Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications

Rachel L. Finn, David Wright

Trilateral Research & Consulting, London, UK

Keywords:
Unmanned aircraft systems
Privacy
Surveillance
Law and policy

ABSTRACT

This paper examines how the use of unmanned aircraft systems (UASs) for surveillance in civil applications impacts upon privacy and other civil liberties. It argues that, despite the heterogeneity of these systems, the same "usual suspects" – the poor, people of colour and anti-government protesters – are targeted by UAS deployments. It discusses how current privacy-related legislation in the US, UK and European Union might apply to UASs. We find that current regulatory mechanisms do not adequately address privacy and civil liberties concerns because UASs are complex, multimodal surveillance systems that integrate a range of technologies and capabilities. The paper argues for a combination of top-down, legislated requirements and bottom-up impact assessments to adequately address privacy and civil liberties.

1. Introduction

Unmanned aerial vehicles (UAVs) can generally be defined as a "device used or intended to be used for flight in the air that has no on-board pilot".[1] These devices are sometimes referred to as "drones", which are programmed for autonomous flight, and remotely piloted vehicles (RPVs), which are flown remotely by a ground control operator.[2] Current generations of UAVs "can be as small as an insect or as large as a charter flight".[3] They are often launched from a road or a small vehicle, and large enough to accommodate cameras, sensors or other information gathering equipment.[4] Recently, discussions of UAVs have used the term unmanned aircraft systems (UASs) to reflect "the fact that in addition to the unmanned aircraft, a complete UAS includes multiple pieces of ancillary equipment, such as vehicle control equipment, communications systems, and potentially even launch and recovery platforms".[5] According to McBride, the versatility of these "systems" is one of the strongest drivers in the rapid development of these technologies, where "the identification of new potential uses leads to the adaptation of the systems".[6] One such use is the deployment of UASs with cameras or sensors in law enforcement applications, which has led the Surveillance Studies Network, in its testimony to the UK

[1] Quoted from Aviation Safety Unmanned Aircraft Programme Office, 2008, in McBride Paul. Beyond Orwell: the application of unmanned aircraft systems in domestic surveillance operations. Journal of Air Law and Commerce Summer 2009;74(3):627–62, 628.

[2] Bolkcom Christopher. Homeland security: unmanned aerial vehicles and border surveillance. Congressional research service report for Congress; 28 June 2004.

[3] Eick Volker. The droning of the drones: the increasingly advanced technology of surveillance and control. Statewatch analysis, no. 106; 2009. p. 1. http://www.statewatch.org/analyses/no-106-the-droning-of-drones.pdf.

[4] McCormack Edward D. The use of small unmanned aircraft by the Washington State Department of Transportation. Washington State Transportation Center; June 2008.

[5] McBride, op. cit., 2009. p. 629. See also Directorate of Airspace Policy. CAP 722: Unmanned aircraft system operations in UK airspace – guidance. Civil Aviation Authority; 6 Apr 2010.

[6] McBride, op. cit., 2009. p. 629.

0267-3649/$ – see front matter © 2012 Rachel L. Finn and David Wright. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.01.005

House of Lords, to assert that UAVs represent one of the technological forms that characterise "new surveillance".[7]

Despite recent growth in the UAV/UAS market, UAVs have a relatively long history. The first unmanned aircraft was a torpedo developed in 1915 for the US Navy, which was designed to fly to a specific location and drive into its target.[8] In the Second World War, they were used as radio-controlled targets and for reconnaissance missions.[9] In the 1990s, the Defense Advanced Research Projects Agency (DARPA) and NASA began research into further uses of UAVs, and a number of well-known UAVs such as the Helios, Proteus, Altus Pathfinder and Predator (which was first used by the US in the Gulf War) resulted from this effort.[10] Drones were so effective in the Gulf War that "Iraqi troops began to associate the sound of the little aircraft's two-cycle engine with an imminent devastating bombardment", which led to "the first instance of human soldiers surrendering to a robot".[11] Growth in this area has recently increased exponentially, particularly because of developments in lightweight construction materials, microelectronics, signal processing equipment and GPS navigation.[12] More than 50 nations currently use drones for military reconnaissance, intelligence-gathering and targeting[13] and as of 2003 at least three dozen nations had active UAV development or application programmes.[14] However, the civil market for UASs is the largest area of predicted sector growth in the next few years. For example, the UK Civil Aviation Authority has stated that model aircraft have been flying successfully for years "performing aerial work tasks, effectively operating as UAVs".[15] Furthermore, a worldwide survey of existing UASs in 2004 found that 79 per cent are aimed at civil research or dual-purpose operations and that this is likely to continue.[16] This emerging civil market includes potential applications such as public security, law enforcement, border patrol, emergency services and commercial services.[17]

This paper examines how the use of UASs for surveillance in civil applications impacts upon privacy and other civil liberties. It argues that, despite the heterogeneity of these systems, the same "usual suspects" are targeted by deployments of UASs. It discusses how current legislation mechanisms might apply to UASs, with specific attention to privacy-related legislation in the USA, European Union and UK. It finds that current regulatory mechanisms do not adequately address privacy and civil liberties concerns because UASs are complex, multimodal surveillance systems that integrate a range of technologies and capabilities. Furthermore, the inadequacy of current legislation mechanisms results in disproportionate impacts on civil liberties for already marginalised populations.

2. Surveillance and civil liberties

Much critique surrounding the introduction of surveillance technologies such as UASs, or their expansion from military to civil applications, has centred on civil liberties concerns. Privacy represents a key framework through which surveillance technologies, and particularly "new surveillance"[18] technologies, are critiqued,[19] although scholars have had difficulty in agreeing on a precise conceptualisation. Whitman described privacy, important though it may be, as "an unusually slippery concept",[20] while Solove, more recently, has said that privacy "is a concept in disarray. Nobody can articulate what it means."[21] Although a widely accepted definition of privacy remains elusive, there has been rather more consensus on a recognition that privacy comprises multiple dimensions, which privacy guru Roger Clarke specified as privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication.[22] Similarly, Solove asserts that privacy is best understood as a "family of different yet related things".[23] One aspect of this family is data protection, where some law-makers have attempted to use data protection legislation to mitigate concerns around the effects of surveillance. However, Lyon argues that data protection is difficult to connect to a basic

[7] House of Lords Select Committee on the Constitution. Surveillance: citizens and the state, vol. 2. HL paper 18, second report, session 2008–09. London: House of Lords; 6 Feb 09.

[8] Dunlap Travis. Comment: we've got our eyes on you: when surveillance by unmanned aircraft systems constitutes a Fourth amendment search. South Texas Law Review Fall 2009;51(1): 173–204.

[9] The Economist. Unmanned aircraft: the fly's a spy. 1 Nov 2007. http://www.economist.com/displaystory.cfm?story_id=10059596.

[10] Nonami Kenzo. Prospect and recent research and development for civil use autonomous unmanned aircraft as UAV and MAV. Journal of Systems Design and Dynamics 2007;1(2):120–8.

