, agencies and

member states with respect to their personal data, without prejudice to specific rules under Article 39 of the Treaty on the European Union (TEU).[97] That article provides that the council may adopt rules regarding the protection of individuals with respect to the processing of their personal data by member states in the exercise of their activities in the areas of foreign policy and public security, subject to the control of independent authorities.[98]

Moreover, Article 6 of the TEU provides that the EU "recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000 … which shall have the same legal value as the [EU] Treaties."[99] The charter provides that everyone has a "right to respect for his or her private and family life, home and communications"[100], and a "right to the protection of personal data concerning him or her."[101] Processing of that data must be done fairly, be for 'specified purposes', be legitimatised by consent or other legitimate basis provided for by law, and rights of access and rectification with respect to the data are granted to the data subject.[102] The charter allows for limitations to be placed on the exercise of these rights, but these must be "provided for by law and respect the essence of those rights and freedoms."[103]

Thus, although current EU treaties and legislation provide various protections for privacy and personal data, some of these instruments exclude protection in the area of criminal offenses and security, thus negating their interest in the context of the use of drones.

Now, let us turn to the current EU data protection framework reform.

On January 25, 2012, the European Commission announced proposals for reform of its data protection framework, including the DP Directive. These included a proposed General Data Protection Regulation (GDPR)[104] and a proposed Police and Criminal Justice Data Protection Directive (Justice DP Directive).[105] Although these two instruments have not yet been adopted and are subject to amendment and debate, we will refer to them in their original form, as initially proposed by the Commission.

The GDPR, which if adopted would repeal the DP Directive, specifically excludes data processing for national or EU security[106], or "by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."[107] Thus, the GDPR excludes the security and justice aspects of drones which are the subject of our study, and is thus irrelevant for our purposes.

On the other hand, the proposed Justice DP Directive, which if adopted would repeal the framework decision, provides specific rules in the fields of judicial and police cooperation. It sets out a duality of interests to be protected or ensured by member states – that of the protection of individuals' fundamental rights and specifically that of the protection of their personal data, and that of ensuring that "the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data."[108] The Justice DP Directive does not apply, however, to the processing of personal data "in the course of an activity which falls outside of the scope of Union law, in particular concerning national security …."[109]

The Justice DP Directive, if adopted, would establish data protection principles applicable to the processing of personal data in the area of justice, such as fair and lawful processing, proportionality, accuracy, limited conservation time, and responsibility[110] that would clarify and enhance the rights of data subjects. In addition, certain data subject rights, such as the right to information about processing, rights of access, rectification,

and erasure exist under the proposed Justice DP Directive.[111] However, member states may require such rights to be "carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings", thus potentially limiting their scope.[112] In addition, as this instrument is in the form of a Directive, it would have to be implemented into the national laws of the member states, and differences in methods or forms of such implementation could result. Nonetheless, the targets of drone surveillance would have certain rights and guarantees with respect to the processing of their personal data obtained through the use of drones, outside of those cases considered as 'national security'.

To conclude, potential advance in terms of EU protections regarding the use of personal data obtained from drones would be obtained with the adoption of the Justice DP Directive, however for a complete analysis of the privacy and data protection provisions applicable to the use of drones in the EU, we must turn to the law of the member states. This article's analysis will be limited to a short discussion of the situation in France, as one example of a member state's legislative provisions.

2.4 France

The French Law on Information Technology, Data Files, and Civil Liberties[113] applies both to public and private sector controllers of personal data, establishing the necessity of complying with privacy principles similar to those in other EU countries under their national legislation that implements the DP Directive. Nonetheless, there are distinctions drawn between the public and private sectors in the text of the legislation. For example, in the case of the "performance of a public service mission" entrusted to it, a data controller is not required to obtain the consent of the data subject prior to processing his or her personal data.[114] Such would be the case, for example, where images constituting personal data are obtained in a police investigation using a drone.

