International Working Group
on Data Protection
in Telecommunications

675.47.25

Working Paper on Privacy and Aerial Surveillance

54th Meeting, 2-3 September 2013, Berlin (Germany)

Background

Surveillance is the monitoring of behavior, activities, or other changing information, for the purpose of influencing, managing, directing, or protecting someone or something. It often involves observation of individuals or groups by government organizations, although there are some exceptions, such as disease surveillance, which monitors the progress of a disease in a community without directly observing or monitoring individuals.

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle. Since the International Conference of Data Protection and Privacy Commissioners first discussed issues of aerial surveillance by satellites in 1992[1], there have been far-reaching technological developments. Whereas satellite-based services such as Google Earth at present do not pose particular risks to individual privacy as long as only snapshots with limited resolution of imagery are collected, the situation is different with regard to low flying surveillance platforms such as drones. Whereas the use of drones for military (combat) purposes is the subject of some limited – due to classification - public debate, similar debate about civilian uses of this technology for information collection purposes and their consequences has so far been neglected. The history of satellite technology since 1989 shows however that reconnaissance technology formerly restricted to military use can eventually become available for civilian use as well.

Surveillance platforms can be used for a wide range of purposes, including:

a) Remote sensing: the use of a variety of sensors (visual, infrared or near infrared spectrum, gamma ray, biological and chemical) to detect the presence of chemicals, microorganisms and other biological factors, radioactive materials, weapons and so on;

[1] Cf. Report of the Working Group on Data Protection in Telecommunications on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the 14th International Conference of Data Protection and Privacy Commissioners, 29 October 1992, Sydney, in: International Documents on Data Protection in Telecommunications and Media 1983 – 2006, p. 51; http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

b) Commercial aerial surveillance: livestock monitoring, wildfire mapping, pipeline security, home security, precision farming, road patrol and anti-piracy[2];

c) Resource exploration: perform geophysical surveys in order to predict the location of oil, gas and mineral deposits, monitoring the integrity of oil and gas pipelines and related infrastructure, comparing the real size of farmland for which subsidies have been received with claims in the corresponding application forms[3];

d) Scientific research: weather observations, including close monitoring of dangerous weather systems such as hurricanes, or use in severe climates such as the Antarctic;

e) Search and rescue: searching for missing persons, damage assessment following a natural (or man-made) disaster; and

f) Conservation: monitoring movements of animals, detecting and monitoring hazardous material spills, forest fire detection, fishery protection, etc.

Surveillance Platforms

A variety of platforms[4], or vehicles, has been or can be used for aerial surveillance, including:

a) Fixed Wing: a fixed-wing aircraft is an aircraft capable of flight using wings that generate lift caused by the vehicle's forward airspeed and the shape of the wings. The wings of a fixed-wing aircraft are not necessarily rigid; kites, hang-gliders and aeroplanes using wing-warping or variable geometry are all regarded as fixed-wing aircraft;

b) Rotary Wing: the term rotary wing describes an airfoil that rotates about an approximately vertical axis, as that supporting a helicopter or autogiro in flight;

c) Unmanned Aircraft Systems (UAS): an unmanned aircraft (UA), commonly known as a drone, is an aircraft without a human pilot on board. Its flight is either controlled autonomously by computers in the vehicle, or under the remote control of a pilot on the ground or in another vehicle. UAS can either be fixed or rotary wing craft;

---

[2] The US-companies Skybox Imaging and Planet Labs are planning to deploy fleets of lightweight microsatellites to engage in Live Earth Screening. They are allowing private investors to buy and downlink imagery, cf. http://www.nytimes.com/2013/08/11/business/microsatellites-what-big-eyes-they-have.html?_r=0 (seen on 20 October 2013).

[3] Cf. the European Integrated Administration and Control System (IACS) <http://ec.europa.eu/agriculture/direct-support/iacs/index_en.htm> aimed at preventing fraud in agricultural subsidies. IACS includes satellite surveillance.

[4] A different categorization appears on page 2 of Stanley, J and Crump. C., "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report dated December 2011 (available online at http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf)

and may be operated singly or in swarms (communicating with each other and with the ground under centralized control) or

d) Other: an aerostat is a craft that remains aloft primarily through the use of buoyant lighter than air gases, which impart lift to a vehicle with nearly the same overall density as air. Aerostats include free and/or moored balloons, airships or dirigibles and may be powered or unpowered.