[11] Wilson JR. UAVs: a worldwide roundup. Aerospace America June 2003. https://www.aiaa.org/aerospace/Article.cfm?issuetocid=365&ArchiveIssueID=39.

[12] The Economist, op. cit., 2007.

[13] Strategic Comments. The drones of war. 2009;15(4):1–2.

[14] Wilson, op. cit., 2003.

[15] Haddon DR, Whittaker CJ. UK-CAA policy for light UAV systems. UK Civil Aviation Authority; 28 May 2004. p. 2.

[16] Ibid.

[17] FH Joanneum University of Applied Sciences. Unmanned aircraft systems – towards civil applications. Graz, Austria; 10 Nov 2009. http://www.fh-joanneum.at/aw/home/Studienangebot_Uebersicht/fachbereich_information_design_technologien/lav/news_events_ordner_lav/Archiv/~btch/lav_news_091110/?lan=de.

[18] According to Gary Marx, "new surveillance" is characterised by new forms of technology, gathering information from categories of interest rather than specific persons, an increase in the amount of data collected, remote operation, less coercive data collection, a routinisation of surveillance and can involve multiple measures in combination. See Marx Gary T. What's new about the new surveillance?: classifying for change and continuity. Surveillance & Society 2002;1(1):9–29.

[19] Lyon David. Surveillance after September 11. Cambridge: Polity Press; 2003.

[20] Whitman James Q. The two western cultures of privacy: dignity versus liberty. The Yale Law Journal 2004;113:1151–221, 1153–4.

[21] Solove Daniel J. Understanding privacy. Cambridge MA and London: Harvard University Press; 2008. p. 12.

[22] Clarke Roger. What's 'privacy'? Australian Law Reform Commission workshop; 28 July 2006. http://www.rogerclarke.com/DV/Privacy.html.

[23] Solove, op. cit., 2008. p. 9.

human right, and thus is problematic as an over-arching civil liberties protection framework.[24]

Lyon argues that privacy is also inadequate to capture all of the negative effects of surveillance, since other civil liberties concerns, in addition to privacy, are implicated in new technologies of surveillance.[25] For example, the use of surveillance technologies may inhibit individuals' freedom of assembly or freedom of expression due to a "chilling effect" that discourages individual participation in social movements or public dissent activities.[26] In relation to profiling via data mining, Schreurs et al. discuss a right of non-discrimination within the framework of the European Convention on Human Rights.[27] Such potential for discrimination is particularly important; Coleman and McCahill argue that the use of surveillance technologies often reinforces existing social positions, particularly positions of marginalisation along the lines of race, class, gender, sexuality and age.[28] Surveillance technologies may impinge upon individuals' freedom of movement, in a clear example of Lyon's notion of social sorting. Such linkages between social position and movement are noted by Graham and Wood[29] and Finn and McCahill[30], where digitalised surveillance systems enable a privileged mobility for some individuals (e.g., the use of iris scanning systems to bypass immigration queues) while marginalised individuals find their mobility further restricted (for example, by false positive matches with individuals on "no fly" lists, or where individuals who refuse body scans at airports are prevented from flying[31]). This restriction on freedom of movement can disproportionately impact some groups of already marginalised travellers, such as Muslim women, for whom religious restrictions on modesty prevent participation in body scanning systems.[32] In addition to these civil liberties concerns around the negative effects on individuals, Lyon reminds us that, via the International Treaty on Human Rights, individuals also have a right to security.[33]

Yet, different surveillance technologies with different capabilities often require different regulatory mechanisms to minimise their impacts on civil liberties. For example, the European Parliament is considering issuing recommendations on body scanners that include provision of an alternative to body scanning technology, and Langheinrich has recommended that RFID applications should protect personal information through privacy enhancing technologies such as encryption.[34] The deployment and use of CCTV systems in public spaces are guided by codes of practice and legislation such as the UK Data Protection Act or the European Data Protection Directive 95/46/EC, while communication interceptions such as wiretapping often require a warrant signed by a judge or some other supervisory authority. The fact that the capabilities and applications of UAS devices vary so much depending upon the technologies they integrate makes it difficult to establish over-arching regulatory mechanisms to prevent intrusion on civil liberties.

3. Capabilities and applications

The expanding capabilities of UAS devices mean that they have already been used, or are currently being used, for various civil applications. Furthermore, as these capabilities are further augmented and differentiated, experts envision that UASs will be used for still more applications. However, the intersection of these capabilities and applications in deployments against individuals for law enforcement or other security-related activities means that already marginalised populations are disproportionately targeted.

3.1. *Current and future capabilities*

UASs have a range of capabilities making them useful not only for military applications, but also the bourgeoning field of civil applications. Specifically, UASs have a "niche" in performing the three Ds: dull, dirty and dangerous work, thereby protecting human pilots from fatigue and various environmental hazards. Brecher identifies the following general capabilities for unmanned aircraft systems:

- They can be deployed on demand.
- They have flexibility in tasking: e.g., surveillance, disasters, etc.
- They have "plug and play" capabilities for their payloads, making tailored systems possible.

[24] Lyon David. Facing the future: seeking ethics for everyday surveillance. Ethics and Information Technology 2001;3:171–81.

[25] Lyon, op. cit., 2001. Raab and Wright make a similar point: "Data protection principles are an essential bedrock, but they do not fully address the range of questions that should be asked about surveillance, especially the 'new surveillance' brought about through new technologies and information systems." Raab Charles, Wright David. Surveillance: extending the limits of privacy impact assessment. In: Wright David, De Hert Paul, editors. Privacy impact assessment. Dordrecht: Springer; 2012.

[26] Cunningham David, Noakes John. What if she's from the FBI? The effects of covert forms of social control on social movements. In: Deflem Mathieu, editor. Surveillance and governance: crime control and beyond. Bingley, UK: Emerald Group Publishing Limited; 2008 and Lyon, op. cit., 2003.

[27] Schreurs Wim, Hildebrandt Mireille, Kindt Els, Vanfleteren Michaël. *Cogitas, ergo sum*. The role of data protection law and non-discrimination law in group profiling in the private sector. In: Hildebrandt Mireille, Gutwirth Serge, editors. Profiling the European citizen: cross-disciplinary perspectives. London: Springer; 2008.

[28] Coleman Roy, McCahill Michael. Surveillance and crime. London: Sage; 2011.

[29] Graham Stephen, Wood David. Digitizing surveillance: categorization, space, inequality. Critical Social Policy May 2003;23(2): 227–48.

[30] Finn Rachel L, McCahill Michael. 'Good' and 'bad' data subjects: media representations of the 'surveilled' in three UK newspapers. In: Leman-Langlois Stéphane, editor. Technocrime2. London: Routledge; 2012, forthcoming.

[31] Klitou Demetrius. Backscatter body scanners – a strip search by other means. Computer Law & Security Report 2008;24(4): 316–25, 317.

