APPG ON DRONES' RESPONSE TO DRAFT EC POLICY RECOMMENDATIONS FOR PRESENTATION AT EUROCONTROL 29 SEPTEMBER

Introduction: timing and methodology

1. The APPG Officers welcome the opportunity to participate in this Commission Study led by Trilateral Research.

2. The draft Policy Recommendations dated 22nd September focus on 'soft law.' They proceed from the premise that the existing legal framework is adequate to address the privacy, data protection and ethical issues raised by civil RPAS. Whilst the Policy Recommendations are welcomed in so far as they go, the basis for this premise, including the research and methodology of the study, is not clear. The APPG Officers would welcome further information on the study, and an opportunity to supplement this submission at a later stage.

3. On the basis of the information available, and timescale for response, it is difficult to engage fully in the consultation. In particular, APPG Officers (on behalf of the APPG) are concerned about the following limitations:

    (i) It has not been possible to circulate the underlying research leading to the conclusion that the legislative framework is adequate (in what is called 'Chapter X' of that research document);

    (ii) It is not clear which 'existing legal framework' is being referred to. It may well be that the reference is to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**'the 1995 Directive'**) and the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter (**'the Framework Decision'**). However, these are shortly to be superseded by a new Regulation and Directive. The Proposal for a Regulation (dated 25 January 2012) says the following about the reforms:

> *'The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal*

uncertainty and a widespread public perception that there are significant risks associated notably with online activity. This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.'

It may be that the legislative frameworks referred to in the draft takes account of other provisions, not limited to data protection, such as the relevant provisions of the Charter of Fundamental Rights, but this is not clear to the APPG Officers either;

(iii) Key definitions and analysis are not present in the draft. There is no discussion or definition of 'privacy' under the relevant data protection legislative framework and human rights legislation and case-law. Similarly, there is no discussion or working definition of 'RPAS' in the draft, nor distinctions between small, light and large civil drones. For example, the APPG has previously suggested that the RUSI identification of four types of drone (nano, miniature, tactical and strategic) is adopted, and privacy implications of each type considered separately.

The Officers of the APPG ('the APPG') notes, however, that the draft circulated for feedback is a summary document and the recommendations are focused on practical steps.

Key points

4. The Officers of the APPG ('the APPG') are not convinced by the claim in that the existing legal framework is adequate. The APPG notes that the focus of the study is data protection, not human rights, other aspects of privacy or ethical issues. The APPG notes that serious doubts have been expressed as to the suitability of the existing legal framework to regulate RPAS by the APPG, leading Human Rights NGOs and others, and that the RPAS industry is widely considered to be 'lightly' regulated.

5. The APPG is not convinced by the claim that the EU has no authority or potential authority over drones operated for the purpose of law

enforcement or by individuals. However, the Data Protection regime is clearly aimed at organisations, not individuals, and there are exceptions for law enforcement. The APPG notes that the EU has recently acceded to the European Convention on Human Rights and is a party to the Convention. The EU may also become a Co-Respondent against Member States for privacy breaches.

6. The APPG suggests that further research and consultation on the need for 'hard law' change at the EU level is necessary to ensure that all aspects of privacy and data protection, as they relate to RPAS, are covered; that there is in-depth research and consultation with a wide range of stakeholders in addition to representatives from the RPAS industry and national data protection agencies; that piecemeal frameworks at both an EU and national level are assessed together; and that the effect of derogations and exceptions are carefully examined in the context of increasing drone use.

7. It is suggested that, without such further work, it will be difficult for the European Commission to make an informed decision on the need for new law at an EU level to:

    (i) comprehensively address all privacy aspects of civil drone use;

    (ii) enable effective monitoring by relevant government bodies and parliament;

    (iii) assess the functions, expertise and capacity of existing regulatory bodies, and their overlap;

    (iv) ensure individual rights can actually be enforced, as well as understood; and

    (v) ensure a sufficient degree of consistency between EU states, noting that some RPAS operations will cross Member State borders.