In France, the *la Commission nationale de l'informatique et des libertés* (CNIL) – the French data protection agency – announced on October 30, 2012 that it has undertaken a study of the subject of drones and privacy following the opening of the French sky to drones.[115] It underscored that, as soon as one of the diverse types of objects known as a drone is equipped with a camera, a video camera, sound-recording equipment or a geopositioning device, it may violate privacy rights and collect and distribute personal data, and that the taking and distributing of images of individuals is subject to the French Data Protection Act.

Thus, although the use of drones for surveillance may be allowed in France, within the constricts of aviation regulation and law, it is controlled and may be subject to criminal procedure requirements and such further limitations as may be decided in the future, based on the results of current study.

3 Legislative proposals and potential future changes to law as a result of the use of drones

3.1 US state laws enacted or proposed

The American Civil Liberties Union (ACLU) is tracking US State legislation proposals involving drones.[116] According to the ACLU, legislation has been proposed in 42 states, enacted in eight states, and is active in six states, and that "almost all of the bills [they]'re seeing require law enforcement to get a probable cause warrant before using a drone in an investigation."

Table 1 States that have adopted legislation restricting drone use (as of October 9, 2013)

State	*Act number*	*Act date*	*Act name*	*Effective date*
Florida	SB 92 (Chapter 2013-33[117])[118]	4/26/2013	Freedom from Unwarranted Surveillance Act (short title)	7/1/2013
Idaho	SB 1134 (Chapter 2, Title 21, Section 21-213) (Session Law Chapter 328)[119]	4/11/2013	Act relating to Aeronautics; to Define a Term, to Establish Provisions Relating to Restrictions on the Use of Unmanned Aircraft Systems, to Provide Exceptions, to Provide for a Civil Cause of Action, to Provide for Certain Damages and to Provide that an Owner of Certain Facilities Shall Not Be Prohibited from Using an Unmanned Aircraft System to Inspect Such Facilities	7/1/2013
Illinois	Public Act 098-0569[120] (S.B. 1587)	8/27/2013	Freedom from Drone Surveillance Act (short title)	1/1/2014
Montana	S.B. 0196 (Codified in Title 45 chapter 5 part 2 and in Title 46 chapter 5)[121]	5/1/2013	Act Limiting the Use of Unmanned Aerial Vehicles by Law Enforcement and Private Users; Prohibiting the Use of Unlawfully Obtained Information as Evidence in Court; and Amending Section 46-1-202 MCA	10/1/2013
Oregon	H.B. 2710 A Chapter 686, (2013 Laws)[122]	7/29/2013	Act relating to drones; and declaring an emergency.	7/29/2013
Tennessee	Pub. Ch. 470 (S. B. 796) (Amends Title 39, Chapter 13, Part 6)[123]	5/31/2013	Freedom from Unwarranted Surveillance Act (short title)	7/1/2013
Texas	H.B. No. 912 (Subtitle B, Title 4, Government Code – Texas Privacy Act – Chapter 423)[124]	6/14/2013	Act relating to images captured by unmanned aircraft and other images and recordings; providing penalties.	9/1/2013
Virginia	*HB 2012 (Chapter 755)*[125]	*4/ 3/2013*	*An Act to place a moratorium on the use of unmanned aircraft systems.*	*7/1/2013*

The states where legislation was enacted (as of December 17, 2013) are indicated in Table 1.

Of these states, the majority (five – Florida, Illinois, Montana, Tennessee and Virginia) restrict drones for law enforcement use, and the others for private use (those others are Idaho, Oregon and Texas; one author argues, however, that Federal aviation law preempts those statutes which restrict private use).[126]

Other state laws have been adopted regarding drones, but not with respect to the central security and justice focus of this article. These include an Illinois bill to prohibit the use of drones to interfere with hunters or fishermen, bills providing financing for potential FAA UAS test sites (Maryland, Nevada, and North Dakota), or financing for a pilot training programme (Hawaii), and one state's legislature (North Carolina) places a moratorium (until July 1, 2015) on the procurement or use by state and local personnel of UAS[127] or disclosure of 'personal information about any person acquired through the operation of an unmanned aircraft system, unless the procurement, use or disclosure is approved through an exception by the Chief Information Officer for the State's Department of Transportation.[128]