[32] Peterson Rohen. The emperor's new scanner: Muslim women at the intersection of the first amendment and full body scanners. Social Science Research Network 6 Mar 2010. http://ssrn.com/abstract=1684246.

[33] Lyon, op. cit., 2003.

[34] Langheinrich Marc. A survey of RFID privacy approaches. Personal and Ubiquitous Computing 2009;13(6):413–21.

- They can support high-resolution imagery or sensors.
- They can cover remote areas.[35]

Ollero et al. note that UASs are heterogeneous and can support the high manoeuvrability and hovering capabilities of helicopters as well as the global views and communications relay capabilities of airships.[36] In addition to these general capabilities, UASs have more specific capabilities in relation to the way they are piloted, their size, flying speed and endurance as well as the technologies they integrate.

Most large UAS are remotely piloted. In current combat operations in Iraq and Afghanistan, large UASs are "controlled by pilots working in shifts and sitting in front of a video screen thousands of miles away at an air force base in America"[37] "from a console with twin video screens shaped to resemble a plane's cockpit"[38]. BAE's HERTI can be programmed to take off, complete a full mission and land automatically.[39] Some smaller models can be carried and deployed by individuals on the ground and flown via remote control. One UAS made by AirRobot can be flown even when out of sight because it beams images from the aircraft back to video goggles worn by the operator.[40] Furthermore, not all UASs require a specially trained "pilot". Interested individuals can build a basic UAV for approximately $1000 USD using Legos, a GPS unit and model aircraft parts.[41] Individuals in Germany can reportedly rent drones for €190 per hour.[42] In terms of future developments related to flying capabilities, manufacturers are working on making UASs more autonomous as well as trying to programme swarms of vehicles that can co-operate with one another.[43] The development of "sense and avoid systems", which many researchers are exploring, will transform UAS technology and allow the devices to be deployed in a range of applications, potentially leading to their wide deployment.[44]

UASs being used in the civil sector have specific capabilities regarding their size, flying speed and endurance. General Atomics' MQ-1 Predator Bs can fly between 20 and 30 h, are 36 feet (11 m) long, have a wing span of 66 feet (26.1 m), weigh 1500 pounds (680 kg), and are powered by 900 horsepower turboprop engines.[45] These large UAVs can cost $4.5 million USD, with the accompanying ground equipment running another $3.5 million. Significantly smaller UASs have fewer capabilities. The Insitu Insight has "a 10 foot [3.05 m] wing span, a maximum altitude of 19,500 feet [5944 m], and a flight endurance of more than 20 h",[46] and Honeywell Micro Air Vehicles weigh 14 pounds (6.35 kg) and have a maximum altitude of 10,500 feet (3200 m). The SkySeer, manufactured by Octatron Inc., has a wing span of 6.5 feet (1.98 m) and weighs 4 pounds (1.8 kg). This Micro-drone which flies at 30 mph (48 kph) is significantly more cost efficient at $25,000 to $30,000 USD. The CannaChopper SUAVE 7, which weighs 7 kg and can fly up to 2 h depending on payload and fuel load, fits into the trunk of a car and can be transported easily.[47] The German AirRobot, a helicopter type UAV, measures 3 feet (.91 m) between the tips of its four carbon fibre rotor blades, and a battery-operated drone manufactured by MW Power, is 70 cm-wide and can fly up to 500 m high.[48] Both the SkySeer and the AirRobot can transmit data to a ground station, enabling an operator to see what the UAS is seeing, in real time and, if necessary, direct officers on the ground.[49] One of the main advantages of UASs is that they are almost undetectable to the person(s) or target(s) being surveilled. The OPARUS project, financed by the European Commission, states that a UAS can operate "almost in silence".[50] Similarly, BAE drones' flight ceiling of 20,000 feet (6096 m) makes them almost invisible from the ground.[51] In terms of future developments in these capabilities, the first revolves around developments in the size and shape of UAVs, or unmanned vehicles (as the case may be). These include the miniaturisation of UAVs to insect-sized surveillance vehicles that could fly through open windows,[52] which is being worked on by the Air Force Research Lab, Onera (France's national aerospace centre), Harvard University and the University of Portsmouth in the UK.[53] Another innovation is a "snake bot": an unmanned vehicle can be fitted with cameras or audio sensors and "slither undetected through grass and raise its head to look around, or even climb a tree for a better view".[54]

[35] Brecher Aviva. Roadmap to near-term deployment of unmanned aerial vehicles (UAV) for transportation applications charge to participants. UAV 2003: roadmap for deploying UAVs in transportation specialist workshop. Santa Barbara, CA; 2 Dec 2003.

[36] Ollero Aníbal, Lacroix Simon, Merino Luis, et al. Multiple eyes in the skies: architecture and perception issues in the COMETS unmanned air vehicles project. IEEE Robotics & Automation Magazine June 2005:46–57.

[37] The Economist, op. cit., 2007.

[38] Bowcott Owen, Lewis Paul. Attack of the drones. The Guardian 16 Jan 2011. http://www.guardian.co.uk/uk/2011/jan/16/drones-unmanned-aircraft.

[39] Page Lewis. BAE in South Coast mouse-click drone spy plan: there'll be ro-birds over the white cliffs of Dover. The Register 8 Nov 2007. http://www.theregister.co.uk/2007/11/08/bae_mouse_click_robot_spy_dover_over/.

[40] Randerson James. Eye in the sky: police use drone to spy on V festival. The Guardian 21 Aug 2007. http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews.

[41] The Economist, op. cit., 2007.

[42] Eick, op. cit., 2009.

[43] Bowcott and Lewis, op. cit., 2011.

[44] Eick, op. cit., 2009.

[45] Matthews William. Border patrol at 19,000 feet: UAVs take flight along Texas border – during daylight. Defense News 14 June 2010. http://www.defensenews.com/story.php?i=4668081.

[46] Dunlap, op. cit., 2009. p. 180–1.

[47] Cannachopper. Suave 7. 2009. http://www.cannachopper.com/helicopters/47-suave7.

[48] Randerson, op. cit., 2007.

[49] Bowes Peter. High hopes for drone in LA skies. BBC News 6 June 2006. http://news.bbc.co.uk/1/hi/world/americas/5051142.stm and Hull Liz. Drone makes first UK 'arrest' as police catch car thief hiding under bushes. Daily Mail 12 Feb 2010. http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N.

[50] OPARUS. Concept and approach; 2010. http://www.oparus.eu/index.php/concept-a-approach.

[51] Lewis Paul. CCTV in the sky: police plan to use military-style spy drones. The Guardian 23 Jan 2010. http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones.

[52] Nevins Joseph. Robocop: drones at home. Boston Review Jan/Feb 2011. http://www.bostonreview.net/BR36.1/nevins.php.

[53] The Economist, op. cit., 2007.

[54] Wired Magazine, quoted in Nevins, op. cit., 2011.

In terms of endurance, Nevins reports that research is being undertaken on a solar-powered UAV that could stay airborne for up to five years.

