

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Consultation on the Safe Use of drones in the UK - Big Brother Watch Response

March 2017

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group that was founded in 2009. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this consultation we have campaigned on the use of drones by both the public and private sector for a number of years. We also participated in the Sciencewise Oversight Group for RPAS and small drones.

Key Points

- **Registration of drone users is the cornerstone of any future system of regulation.**
- **Any system of registration has to consider the privacy of drone users.**
- **Work needs to be progressed quickly on an electronic identification system.**

Response

The response will consider *Proposal D: Improving leisure drone user awareness of the law*, *Proposal G: Registration of drones* and *Proposal H: Electronic Identification of drones*.

Registration

In December 2015 Sky News reported that the number of public complaints to the police about drones had risen by 2000% in three years¹. Clearly this is an issue and law enforcement has to be able to respond effectively.

Key to helping the police deal with the rising number of concerns is the idea of registering drones. Without a workable system of registration for privately used drones it could be argued that very little progress can be made towards policing their use or making sure they are flown in a legal way. Registration is a process which needs to be given serious consideration sooner rather than later. The longer a system takes to implement the more drones will need to be registered retrospectively increasing the administrative burdens needed to make the system effective.

Whilst speed is of the essence it shouldn't be an excuse to cut corners. Whatever system is introduced has to inspire confidence in both members of the public and users, be sensible, easy to administer and easy to promote.

¹ Sky News, *Calls To Police Over Drones Up By 2,000%*, 16th December 2015: <http://news.sky.com/story/calls-to-police-over-drones-up-by-2000-10335752>

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

The creation of a registration system will necessitate the creation of a database to store the personal information of drone users. Any information or data provided to a registration service must be properly protected. This should include a high level of encryption and an audit system to maintain a consistent record of who has accessed information and for what purpose. In addition to this the Government must only collect the minimum amount of information it needs to make the system work. A register must not become an opportunity for the collection of more personal data just in case it becomes useful at some point in the future. Any system could understandably hold the following information about users:

- Their name.
- Their address.
- Their contact details.

Any plans to collect further information must be properly justified. An instructive case on this is the Federal Aviation Authority's (FAA's) system of registration in the USA. Despite initially keeping the details of registered drone users private, the FAA has hinted that it will allow members of the public to search it in the future². This would make private information about drone users public. A repetition of this in the UK would be unacceptable. The database must be a tool to resolve genuine concerns, not just a method of snooping on people.

It is important that any system of registration minimises the number of people who will be required to store or transmit information. To ensure this proper thought should be given to where and how drone users are registered. Ahead of the US registration scheme the Retail Industry Leaders Association (RILA) argued that drones should not be registered at the point of sale³. The RILA pointed out that this would almost certainly involve customers handing over personal information at checkouts and could potentially be overheard by others. This kind of approach would also create another layer of storage and more opportunities for data to be lost, stolen or misused.

Transparency should be a key requirement of the registration scheme. It is important that any data provided by the individual is maintained by them, that the individual can amend any errors, have full sight of their data and control over who sees it, uses it or where it is shared. The General Data Protection Regulation (GDPR) will come into force in May 2018 and any scheme must clearly adhere to the systems of control, consent and protection as outlined in it.

Improving awareness of the law

Ensuring that people, particularly leisure users, know how to use drones safely and legally will be crucial to cutting down on accidental infringements on privacy and lawbreaking. Mandating that

² Engadget, *Confusion over FAA drone registry results in privacy problems*, 2nd March 2016:

<https://www.engadget.com/2016/02/03/faa-drone-registry-is-a-privacy-nightmare/>

³ Law360, *Point-Of-Sale Drone Registration Wouldn't Fly*, FAA Told, 21st January 2016:

<https://www.law360.com/privacy/articles/749311/point-of-sale-drone-registration-wouldn-t-fly-faa-told>

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

official guidance is issued at the point of sale or activation would go a long way towards making sure users know there are guidelines to follow and what they should be doing.

Thorough research needs to be done to understand what the best format for engaging users will be. This should include work to identify whether it is more effective to issue guidance at the point of sale or the point of activation. This is important because it won't matter how well written or informative the guidance is if only a small number of users are aware of it.

Any guidance should be as simple and succinct as possible. This will maximise the chances of it being read and understood before a drone is used. Whilst it is not for Big Brother Watch to say exactly what should appear in the guidance to address the safe flying of a drone, we would stress the importance of providing a detailed explanation of the potential privacy risks that drones bring and how breaches of privacy can be avoided.

The Dronesafe website, developed by National Air Traffic Services and the Civil Aviation Authority, is a good first step and could be used as a basis for further materials.

Electronic Identification

Big Brother Watch supports the idea of making drones electronically identifiable. Allowing drones to be identified by citizens on the ground will make it much easier for them to report any drone they think is being misused to the police. It complements the idea of a register of drone users and will further help the police to apprehend and sanction drone users who break the law.

As with the registration of drones it is important that privacy is considered from the outset of any project. No personal information about the user should be included in the identification process. Other members of the public should only be able to obtain something such as an identification code or a serial number which can then be passed to the relevant authorities who can search the register, if necessary, and discover the identity of the user.

It is important that electronic identification is pursued as a priority. It will allow the police to proactively stop those using drones to break the law, rather than just reacting to events and relying on recovering the drone or catching the individual in the act of controlling of it.