3.2 Federal bills proposed and potential future legislative impact

There have been several bills[129] proposed in the US House of Representatives and in the US Senate concerning drones, such as Senator Paul Rand's "Preserving Freedom from Unwarranted Surveillance Act of 2013"[130], or Senator Mark Udall's "Safeguarding Privacy and Fostering Aerospace Innovation Act of 2013".[131] Both bills cited have been submitted to the Senate Committee on the Judiciary (where they stand as of this writing), however no bill restricting the use of drones has yet to be enacted at the Federal level.

Already two years ago, the prospect of the use of drones as "a new and relatively cheap surveillance tool in domestic law enforcement", able to operate low in the sky, while remaining relatively unseen by the human eye, was seen as a potential catalyst for a privacy debate.[132] This may be due in part to the expectation that they could be used pervasively for surveillance, and also allowing for the power of the cameras that they may carry over private property.[133] As University of North Dakota Aviation Department Professor Joseph J. Vacek said, "[m]ost people are not okay with constant watching. That hover-and-stare capability [of drones] used to its maximum potential will probably ruffle a lot of civic feathers."[134]

So, yes, there is the potential for greater impetus for the adoption of privacy legislation at the Federal level as a result of the use of drones but that legislation, like the legislation currently being adopted at the state level, might just be limited to drones, and not a more global general privacy legislation. Or perhaps, another example of harm done to privacy – that revealed in Edward Snowden's disclosure of the NSA's PRISM programme[135], might be the catalyst for privacy reform instead.

3.3 Implications for justice, freedom and security

We might ask, why worry so much about privacy in the context of the use of drones? Why does the use of drones pose so many threats to justice and freedom?

Drones can be inexpensive and easy to obtain and use, thus easy to adopt, without reflecting much on the necessity or the wisdom of their use. Drones, because of their

'stealth' nature, that is their being able to operate without easy detection, because of their ability to hover over a surveillance target for large time spans, because of their ability to use precision technology to capture images of small objects from high up, have been described as "silent monitors in the sky that can observe everything we do in any area exposed to the sky."[136] Thus, privacy becomes impossible in areas which are open to the sky.

An additional danger is that new technology is adopted without ample thought of about its implications. A staff attorney at the ACLU describes the situations as follows:

> "More and more when it comes to monitoring the public, capability is driving policy. The limits of law enforcement surveillance are being determined by what is technologically possible, not what is wise or even lawful. And it's not uncommon for the police to use a new technology in secret for as long as they can, and then allow the courts to sort out legality once the issue finally comes before them."[137]

As more technological possibilities become available for incorporation onboard drones, the more police will use them, the logic goes. And there is also the possibility that the personal data collected be subject to 'mission creep'[138] when shared with others, and deviated from its original purpose to be used for other, perhaps less societally justifiable purposes. That is, unless the legislator or the courts set limits.

4 Conclusions

The use of images and other data from drones for security purposes has not yet been the subject of specific legal provisions. However, existing legal principles must be complied with in order to allow this use. Characteristically, European law provides more protections once data has been obtained from drones (information privacy), based on existing constitutional principles and legislation related to rights of personhood including dignity of the person, than US law focused on government intrusion (location privacy). Constitutional guarantees in the US do exist, but these focus on the initial obtaining of the data and its use as evidence, as well as on the home and the area of curtilage around the home, with the plain view exception that we have seen.

Already, in the USA, various legislative proposals have been made to regulate the use of drones – at the federal, state and local level – and several state acts have been adopted in this sense. Because of the nature of drones there is the possibility that their use may give impetus to the adoption of new privacy legislation at the Federal level in the USA, although these elements may be of lesser influence than the disclosure of the NSA PRISM programme.