These drones can also incorporate attachments, which themselves have specific capabilities. For example, the Insitu Insight carries out surveillance through a camera attached to the underside of the vehicle, and can incorporate low-light and infrared cameras enabling officers to find heat signatures; however, carrying both cameras decreases the vehicle's endurance to 15 h.[55] The Honeywell MAV incorporates both a forward-looking and downward-looking video camera and is able to hover and continuously monitor a space. The MW Power drone can be fitted with high-resolution still cameras, colour video cameras and infrared night vision cameras. Even micro-drones, such as the SkySeer, can be fitted with video cameras, thermal imaging devices, radiation detectors, mobile-phone jammers and air sampling devices.[56] The cameras on these drones can be so powerful that UASs fitted with electro-optical sensors "can identify an object the size of a milk carton from an altitude of 60,000 feet [18,288 m]".[57] In the future, UASs may also incorporate lethal and non-lethal weapons. Discussing the police force's use of UASs for visual surveillance, an American sheriff in South Carolina stated "We do have the capability of putting a weapon on there if we needed to."[58] Other developments could include weapons such as combustible materials, incapacitating chemicals or explosives being integrated into UAV payloads,[59] or long range acoustic devices that send piercing sounds into crowds, high intensity strobe lights which can cause dizziness, disorientation and loss of balance, tasers that administer an electric shock[60] or tear gas and rubber rounds.[61] Other capabilities could include tagging targets with biological paints or micro-sensors that would enable individuals or vehicles to be tracked from afar.[62]

3.2. *Current and future applications*

UASs have been used, are being used or are actively being considered for different applications in North America, Europe and beyond. While UASs also have a range of potential environmental or commercial applications (emergency response, pollution detection, crop spraying, etc.), they can be deployed in surveillance applications against civilians, such as applications in policing and border surveillance. Like other surveillance devices, UASs often target the "usual suspects", including the poor, people of colour and anti-government protesters. Some police departments in Europe and North America (where data is most available) have been using UASs since 2006. At least five police forces in the UK (Essex, Merseyside, Staffordshire, Derbyshire and the British Transport police) have purchased or used micro-drones, and Los Angeles, Houston and Miami-Dade police (among others) have all used or are considering UASs. The range of potential applications is clear to police forces, where, for example, the "South Coast Partnership" between Kent Police and five other police forces in the UK is seeking to "introduce drones 'into the routine work of the police, border authorities and other government agencies' across the UK".[63]

Police forces use UASs to monitor large crowds, prevent or detect crime and assist in incident responses. UK police have used UASs to monitor festival-goers by "keep[ing] tabs on people thought to be acting suspiciously in car parks and to gather intelligence on individuals in the crowd",[64] to monitor protests at a right-wing festival[65] and to monitor the Olympic handover ceremony at Buckingham Palace.[66] In 2007, drones were reported over political rallies in New York and Washington, DC.[67] The CannaChopper has been deployed in the Netherlands and Switzerland against cannabis smokers, football fans at the European football championship in 2008 and "troublemakers" at the NATO summit in 2009.[68] India has also recently begun using UASs to help secure sensitive sites and events. A popular shrine that is often the target of "anti-social elements" and other security threats may get UAS surveillance.[69] Furthermore, UASs were reportedly given the "go-ahead" to assist Indian security forces in providing surveillance coverage of game venues and residential zones during the 2010 Commonwealth Games.[70]

In addition to large crowd monitoring, UASs have been used to monitor small groups or particular spaces to prevent or detect crime. The Merseyside police force in Liverpool has used two drones to police "public order" and "prevent anti-social behaviour". Police in Liverpool have flown a drone over groups of young people loitering in parks and used it for covert surveillance.[71] German police have been using drones to monitor "alleged hooligans" and urban areas, although Eick reports that Germany is relatively "behind" other western European countries in UAS deployment.

A North Carolina county is using UAVs with infrared cameras to monitor "gatherings of motorcycle riders" and to detect marijuana fields.[72] In this deployment, the UAV flies

[55] Bowes, op. cit., 2006.
[56] Bowcott Owen, Lewis Paul. Unmanned drones may be used in police surveillance. The Guardian 24 Sept 2010. http://www.guardian.co.uk/uk/2010/sep/24/police-unmanned-surveillance-drones.
[57] The Economist, op. cit., 2007.
[58] WLTX. A.I.R. (Ariel Intelligence and Response) to help law enforcement. 22 Mar 2011. http://www.wltx.com/news/article/129337/2/From-Toy-to-Life-Saving-Tool.
[59] Nevins, op. cit., 2011.
[60] Whitehead John W. Drones over America: tyranny at home. Charlottesville, VA: The Rutherford Institute; 28 June 2010. http://www.rutherford.org/articles_db/commentary.asp?record_id=661.
[61] Ibid.
[62] Nevins, op. cit., 2011 and Randerson, op. cit., 2007.
[63] Ibid.
[64] Randerson, op. cit., 2007.
[65] Hull, op. cit., 2010.
[66] AirRobot UK. AirRobot: the London 2012 Olympics handover ceremony at Buckingham Palace, AirRobot UK News 2008.
[67] Whitehead, op. cit., 2010.
[68] Eick, op. cit., 2009.
[69] IANS [Indo-Asian News Service]. Tirupati temple may get UAV surveillance. Deccan Herald 19 Oct 2010. http://www.deccanherald.com/content/105844/tirupati-temple-may-get-uav.html.
[70] Sarin Ritu. UAVs to provide real-time surveillance during games. Indian Express.com 22 Sept 2010. http://www.indianexpress.com/news/uavs-to-provide-realtime-surveillance-durin/685737/.
[71] Randerson, op. cit., 2007.
[72] McCullagh Declan. Drone aircraft may prowl U.S. skies. CNET News 29 March 2006. http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html#ixzz1JURmGB4a.

a few hundred feet in the air, which is close enough to identify faces.[73] Six police departments in Canada are using UASs in sparsely populated areas to record crime scenes,[74] and Canadian police are responsible for the first photographs taken by a UAV being admitted as evidence in court after the local police force used a UAV to photograph a homicide scene in 2007.[75] The "South Coast Partnership" mentioned above is seeking to use UASs for maritime surveillance as well as a range of other police issues including surveillance at the 2012 Olympic Games in London.[76] Belgium, France and Italy have used UASs to monitor "undocumented workers, undocumented migrants and demonstrators".[77]

UASs may also be used to assist police in incident response. Merseyside police are credited with the first UK arrest using a drone, where a car thief was tracked through undergrowth by the UASs' thermal imaging camera.[78] Once the teenage suspect's location was detected by the AirRobot flying at 150 feet (45.7 m), the information was relayed to ground forces who arrested the youth.[79] The Netherlands have also used UAVs to "support police in the eviction of a squat"[80]. In Los Angeles, a sheriff's department deployed their SkySeer drone to seek missing persons in rural areas, monitor accident or crime scenes and assist police in pursuits.[81]