Each of these platforms will have different operating characteristics such as operating altitude, speed, range, endurance (i.e., how long can the platform remain aloft), ability to loiter, and payload capacity.

Surveillance Technologies

A variety of surveillance technologies can be carried by the above-mentioned platforms, the exact payload being dependent on a number of factors including mission, weather, payload capacity, the range of the sensor, its field of view and resolution, and so on. Sensors include (but aren't necessarily limited to):

a) Visible spectrum: these sensors are typically in the form of cameras, including high-definition and full motion video systems[5]; they allow for continuous live surveillance and storage of the entire video footage;

b) Infra-Red (IR): these types of sensors detect energy emitted or reflected from the target. Most IR sensors are passive, although they may be used in conjunction with an IR illumination source. They can "see" through smoke, fog, haze and other atmospheric obscurants better than a visible light camera;

c) Night Vision: the ability to see in low light conditions, based on a combination of sufficient spectral range (i.e., how much of the electromagnetic (EM) spectrum the device can detect) and sufficient intensity range (i.e., how much light is needed to form a useful image). Night vision technologies can be broadly divided into three main categories:

1) Image intensification: these technologies work on the principle of magnifying the amount of received photons from various natural sources such as starlight or moonlight. Examples of such technologies include night glasses and low light cameras;

[5] The U.S. Army recently acquired a 1.8 gigapixel camera for use on its drones. This camera (Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System - ARGUS IS) offers 900 times the pixels of a 2 megapixel camera found in some cell phones; it was built at low cost using 368 camera chips from cell phones. It can track objects on the ground 65 miles away from an altitude of 20,000 feet. Cf. *US Army unveils 1.8 gigapixel camera helicopter drone*, BBC NEWS (29 December 2011), http://www.bbc.com/news/technology-16358851. An instructive video can be seen at: http://www.youtube.com/watch?v=QGxNyaXfJsA> accessed on 2 April 2013.

2) Active illumination: these technologies work on the principle of coupling imaging intensification technology with an active source of illumination in the near infrared (NIR) or shortwave infrared (SWIR) band. Examples of such technologies include low light cameras; and

3) Thermal imaging: these technologies work by detecting the temperature difference between the background and the foreground objects.

d) Radar: radar uses very high frequency radio waves to determine the range, altitude, direction or speed of an object. Radar can also be used to identify and track objects, such as vehicles, on the ground (using, for instance, Side Looking Airborne Radar (SLAR)); and

e) Specialized sensors: a range of specialized sensors (e.g., to detect traces of chemical, biological, nuclear, radiological and explosive materials; license plate scanners; acoustic sensors, etc.) can also be carried by aerial surveillance platforms.

Combinations of these sensor types can provide organizations with the capability to conduct aerial surveillance under almost any conditions.

Privacy Implications

There are a number of aspects of surveillance that raise privacy concerns, including the surveillance being hidden, intrusive, indiscriminate and/or continuous.[6] Although these aspects were articulated in the context of electronic surveillance, they are also applicable to aerial surveillance:

a) Hidden: depending on size, operating altitude, sensor capabilities and so on, it may not be possible to detect aerial surveillance (either the platform itself or the sensors being used). Those subject to surveillance would have to rely on self-disclosure by the organization conducting the surveillance or disclosure by a third party. Those subject to hidden surveillance are less able to hold the organization conducting the surveillance accountable;

b) Intrusive: the range of possible operating conditions for aerial surveillance platforms and the capabilities of their associated sensors increase the intrusiveness of aerial surveillance (they can "see" almost anything and everything);

c) Indiscriminate: aerial surveillance generally covers an area that includes individuals and activities that do not warrant being subject to surveillance, resulting in an over-collection of information; and

[6] Freiwald, Susan, "A First Principles Approach to Communications Privacy", published in the Stanford Technology Law Review (2007 STAN. TECH. L. REV. 3), dated 2007. Available online at http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

d) Continuous: emerging aerial platforms combine increasing endurance and the ability to "stare" at an area to effectively create continuous surveillance of any given area[7].

These characteristics give rise to some specific privacy concerns[8]:

a) Mission creep: although most people would likely support the use of aerial surveillance (e.g. for detecting and monitoring natural disasters), or for use in specific, limited law enforcement circumstances, it seems inevitable that other privacy-invasive uses would be found for such technology;

b) Tracking: the ability to maintain surveillance over an extended area for an extended period of time raises the possibility that individuals and vehicles could be tracked on an on-going basis;

c) Proliferation as the cost of UAS technology is rapidly falling. UAS may be bought or built by private individuals for use as "personal" or "DIY" UAS.