Notes

1 http://www.merriam-webster.com/dictionary/drone (accessed 10 December 2013).

2 Unmanned aircraft systems or UASs include the drone together with "associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system." FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95 [hereinafter FMRA], Sec. 331(9), at 62, available at http://www.gpo.gov/fdsys/pkg/BILLS-112hr658enr/pdf/BILLS-112hr658enr.pdf/. The FAA now uses the term UAS and no longer

refers to UAVs. See, e.g., Federal Aviation Administration, *Aeronautical Information Manual (AIM) 0705*, Sec. 5 (potential flight hazards), para. 7-5-5(a) (unmanned aircraft systems) (August 22, 2013) at http://www.faa.gov/air_traffic/publications/atpubs/AIM/aim0705.html.

3 See Eur. RPAS Steering Grp. (ERSG), Final Report: Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, June 2013, p.5 [online] http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf.

4 FMRA, *op cit*., fn. 3.

5 Arrêté du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord [Order of Apr. 11, 2012 Relating to the Use of the Airspace by Unmanned Aircraft], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], May 10, 2012, p.8655.

6 Staff of S. Comm. on Armed Forces, 112th Cong., Rep. on National Defense Authorization Act for Fiscal Year 2013 to Authorize Appropriations for Fiscal Year 2013 for Military Activities of the Department of Defense, for Military Construction, and for Defense Activities of the Department of Energy, to Prescribe Military Personnel Strengths for such Fiscal Year, and for other Purposes, Together with Additional Views, Rep. 112-173, Sec. 1046, p.191 (2012), available at http://beta.congress.gov/112/crpt/srpt173/CRPT-112srpt173.pdf. This report is briefly discussed in Gene Healy, Game of Drones, Washington Examiner, June 11, 2012 [online] http://washingtonexaminer.com/game-of-drones/article/718086.

7 See, e.g., Boghosian, H. (2013) *Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance*, p.28.

8 Byman, D. (2013) *Why Drones Work: The Case for Washington's Weapon of Choice*, Foreign Aff. 32, July/August, Vol. 92, No. 4, p.41.

9 A 'public aircraft' is defined in 14 CFR 1.1, and specifically excludes aircraft operated for a commercial purpose. It includes, however, federal, state and local government agencies, the Department of Defense, the military, state universities, etc. See 14 CFR 1.1 [online] http://www.law.cornell.edu/cfr/text/14/1.1.

10 For a discussion of FAA policy on allowing UAS to be operated, see, e.g., Dept. of Transportation, Fed. Aviation Admin., *Unmanned Aircraft Operations in the National Airspace System*, Notice of Policy (February 6, 2007) [online] http://www.faa.gov/about/initiatives/uas/reg/media/frnotice_uas.pdf.

11 Model aircraft may not be flown more than 400 feet over the surface, and if flying within 3 miles of an airport, the model aircraft hobbyist must notify the airport operator, or if there is an air traffic facility, the control tower or flight service station. US Dept. of Transportation, Federal Aviation Admin., Advisory Circular (AC) 91-57 (Model Aircraft Operating Standards) June 9, 1981, para. 3(c) [online] http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf.

12 Fed. Aviation Admin. February 6, 2007 notice of policy, *op cit*., fn 8.

13 See Dept. of Transportation, Fed. Aviation Admin., Unmanned Aircraft Systems Operations in the US National Airspace System – Interim Operational Approval Guidance 08-01 (March 13, 2008) [online] http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/faq/media/uas_guidance08-01.pdf.

14 See, e.g., US Dept. of Transportation, Fed. Aviation Admin., *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, 1st ed., November 7, 2013, Appendix C, para. C. 7 at 60.

15 US Dept. of Transportation, Fed. Aviation Admin. [4910-13], *Unmanned Aircraft System Test Site Program: Notice of availability of final privacy requirements for the unmanned aircraft system ('UAS') test site program; response to comments*,

16 *Id*., Art. 3(a)(i)–(ii), at p.13.