UASs have been used in border surveillance operations in the USA since 2002. The US is one of the most well documented users of UASs in this capacity along the US–Mexico border and the US–Canada border. In 2002, a US Marine-operated Pioneer UAV intercepted people who were attempting to smuggle 45 kg of marijuana from Canada into the US.[82] In 2004–2005, UASs were deployed in routine operations along the US–Mexico border. The success of these systems is evidenced by one Predator UAV flying 886 h and assisting officers to capture 2300 undocumented immigrants as well as 3760 kg of marijuana in its first seven months.[83] In 2005, Predator UAVs along Arizona's border with Mexico were integrated into a surveillance system that included seismic sensors, infrared cameras and laser illuminators. If the seismic sensor is triggered by drug smugglers, "the Predator can investigate and, upon finding drug smugglers, tag them with its laser illuminator. With the GPS coordinates and the infrared illuminator, agents have no difficulty intercepting the smugglers".[84] Canadian authorities have also used UASs to patrol smuggling corridors along their border with the USA.[85] Austria also uses UAVs to monitor its borders[86] and Frontex, the European border agency, has held UAV demonstrations, while the UK envisions using UAS for maritime border surveillance.[87]

In the development of new applications, UASs could be used for a variety of new policing functions. Drones could be used for safety inspections, perimeter patrols around prisons and thermal imaging to check for cannabis being grown in roof lofts.[88] The police could use them to capture number plates of speeding drivers.[89] The UK newspaper, *The Guardian*, has identified other deployments including "[detecting] theft from cash machines, preventing theft of tractors…railway monitoring, search and rescue… [and] to combat fly-posting, fly-tipping, abandoned vehicles, abnormal loads, waste management".[90] Mike Heintz of the UNITE Alliance (which represents major companies such as Boeing, Lockheed Martin and Northrop Grumman) stated that further examples of UAS applications "are limited only by our imagination".[91]

This overview demonstrates that while UAS devices have been used in a range of applications, it is the same "usual suspects" who are targeted by UAS surveillance. Eick argues that in Western Europe, there is "hardly a marginalised group that is not targeted by UAVs", and this paper illustrates that this is common to other countries as well. Large crowd monitoring generally focuses on protesters, "hooligans" and "anti-social" elements. The use of UASs to prevent or detect crime through monitoring spaces or small crowds have been deployed against "bikers", groups of young people and undocumented migrants, while UASs which support police in incident response have been used against young people and squatters. Similarly, border surveillance, particularly as used along the US–Mexico border and for maritime surveillance, often have people of colour as their intended targets. As Coleman and McCahill note, surveillance systems often reinforce positions of marginalisation,[92] introducing civil liberties concerns regarding discrimination into deployments of UAS devices. Furthermore, despite the benefits to policing and border surveillance, the use of UAS technology raises safety, ethical and privacy concerns alongside this disproportionate targeting of already marginalised populations.

4. Privacy impacts and ethical issues raised by the technology

While there are clear beneficiaries in relation to the deployment of UASs in civil applications, some academics, civil society organisations and journalists voice significant concerns about their large-scale deployment. Although safety is a significant consideration, the potential for ethical and privacy infringing practices represents a clear threat to civil

[73] Ibid.
[74] Nevins, op. cit., 2011.
[75] Homeland Security News Wire. Canadian police push limits of civilian UAV laws. 17 Feb 2011. http://homelandsecuritynewswire.com/canadian-police-push-limits-civilian-uavs-laws.
[76] Lewis, op. cit., 2010.
[77] Ibid., p. 4.
[78] Hull, op. cit., 2010.
[79] Lawrence Mark. Setting matters straight. AirRobot UK News 2008. http://www.airrobot-uk.com/air-robot-news.htm.
[80] Ibid., p. 4.
[81] Bowes, op. cit., 2006.
[82] Sia Richard HP. Agencies see homeland security role for surveillance drones. Congress Daily 12 Dec 2002. http://www.govexec.com/dailyfed/1202/121202sia.htm.
[83] McBride, op. cit., 2009. p. 635.
[84] Dunlap, op. cit., 2009. p. 180. See also Matthews, op. cit., 2010.
[85] Nevins, op. cit., 2011.
[86] Eick, op. cit., 2009.
[87] Bowcott and Lewis, op. cit., 2011 and Page, op. cit., 2007.
[88] Bowcott and Lewis, op. cit., 2011.
[89] Whitehead, op. cit., 2010.
[90] Lewis, op. cit., 2010.
[91] McCullagh, op. cit., 2006.
[92] Coleman and McCahill, op. cit., 2011.

liberties. Those who deploy UAS devices appear to be cognisant of these potential civil liberties concerns, where, for example, Lewis finds that police forces in the South Coast partnership sought to stress the "good news story" of UAS maritime surveillance rather than the general usage of UASs in police work to minimise civil liberties concerns and deflect fears about "big brother".[93] However, given that UASs are often deployed against marginalised persons within specific populations, this means that the safety, ethical and privacy issues are far more likely to impact upon and further marginalise these populations.

4.1. *Safety*

Safety is a primary consideration for individuals commenting on the possibility of large-scale deployments of UASs due to issues such as maintenance, pilot error and the potential use of UASs as weapons. Because they are unmanned, UASs may be less well maintained and subsequently less reliable than aircraft which carry persons[94] – the current accident rate for UAVs is 100 times that of manned aircraft.[95] The Electronic Privacy Information Center (EPIC) argues this poor safety record increases risks to commercial aircraft and civilians being monitored.[96] In 2007, the US National Transportation Safety Board (NTSB) reported that pilot error was the cause of an April 2006 Predator B crash, as the team piloting the UAV accidentally turned the engine off.[97] There is also a serious risk that UAVs, particularly as payloads become more sophisticated, could be used as a weapon, as they were in early World War I deployments.[98] For example, despite police interest in using UASs to monitor the 2012 Olympic Games, *The Guardian* reports that the UK Civil Aviation Authority is unlikely to allow UASs so close to large crowds and London City Airport.[99]

4.2. *Ethics*

In addition to safety concerns, there are significant ethical considerations surrounding the use of UASs for surveillance in civil applications. There has been an on-going debate on the ethics of using remotely piloted vehicles in combat operations. They have been blamed for significant losses of life on the ground in combat zones, the removal of soldiers "from the human consequences of their actions".[100] In relation to civil applications, Hayes, of Big Brother Watch, states that "drones and other robotic tools will add to the risks of a Playstation mentality developing along Europe's borders",[101] where bodies are objectified into "things to track, monitor, apprehend, and kill".[102] Hayes further argues that the European Union's security-industrial complex has placed law enforcement demands ahead of civil liberties concerns.[103] Nevins agrees, stating that "the normalization of previously unacceptable levels of policing and… official abuse" has "disturbing implications for civil and human rights". Whitehead concurs, stating that "the logical aim of technologically equipped police who operate as technicians must be control, containment and eventually restriction of freedom".[104] Nevins also reports fears of "mission creep" in police use of UASs.[105]