More privacy intrusive than CCTV

The privacy implications of CCTV have been a subject of debate for years, and many privacy authorities have issued guidelines on the necessary safeguards regarding its use. As explained above, aerial surveillance systems have the potential to be much more privacy intrusive than CCTV systems, for several reasons including:

- Aerial surveillance systems may use many more different sensors than CCTV systems.
- The installation of CCTV usually requires access to and control of the premises concerned, which is not required for aerial surveillance systems, in particular for outdoor locations.
- Depending on flight height and other factors (e.g. miniaturization) aerial surveillance systems may be more difficult – if not impossible - to detect by the persons observed than most CCTV systems.
- Aerial surveillance systems may be deployed without any delay, not requiring installation or configuration on site.

This clearly indicates that the safeguards in place for CCTV, while indicating a minimal standard, cannot be considered sufficient in the context of aerial surveillance systems and

---

[7] The U.S. Air Force has developed the "Gorgon Stare" technology, a spherical array of nine cameras fitted to a drone which is able to capture motion imagery of whole cities ("With Air Force's Gorgon Drone 'we can see everything'", http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html

[8] A discussion of different potential privacy concerns/issues appears on page 11 of Stanley, J and Crump. C., "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report dated December 2011 (available online at http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf)

have to be adapted and complemented by specific measures appropriate for the different aerial surveillance systems and usage scenarios.

Therefore certain new essential safeguards should be adopted by regulators on a national level taking into account possible differences between the public and the private sector. Furthermore, since aerial surveillance does not stop at national borders international agreements will be necessary to prevent a "global panopticon" from emerging.

Recommendations

Whether operated by law enforcement or other public sector agencies, by private sector companies, or flown recreationally by citizens, the increasing use of aerial forms of surveillance will likely intensify concerns about how to preserve and protect individual and collective privacy as people go about their daily lives. If aerial surveillance becomes an increasingly common fixture in today's society, and society accepts that presence as normal, it is conceivable that society's expectations of privacy in public could seriously erode. It is important to secure an appropriate balance between the needs of law enforcement, public safety, etc. on the one hand and the legitimate privacy interests of individuals on the other. With that in mind, the Working Group makes the following recommendations:

a) the use of aerial surveillance should be limited to specific purposes[9] (e.g., searching for missing persons, border surveillance, legitimate private purposes such as access to information by journalists);

b) the use of personal data such as images collected from the air by government agencies should require a judicial warrant;

c) to the maximum extent possible, the public should be notified about the use of aerial surveillance; this requires e.g. that any UAS with the ability to collect and transmit information over a data link reports a GPS location, capabilities and ownership (e.g., government agency, company or private individual responsible for the particular platform or vehicle), in real time, to a competent authority

---

[9] The ACLU describe the following constraints on the use of drones:
a) **USAGE LIMITS**: Drones should be deployed by law enforcement only with a warrant, in an emergency, or when there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific criminal act;
b) **DATA RETENTION:** Images should be retained only when there is reasonable suspicion that they contain evidence of a crime or are relevant to an ongoing investigation or trial;
c) **POLICY:** Usage policy on domestic drones should be decided by the public's representatives, not by police departments, and the policies should be clear, written, and open to the public; and
d) **ABUSE PREVENTION & ACCOUNTABILITY:** Use of domestic drones should be subject to open audits and proper oversight to prevent misuse.
See http://www.aclu.org/blog/tag/domestic-drones; see also the resources listed by EPIC at http://www.epic.org/privacy/drones mentioning several bills addressing these issues currently before the U.S. Congress.

and that this authority makes location information available, as open data, in real time;

d) surveillance should be restricted to as confined an area as possible (by limiting sensor fields of view), in order to minimize the likelihood of "over-collection";

e) stringent controls over how aerial surveillance information can be used and who has access to that information should be implemented. Exceptions can be made for emergencies (e.g., searching for missing persons); and

f) there should always be a "man in the loop" so that if there are any problems or unusual circumstances (e.g., the UAS starts to drift into a residential area), these can be addressed in as timely a manner as possible.

In view of the rapidly evolving technology, the Working Group will continue to monitor developments in this field closely.