17 *Id*., Art. 3(b)–(c), at p.14.

18 *Id*., Art. 3(e)(ii) at p.15.

19 See, e.g., Streitfeld, D. (2013) 'Amazon delivers some pie in the sky', *The New York Times*, 2 December 2013.

20 See Eur. RPAS Steering Grp. (ERSG), Final Report, *op. cit.* fn. 4, para. 4.1 at p.21.

21 Regulation (EC) No. 216/2008 of the European Parliament and of the Council of 20 February 2008 on Common Rules in the Field of Civil Aviation and Establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No. 1592/2002 and Directive 2004/36/EC, 2008 O.J. (L 79) 1 (EC) (March 19, 2008) [hereinafter Basic Regulation], Art. 1(2) at p.5.

22 Arrêté du 1 août 2007 relatif aux conditions d'insertion et d'évolution dans l'espace aérien des aéronefs civils ou de la défense non habités [Order of August 1, 2007 Relating to the Conditions for the Integration and Development in the Airspace of Unmanned Civil or Defense Aircraft], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], August 18, 2007, p.13817.

23 See Asencio, M. (2008) *L'utilisation civile des drones – problèmes techniques, opérationnels et juridiques* [The Civil Use of Drones – Technical, Operational and Legal Problems], NOTE DE LA FONDATION POUR LA RECHERCHE STRATÉGIQUE, No. 08/2008 (March 28, 2008), at p.5.

24 Arrêté du 21 décembre 2009 relatif aux conditions d'insertion et d'évolution dans l'espace aérien des aéronefs civils ou de la défense non habités [Order of December 21, 2009 on the Conditions for the Integration and Development in the Airspace of Unmanned Civil or Defense Aircraft], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], January 12, 2010, p.600.

25 Order of Apr. 11, 2012, *op cit*. fn 6.

26 Finn, P. (2011) *Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate*, The Washington Post (January 23, 2011) [online] http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html (accessed 10 December 2013).

27 Charles Carrasco, *Au Bourget 2013, les drones sont partout* [Drones Are Everywhere at the 2013 Paris Air Show] [online] http://www.europe1.fr (accessed 7 June 2013).

28 Alonso, P. (2013) *Drones à tout faire,* SLATE.FR (February 5, 2013) [online] http://www.slate.fr/print/story/67989/drones.

29 France 24, *Quand le 'drone journalism' atterit dans les redactions françaises*, (June 9, 2013) [online] http://www.france24.com/fr/print/4703787?print=now. Drones have been used to film, among other locations, inside the Château de Vincenne's walls, in the Paris night spot the 'Bains Douches', and their use was planned for the Tour de France bicycle race. See also, *Tour de France – Drôles de drones au-dessus des têtes*, LA NOUVELLE RÉPUBLIQUE.FR (July 10, 2013) [online] http://www.lanouvellerepublique.fr/Indre-et-Loire/Loisirs/Sports-et-loisirs/n/Contenu..., for a discussion of the use of drones for television images during the Tour de France.

30 See Charles Carrasco, *op cit.*, fn. 28.

31 See Marseille, A. (2013) *des drones contre la drogue* [In Marseilles, Drones against Drugs] [online] http://www.latribune.fr (accessed 20 September 2013). See also, Bindler, M-A. and Chevance, N. (2013) *Marseille: des drones pour lutter contre l'insécurité? [Marseilles: Drones to Fight against Insecurity?]* [online] http://www.europe1.fr (accessed 19 September 2013).

32 One academic affirms as much. See Goussard, L. (2013) *La Rationalisation dans tous ses états: Usages du concept et débats en sciences sociales [Rationalization in All Its States: Uses of the Concept and Debates in the Social Sciences]*, p.214.

33 Dufresne, S. (2008) *Drones: révélations sur les projets de la police [Revelations about Police Plans for Drones]* [online] http://www.mediapart.fr (accessed 15 April 2008) [online] http://www.mediapart.fr./journal/france/150408/drones-revelations-sur-les-projets-de-la-police.