However, there is some debate about how UASs affect the targets of this distantiated surveillance. Whitehead argues that drones raise civil liberties concerns because "[e]veryone gets monitored, photographed, tracked and targeted".[106] Similarly, Nevins notes that while UASs are seen by law enforcement as "just another tool in the toolbox" and technologically neutral, "[t]here is every reason to be concerned about how the law enforcement and 'homeland security' establishments will take advantage of their new tools".[107] Wall and Monahan argue that in combat situations this distantiation is racialised, where the use of UASs has:

> *harm[ed] ethnic and cultural others with great prejudice…[and] lump[ed] together innocent civilians with enemy combatants, women and children with wanted terrorist leaders. From the sky, differences among people may be less detectable, or—perhaps more accurately—the motivations to make such fine-grained distinctions may be attenuated in the drive to engage the enemy.*[108]

We have already seen evidence that similar racialised marginalisation as well as class, gender and political marginalisation is occurring in relation to UAS surveillance in civil applications. Furthermore, the potential for UASs to carry weapons raises more immediate safety and ethical concerns about the right to life. According to PrisonPlanet.com, the death toll from non-lethal Tasers in the US is more than 350 people,[109] which Wall and Monahan predict could "further the violent dehumanization and non-differentiation" of UAS devices.[110] Thus, despite apparent technological neutrality, the negative ethical impacts of UAS devices are likely to fall disproportionately on marginalised populations.

[93] Ibid.
[94] Dunlap, op. cit., 2009.
[95] Bolkcom, op. cit., 2004.
[96] EPIC, op. cit., 2005.
[97] The Economist, op. cit., 2007.
[98] Coifman Benjamin, McCord Mark, Mishalani Rabi G, Redmill Keith. Surface transportation surveillance from unmanned aerial vehicles. In: Proceedings of the 83rd annual meeting of the Transportation Research Board; 2004. http://www.ceegs.ohio-state.edu/~coifman/documents/UAV_paper.pdf.
[99] Bowcott and Lewis, op. cit., 2011.
[100] Cronin, op. cit., 2010.
[101] Hayes Ben. Arming big brother: the EU's security research programme, summary of the report. Transnational Institute; April 2006. http://www.tni.org/es/archives/act/4451.
[102] Wall Tyler, Monahan Torin. Surveillance and violence from afar: the politics of drones and liminal security-scapes. Theoretical Criminology 2011;15(3):239–54, 246.
[103] Hayes, op. cit., 2006.
[104] Whitehead, op. cit., 2010.
[105] Nevins, op. cit., 2011.
[106] Whitehead, op. cit., 2010.
[107] Nevins, op. cit., 2011.
[108] Wall and Monahan, op. cit., 2011. p. 243.
[109] Whitehead, op. cit., 2010.
[110] Wall and Monahan, op. cit., 2011. p. 243.

4.3. *Privacy*

Privacy emerges as a key civil liberties concern in relation to the deployment of UASs. Policy-makers and law enforcement agencies have attempted to mitigate concerns about privacy by claiming that UAS devices are no different from a range of existing surveillance systems, such as CCTV or helicopter surveillance. While this may be broadly true, the argument does not address the current complexity of UAS systems which may used like fixed CCTV cameras in some situations or like helicopters in other situations, nor does it address the likely future developments in UAS capabilities or payloads.

Some journalists have relayed worries about the distinct lack of concern about the potential for civil liberties intrusions by UASs. Nevins quotes Stephen Graham, Professor of Cities and Society at Newcastle University, who says that "broader concern about the regulation and control of drone surveillance of British civilian life has been notable by its absence."[111] Evidence from projects on UASs suggests that the focus of web materials, reports and deliverables is on the technical capabilities and potential applications of UASs and they only mention privacy in passing.[112] Similarly, when discussing the revocation of the LA sheriff's licence to deploy UASs, Killam briefly mentions ACLU concerns about the surveillance of private citizens.[113]

Yet some journalists and other stakeholders have made concerted efforts to raise privacy issues in relation to UASs. A report in *The Economist* notes that "UAVs can peek much more easily and cheaply than satellites and fixed cameras can"; they can "hover almost silently above a property" and that "the tiny ones that are coming will be able to fly inside buildings".[114] *The Economist* also quotes an FAA spokesman who stated that "It smacks of Big Brother if every time you look up there's a bug looking at you".[115] EPIC notes that UAVs give the US federal government "a new capability to monitor citizens clandestinely" and states that the costs of these vehicles may outweigh the benefits.[116] Liz Hull of *The Daily Mail* describes UASs as a "worrying extension of Big Brother Britain",[117] while Sia in *Congress Daily* reports that the Senate Armed Services Committee Chairman acknowledged that UASs are "quite intrusive"[118]. Other journalists have noted that specific victims of the mass deployment of UASs in civil air space could be celebrities subject to paparazzi drones.[119]

Some of the consequences of the intrusions of UASs include physical, psychological and social effects. For example, McBride notes that conventional surveillance aircraft, such as helicopters, provide auditory notice that they are approaching and allow a person "to take measures to keep private those activities that they do not wish to expose to public view".[120] McBride opines that the mass deployment of UAS surveillance vehicles which are imperceptible from the ground "could lead to an environment where individuals believe that a UAS is watching them even when no UASs are in operation".[121] This could have a self-disciplining effect, as first described by Bentham and Foucault, where individuals adjust their behaviour as though they were being watched at all times.[122] As a result, "this advancement of surveillance technology threatens to erode society's expectation of privacy, just as the airplane once erased individuals' expectations of privacy in their fenced-in backyards."[123]

Privacy concerns *could* impede the large-scale deployment of UASs, but they face countervailing views. In the US, local law enforcement officials have recognised that privacy concerns represent a stumbling block to the deployment of UASs; however, they have sought to assure the public that "they will not be spied upon by these unmanned drones" and that "this is not [sic] different than what police have been doing with helicopters for years".[124] In LA, police officials reminded citizens that "There's no place in an urban environment that you can go to right now that you're not being looked at with a video camera".[125] While in the UK, senior police officials have argued that "unmanned aircraft are no more intrusive than CCTV cameras and far cheaper to run than helicopters."[126] Similarly, in relation to reports that Google has acquired a UAS, Dillow argues that although "adding an aerial surveillance drone to the mix could stir the ire of privacy advocates", "[i]t's tough to make a case that shooting photos on a public street is an invasion of privacy".[127]

5. Extent to which the existing legal framework addresses the privacy impacts

The numerous, relevant concerns about the safety, ethics and privacy impacts of UASs demonstrate that the use of these devices needs to be regulated. Broadly speaking, few regulations exist for the deployment of UAS surveillance. Part of the difficulty in drawing up regulatory parameters for the use of UASs is that UAVs span an entire spectrum between model aircraft and manned aerial vehicles such as planes and helicopters. Some UAVs are comparable to "large jet-powered machines capable of flying across the Atlantic", while micro-UAVs are more closely related to remotely controlled model aircraft.[128] This means that UAS regulations will likely vary depending on the model, size, weight and speed, making regulations significantly more complex and difficult to

[111] Nevins, op. cit., 2011.
[112] McCullagh, op. cit., 2006; OPARUS, op. cit., 2010; Nevins, op. cit., 2011.
[113] Killam Tim. US perspective on unmanned aerial vehicles. Institution of Engineering and Technology; 5 Dec 2007.
[114] The Economist, op. cit., 2007.
[115] Ibid.
[116] EPIC, op. cit., 2005.
[117] Hull, op. cit., 2010.
[118] Sia, op. cit., 2002.
[119] Bowcott and Lewis, op. cit., 2011.
[120] McBride, op. cit., 2009. p. 659.
[121] Ibid., p. 661.
[122] Foucault Michel. Discipline and punish: the birth of the prison. New York: Vintage; 1977.
[123] Dunlap, op. cit., 2009. p. 202.
[124] Ibid., p. 182.
[125] Bowes, op. cit., 2006.
[126] Lewis, op. cit., 2010.
[127] Dillow Clay. Google is flying a quadcopter surveillance robot, says drone maker. Popular Science 9 Aug 2010. http://www.popsci.com/technology/article/2010-08/german-spy-drones-maker-sayd-google-testing-quadcopter-surveillance-drone.
[128] The Economist, op. cit., 2007.

understand and enforce. With regard to surveillance, the section above described how many law enforcement organisations have argued that there is no difference between surveillance by UAS and surveillance by other equipment, such as helicopters or CCTV, which police have been using for some time. This section focuses on the tension between the deployment of UAS for law enforcement purposes and the various privacy or data protection regulations with which they may come into conflict. It focuses specifically on case law based on the US Fourth Amendment, EU legislation and UK legislation.

5.1. *The US Fourth amendment*

The Fourth Amendment of the US Constitution protects citizens from unreasonable searches, particularly in areas where individuals have a reasonable expectation of privacy, such as their home or the curtilage (i.e., yard or garden) of their home. Case law has set a precedent where searches are considered unreasonable if a person exhibited a reasonable expectation of privacy, and if that expectation is one which society recognises as reasonable.[129] A US Supreme Court Justice has argued that "a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited".[130] As a result, officers have been able to act on information that they gleaned "from naked-eye observations"[131] and "the Fourth Amendment has never required police officers 'to shield their eyes when passing by a home'."[132] This includes material or activities that are visible to the naked eye from aerial vehicles such as helicopters and airplanes, due to the fact that the airways are "public" and that "any member of the public could fly over [a person's] backyard and observe" illegal materials or activity.[133] Furthermore, in *California vs. Ciraolo*, where the defendant was convicted of growing marijuana plants as a result of photographs from an airplane secured by the police, the Supreme Court ruled that the use of a normal 35 mm camera in the operation did not constitute an unreasonable search because it used photographic technology that is "generally available to the public"[134] and the flight itself was judged to be "routine".[135]

However, the opinion of the Court did reflect the possibility that the use of technology which was not generally available to the public might constitute an unreasonable search. For example, the Court stated that "[a]erial observation of curtilage may become invasive, either due to physical intrusiveness or though modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens."[136] Thus, the court ruled that obtaining information about activities inside a home via thermal imaging cameras "constitutes a search – at least where (as here) the technology in question is not in general public use".[137]

Both McBride and Dunlap find that, as long as UASs are not in "general public use", their use for surveillance in places where individuals have a reasonable expectation of privacy would be covered by the Fourth Amendment and the police would be required to obtain a search warrant prior to their use. This is especially true if the UAS incorporates technology such as thermal imaging which is not in "general public use" or if the flights were not considered "routine", for example, if they were flying at non-routine altitudes.[138] However, both point out that if ever UASs are in "general public use", this protection could be nullified. One danger surrounding the general usage principle is that UAVs that could see through "windows or skylights would not constitute a search if the activities or objects inside could be seen with the naked eye" if they were in general use.[139] Furthermore, because electro-optical lenses function similarly to binoculars, telescopes and conventional cameras already used by the public, these sorts of searches could be constitutional even if UASs themselves were not in general public usage.[140] In a similar vein, the courts could argue that UASs are similar enough to helicopters and other methods already used by the police to make surveillance of the area outside the home constitutional.[141]

5.2. *EU legislation and judicial decisions*

In Europe, the use of aerial surveillance technologies is covered by the Charter of Fundamental Rights of the European Union 2000. Article 7 of the Charter of Fundamental Rights states that a person has a right to respect for their private and family life, home and communications, while Article 8 states that an individual has the right to the protection of their personal data. This protection of personal data includes fair processing, consent, access to data and right to rectification. In *Peck vs. the United Kingdom*, the European Court of Human Rights reiterated an understanding that "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life", making public space surveillance such as CCTV lawful under the Charter of Fundamental Rights.[142] Under this consideration, UAS surveillance that monitors public space but does not record would be lawful, but surveillance which includes the private home would likely require oversight.

Video surveillance, such as CCTV, which does record falls under the scope of the EU Data Protection Directive of 1995 (95/EC/46). According to the Article 29 Working Party, images or voices are considered to be personal data if they "provide information on an individual by making him/her identifiable

[129] Dunlap, op. cit., 2009. p. 185.
[130] Ibid.
[131] McBride, op. cit., 2009. p. 627.
[132] Dunlap, op. cit., 2009. p. 186.
[133] Ibid., p. 186–7.
[134] Ibid., p. 189.
[135] McBride, op. cit., 2009.
[136] McBride, op. cit., 2009. p. 649.
[137] Dunlap, op. cit., 2009. p. 195, and McBride, op. cit., 2009. p. 655.
[138] McBride, op. cit., 2009. p. 647.
[139] Dunlap, op. cit., 2009. p. 199.
[140] Ibid.
[141] Ibid.
[142] Williams Victoria. Privacy impact & the social aspects of public surveillance. Covert Policing Review 2008.

even if indirectly".[143] Thus, public space surveillance which records visual data would be considered "personal data" under the Charter of Fundamental Rights and the Data Protection Directive and would mean subjects have rights of consent, access and correction. This is particularly the case after the abolition of the pillar structure of the EC, whereby the original Data Protection Directive did not apply to law enforcement or border protection activities. At present, the abolition of the pillar system means that the way in which the Data Protection Directive now applies to these activities is uncertain. However, if the Data Protection Directive is applicable, individuals in Europe would have the right to access data recorded about them (even indirectly) via a UAS device and they should be given an opportunity to consent to this surveillance.