34 See *Article 29 Working Party*, European Commission [online] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm. The guidance may also be referred to by practitioners to anticipate member state application of the Directive to new issues, such as those raised by data processing for new uses or using new technologies.

35 Art. 29 Data Prot. Working Party, Opinion 3/2012 on Developments in Biometric Technologies (April 27, 2012), (WP 193), p.23 [online] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

36 Speaking of drones, one journalist said, "[s]uch technology could allow police to record the activities of the public below with high-resolution, infrared and themal-imaging cameras." *Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate, op cit.* fn. 27.

37 United Nations, The Universal Declaration of Human Rights (December 10, 1948) [online] http://www.un.org/en/documents/udhr/.

38 See http://ec.europa.eu/enterprise/sectors/aerospace/uas/.

39 European RPAS Steering Group, *Annex 3: A Study on the Societal Impact of the Integration of Civil RPAS into the European Aviation System* (June 2013), pp.20–21 [online] http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap-annex-3_en.pdf.

40 Whitman, J.Q. (2004) 'The two western cultures of privacy: dignity versus liberty', *Yale L. J.*, April, Vol. 113, No. 1151, p.1155.

41 *Id*., at p.1161.

42 Whitman, *op cit.* fn. 41, at p.1215.

43 US Const. Amend. IV [online] http://www.law.cornell.edu/constitution/fourth_amendment.

44 See http://www.law.cornell.edu/wex/plain_view, for a description of 'plain view'. (For the anecdote, when this author consulted that page, an online behavioral advertisement placed there showed a Quadrirotor DJI Phantom RTF Drone, 'prêt à voler' [ready to fly]!)

45 Katz v. United States, 389 US 347 (1967) [online] http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html.

46 Smith v. Maryland, 442 US 735 (1979) [online] http://www.law.cornell.edu/supremecourt/text/442/735.

47 Ciraolo, *op cit*. fn. 46, at p.211.

48 Ciraolo, *op cit*. fn. 46, at p.211.

49 Oliver v. United States, 466 US 170 (1984) [online] http://www.law.cornell.edu/supct/html/historics/USSC_CR_0466_0170_ZO.html.

50 Ciraolo, *op cit*. fn. 46, at p.212, citing Oliver, *op cit.* fn. 14, at pp.181–183.

51 'Curtilage' may be defined as "a piece of ground (as a yard or courtyard) within the fence surrounding a house". http://www.merriam-webster.com/dictionary/curtilage (accessed 4 October 2013). It is an area "to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life.'" Thus, it is an area where expectations of privacy are 'heightened'. Ciraolo, *op cit*. fn. 46, at pp.212–213.

52 *Id*., at pp.213–214.

53 Florida v. Riley, 488 US 445 (1989) [online] http://www.law.cornell.edu/supremecourt/text/488/445.

54 *Id*., at p.449–450.

55 *Id*., at p.451.

56 *Id*., at pp.451–452.

57 Dow Chemical Company v. United States, 476 US 227 (1986) [online] http://www.law.cornell.edu/supremecourt/text/476/227.

58 See Oliver, *op cit.* fn. 50, generally, for a discussion of the 'open fields' doctrine, where police officers may enter and search an open field without a warrant, given that there is not a reasonable expectation of privacy there.

59 Dow Chemical Co., *op cit*. fn. 58, at p.239.

60 "American privacy protections, at their metaphoric core, are the sorts of protections afforded by the walls of one's home. They have been extended beyond the literal home, of course, since the eighteenth century. Nevertheless, it remains the case that American protections become progressively weaker the further the affected person is from home." Whitman, *op cit*. fn. 41, at p.1194.

61 *Id*., at p.238.

62 In the dissenting opinion of Justices Brennan, Marshall and Stevens, this point is raised: "What, one wonders, is meant by 'intimate details'? If the police had observed Riley embracing his wife in the backyard greenhouse, would we then say that his reasonable expectation of privacy had been infringed? Where in the Fourth Amendment or in our cases is there any warrant for imposing a requirement that the activity observed must be 'intimate' in order to be protected by the Constitution?" Florida v. Riley, *op cit*., fn. 54, at p.463.