5.3. *UK legislation*

In the UK, surveillance by UAS devices could be covered by the Data Protection Act 1998 or the Regulation of Investigatory Powers Act (RIPA) 2000. In current deployments of visual surveillance systems such as CCTV, the Data Protection Act 1998 stipulates that, like the EU Data Protection Directive, individuals must be told that a surveillance system is in operation and individuals can request copies of the data the CCTV data controller holds about them.[144] Thus, the Data Protection Act only applies to overt surveillance systems. This could also cover helicopter surveillance, in that helicopter surveillance can be considered overt, due to the noise and visibility of helicopters themselves. However, it would be difficult to inform individuals that UAS surveillance is in operation, particularly as one of the advantages of UAS surveillance is that they are silent and fly at altitudes which make them practically invisible.

In relation to covert surveillance, where the authorities are not obligated to inform individuals that surveillance is taking place, their activities must conform to RIPA. RIPA was enacted to ensure that police investigatory powers were deployed in accordance with the Human Rights Act 1998.[145] RIPA covers both intrusive and directed surveillance, where intrusive surveillance includes surveillance carried out in relation to residential premises or private vehicles and directed surveillance is surveillance that is likely to discover personal information about a target.[146] UAS devices which can hover over homes, can see inside windows and which are fitted with devices such as thermal imaging cameras that may "interfere with a person's private life" would likely need RIPA authorisation in order to be deployed.[147] According to Purdy, RIPA legislation means that large scale, random surveillance of communities or populations using such enhanced UASs would be difficult to justify and are unlikely.

5.4. *Discussion*

This exploration suggests three separate conclusions regarding the current regulation of UAS surveillance. First, this article demonstrates that the complexity of UAS capabilities, available payloads and applications means that a range of laws may apply to the use of UAS devices for surveillance. Some deployments of UASs are similar to CCTV systems or incident response by police helicopter. Because they monitor public space, over-arching regulations like the Charter of Fundamental Rights in the EU or the Data Protection Act in the UK are appropriate to these deployments, as long as the difficulties surrounding consent and access to data can be addressed. However, UAS surveillance that is covert, that uses attachments such as thermal imaging cameras or that is used to monitor private spaces (e.g., a home) would require additional oversight mechanisms, such as search warrants or RIPA approval, in order to be lawfully deployed. Thus, despite Big Brother Watch's call for "stringent, clear, and easily accessible guidelines about how and when these drones can be deployed"[148], such clarity may not be possible given the complexity of these systems.

Second, while current regulations attempt to mitigate some of the privacy issues raised by UAS surveillance, these regulations do not address the other ethical implications of UAS deployment. None of the privacy-focused regulations discussed in this paper adequately addresses the possibilities for social sorting, discrimination or the distantiation effects of UAS surveillance. The Fourth Amendment, the Data Protection Directive and the Data Protection Act do not protect already marginalised individuals and populations from disproportionate surveillance by UAS devices. Furthermore, this legislation does not protect individuals from the "Playstation mentality" of which operators of unmanned aircraft systems have been accused in combat scenarios.

Finally, given the complexity of UASs and the inadequacy of current legal instruments, we find that over-arching legal instruments are not appropriate to protect privacy and other civil liberties in UAS deployments. In the US, McBride has argued that since privacy cannot be adequately protected, the only possible over-arching solution is to consider UAS surveillance "presumptively unconstitutional" because UASs *require* technology to undertake visual surveillance, and the benefits of UASs are specifically associated with high powered cameras, thermal imaging cameras and other sensors.[149] Dunlap states that if they are deployed, administrative measures must accompany legislation, and police departments should be subject to external direction and independent oversight.[150] However, even a legislation combined with oversight may not adequately protect individuals from new

[143] Article 29 Data Protection Working Party, Opinion 4/2004 on the processing of personal data by means of video surveillance. 11750/02/EN, WP 89; 11 Feb 2004.
[144] Information Commissioners Office. CCTV code of practice. Wilmslow, Cheshire, UK; 2008.
[145] Purdy Ray. The heat is on. The New Law Journal 19 May 2006; 156(7225):1–4, 2. http://www.ucl.ac.uk/laws/environment/satellites/docs/The_heat_is_on156_NLJ_834.pdf.
[146] Home Office. Covert surveillance and property interference revised code of practice; 2010.
[147] Purdy, op. cit., 2006. p. 2.
[148] Sharpe Dylan. Surveillance drone grounded days after 'success'. Big Brother Watch 16 Feb 2010. http://www.bigbrotherwatch.org.uk/home/2010/02/surveillance-drone-grounded-days-after-success.html.
[149] McBride, op. cit., 2009. p. 655.
[150] Dunlap, op. cit., 2009. p. 203.

applications or new capabilities. Instead, a bottom-up mechanism is advocated by Wright et al. who argue that:

> "*today's 'smart surveillance' approaches require explicit privacy assessments in order to sort out the necessity and proportionality of surveillance programmes and policies vis-à-vis privacy…. [I]mprovements are needed in our legal and regulatory framework if privacy is indeed to be respected by law enforcement authorities and intelligence agencies*."[151]

They assert that one of the primary ways to correct the imbalance between privacy and law enforcement is to explicitly thread privacy considerations through the development and implementation phases of surveillance technology deployment. Such a mechanism may encourage those who deploy UASs for civil applications to focus on what they should do, rather than what they may do. This bottom-up procedure could be combined with a top-down requirement that a privacy or ethical impact assessment must be conducted in order to ensure compliance, whilst simultaneously ensuring that the assessment process is flexible enough and organic enough to address concerns specific to the technological capabilities and deployment procedure under consideration.

6. Conclusion

This consideration of UASs as a "new surveillance" system being introduced for deployment in civil applications has raised significant issues. First, it finds that as a surveillance system, UASs continue a disproportionate attention to the activities of already marginalised populations. Existing divisions such as race, class, political orientation, gender and sexuality are already reflected in current deployments of UASs for policing and border control. Furthermore, the heterogeneity of UAS surveillance devices, capabilities and applications and the way in which many can be deployed covertly, introduce a range of safety, privacy and ethical concerns surrounding their use. We find that these privacy and ethical concerns are not adequately addressed by existing regulatory mechanisms or legislation in the US, EU and UK. Instead, we conclude that multi-layered regulatory mechanisms that combine legislative protections with a bottom-up process of privacy and ethical assessment offer the most comprehensive way to adequately address the complexity and heterogeneity of unmanned aircraft systems and their intended deployments.

Acknowledgement

This paper draws on research performed in the context of the PRESCIENT project (Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment), funded by the European Commission under grant agreement no. 244779. The views in this paper are those of the authors alone and are in no way intended to reflect those of the European Commission or other members of the PRESCIENT consortium.

Rachel L. Finn *(rachel.finn@trilateralresearch.com), Trilateral Research & Consulting, LLP, London, UK.*

David Wright *(david.wright@trilateralresearch.com), Trilateral Research & Consulting, LLP, London, UK.*

[151] Wright David, Friedewald Michael, Gutwirth Serge, Langheinrich Marc, Mordini Emilio, Bellanova Rocco, et al. Sorting out smart surveillance. Computer Law & Security Review 2010;26(4): 343–54, 344.