63 Kyllo v. United States, 533 US 33 (2001) [online] http://www.law.cornell.edu/supct/pdf/99-8508P.ZO.

64 In response to the dissent, Justice Scalia, writing for the Court, stated: "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," [citation omitted] constitutes a search – at least where (as here) the technology in question is not in general public use.", 533 US 33, at __.

65 See, e.g., Calo, M.R. (2011) 'The drone as privacy catalyst', *Stan. L. Rev. Online*, 12 December, Vol. 64, No. 29, p.31: "Neither the Constitution nor common law appears to prohibit police or the media from routinely operating surveillance drones in urban and other environments." (Citation omitted.). While agreeing that "drone aerial surveillance of open fields would not violate the Fourth Amendment anymore than surveillance of public highways and other public spaces", and that this could also be the case for the curtilage area for short periods of time from NAS where the surveillance does not create nuisances such as noise, wind, etc., one scholar posits that the condition will be different in the case of a hummingbird-size drone inside someone's home. See Molko, R. (2012) *The Drones Are Coming! Will the Fourth Amendment Stop their Threat to our Privacy?*, September, pp.29–34 [online] http://works.bepress.com/robert_molko/1.

66 See http://www.fbi.gov/about-us/cjis/ncic.

67 5 U.S.C. §552a (1974).

68 *Id*., para. (b).

69 *Id*., para. (c).

70 *Id*., para. (d)(1).

71 *Id*., para. (d)(2).

72 *Id*., para. (e).

73 *Id*., para. (g) and (i).

74 *Id*., para. (k)(2).

75 Notice, FBI, DOJ, Privacy Act of 1974; System of Records, 66 Fed. Reg. 33,558, 33,559 (June 22, 2001).

76 For a list of the 47 member states of the Council of Europe as well as http://hub.coe.int/.

77 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 28, 1981, CETS, No. 108 (Convention 108), Art. 1 [online] http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

78 *Id*., Arts. 5–8.

79 *Id*., Art. 9(2)(a).

80 *Id*., Art. 7.

81 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, CETS, No. 005 (ECHR) [online] http://www.conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

82 *Id*., Art. 8.

83 See, e.g., Privacy International, *Report: Legal Assessment of Communications Data Retention – A Violation of the European Convention of Human Rights* (September 9, 2003), 'Chapter: the right of privacy in the European convention on human rights' [online] https://www.privacyinternational.org/reports/data-retention-violates-human-rights-convention/the-right-of-privacy-in-the-european.

84 Uzun v. Germany, App. No. 35623/05 (September 2, 2010)

85 *Id*., p.33.

86 *Id*., p.52.

87 *Id*., p.64.

88 *Id*., pp.69–72.

89 *Id*., pp.77–81.

90 Eur. RPAS Steering Grp. (ERSG), Final Report, *op cit*. fn. 4, para. 4.1 at p.22.

91 See Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter DP Directive].

92 See DP Directive, Art. 3(2) at p.39.

93 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 2008 O.J. (L 350) 60 (December 30, 2008) [online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF.

94 *Id*., Art. 1(1) at p.64.

95 *Id*.., Art 1(2) at p.64.

96 Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. (C 115) 47 (EU) [hereinafter TFEU], Art. 16(1) at p.55.

97 *Id*., Art. 16(2) at p.55.

98 Consolidated Version of the Treaty on European Union, 2012 O.J. (C 326) 13 (October 26, 2012) [hereinafter TEU], Art. 39 at p.36.

99 *Id*., Art. 6(1) at p.19.

100 Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 01 (December 18, 2000) [hereinafter Charter], Art. 7 at p.10.

101 *Id*., Art. 8(1) at p.10.

102 *Id*., Art 8(2) at p.10.

103 *Id*., Art. 52(1).

104 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (January 25, 2012) [hereinafter GDPR] [online] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

105 *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012) [hereinafter Justice DP Directive] [online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

106 See GDPR., Art. 2(a) and (c).

107 *Id*., Art. 2(e) at p.40.

108 See Justice DP Directive, Art. 2(a)–(b) at p.26.

109 *Id*., Art. 3(a).

110 See *id*., Art. 4 at p.28.

111 *Id*., Arts. 11, 12, 15 and 16 at pp.30–34.

112 *Id*., Art. 17 at p.34.

113 *Id. "Dès lors qu'il est équipé d'un appareil photo, d'une caméra mobile, d'un capteur sonore ou encore d'un dispositif de géolocalisation, un drone peut donc potentiellement porter atteinte à la vie privée, capter et diffuser des données personnelles. … la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi Informatique et Libertés" Note: the law referred to here is Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* [Law 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties], J.O., January 7, 1978, p.227 (Fr.), as amended [online] http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (English translation).

114 *Id*., Art. 7(3) at p.9.

115 Commission nationale de l'informatique et des libertés [CNIL] [National Commission for Data Protection Authority], *Usages des drones et protection des données personnelles [The Use of Drones and the Protection of Personal Data]* (October 30, 2012) (Fr.) [online] http://www.cnil.fr/linstitution/actualite/article/article/usages-des-drones-et-protection-des-donnees-personnelles/.

116 See https://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states (last updated October 9, 2013) (last consulted on December 10, 2013).

117 See http://laws.flrules.org/2013/33.

118 See http://flsenate.gov/Session/Bill/2013/0092/.

119 See http://www.legislature.idaho.gov/legislation/2013/S1134.pdf.

120 See http://www.ilga.gov/legislation/publicacts/98/PDF/098-0569.pdf.

121 See http://data.opi.mt.gov/bills/2013/billpdf/SB0196.pdf.

122 See https://olis.leg.state.or.us/liz/2013R1/Measures/Text/HB2710/Enrolled.

123 See http://state.tn.us/sos/acts/108/pub/pc0470.pdf.

124 See http://www.legis.state.tx.us/tlodocs/83R/billtext/pdf/HB00912F.pdf.

125 See http://leg1.state.va.us/cgi-bin/legp504.exe?131+ful+CHAP0755+pdf.

126 See Silversmith, J.A. (2013) 'You can't regulate this: state regulation of the private use of unmanned aircraft', *26 The Air & Space Lawyer*, Vol. 1, No. 3, p.23.

127 http://www.ncsl.org/research/civil-and-criminal-justice/unmanned-aerial-vehicles.aspx.

128 North Carolina Senate Bill 402, Sec. 7.16(e), at p.41 [online] http://www.ncga.state.nc.us/Sessions/2013/Bills/Senate/PDF/S402v7.pdf.

129 See, e.g., http://www.ncsl.org/documents/summit/summit2013/online-resources/dronefederallegislation.pdf.

130 See http://thomas.loc.gov/cgi-bin/bdquery/z?d113:s.01016.

131 See http://thomas.loc.gov/cgi-bin/bdquery/z?d113:s.01057.

132 See *The Drone as a Privacy Catalyst, op cit*., fn. 66.

133 *Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate, op cit*. fn. 22.

134 *Id*.

135 See Mazzetti, M. and Schmidt, M.S. (2013) *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013) [online] http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?pagewanted=all&_r=0.

136 Robert Molko *op cit*., fn. 66.

137 Crump, C. (2013) *Capability is Driving Policy, Not Just at the NSA but also in Police Departments*, American Civil Liberties Union (November 1, 2013) [online] https://www.aclu.org/blog/technology-and-liberty-national-security/capability-driving-policy-not-just-nsa-also-police.

138 For a discussion of mission creep and purpose limitation, see Art. 29 Data Prot. Working Party, Opinion 3/2013 on Purpose Limitation (April 2, 2013), (WP 203), p.4 [online] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.