8. The APPG suggests that such further work may be carried out in parallel to ongoing EC work on the need for new laws to enable safe integration of drones into civil air space. Where new hard law on safe integration is anticipated, the EC should consider an additional Part to consolidate and

supplement privacy and data protection regulation at an EU level. At least, the APPG considers that the EC should not shut the door to the option of new hard law at this stage.

9. Further, it is preferable that the existing recommendations for mandatory privacy impact assessments and transparency/certification protocols are implemented and enforced by detailed hard law measures at EU level. These are the 'core' safeguards which protect fundamental rights. The APPG would welcome dialogue on how this might be possible.

10. Overall, the draft recommendations appear to be somewhat industry led. Whilst it is important to consult the industry and consider the impact of hard and soft measures on the emerging RPAS industry, without further research, analysis and consultation, the policy recommendations risk criticism from a concerned public. This may be considered a high-risk strategy, where there is general consensus that public understanding and confidence is important. Without new hard laws to clarify legal duties and expectations, 'reputable civil RPAS operators' may also be exposed to the risk of litigation that would otherwise be ill-founded.

11. The APPG notes that the focus of the study for DG ENTR is commercial use of drones for civil missions. However, government bodies are likely to continue to sub-contract missions to commercial RPAS agencies and information is likely to be shared between companies and government bodies. It is hoped that the final study will address these areas of overlap.

12. Member States should be encouraged to carry out comprehensive reviews of civil drone use, collate and share information centrally and hold inclusive debates within parliaments on the need for new domestic hard laws to supplement those at EU level, ensuring that any gaps in existing piecemeal regulation are filled. Please see the UK's new draft CCTV Code and APPG submission as a case study.

13. It would be helpful if the final recommendations could flag and encourage such additional work needed at a national level. In particular, it should highlight those areas that Member States and their parliaments must consider independently, including law enforcement.

The legislative framework

14. As mentioned above, the APPG cannot be certain what legislative framework the draft Policy Recommendations proceed from, given that there are reforms pending. However, the APPG has proceeded on the footing that the relevant 'framework' is the existing one, as it is unknown when the legislative reforms at the EU level will be finalised. The APPG believes (although there has not been time to consider fully) that many of the issues highlighted in this response will still be of concern even after the new Regulation come into play.

15. The key pieces of the existing EU framework are:

    (i) In relation to data protection: the 1995 Directive, the Framework Decision, Article 16(1) TFEU and Article 8 of the Charter of Fundamental Rights, as interpreted in the *Digital Rights Ireland* case

    (ii) In relation to privacy rights more broadly: the Charter rights (especially Article 7) , as interpreted in the *Digital Rights Ireland* case (and relevant ECHR case law on Article 8 ECHR)

16. It may be appropriate to consider the status of the negotiations on the draft General Data Protection Regulation, in particular the detail required by Article 33 and whether privacy impact assessments should include reference to the type of data collected, use and retention of data and any plans for sharing or selling data to third parties. This would impact on the need for hard law, to some extent.

Potential inadequacies in the legislative framework

Lack of specific regulation regarding privacy generally

17. The hard law that exists only provides specific safeguards in relation to data protection, and not in relation to the protection of privacy more generally. The latter is protected at the highest level of generality, in Article 8 of the Charter and Article 16 TFEU. Thus, Article 1(1) of the 1995 Directive provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

18. This is of particular concern in relation to RPAS, which have the potential to have a far broader and more pervasive impact on privacy than other forms of data collection, or surveillance. RPAS have the potential to access zones of private life which have previously not been under a significant threat of incursion. The availability of thermal and biometric imagery, for example, opens up the possibility of a hitherto unprecedented level of access to the private lives of individuals, which goes beyond the incursion on private life represented by mere data collection and/or retention.

19. In relation to the communications intercept data at issue in the *Digital Rights Ireland* case, the CJEU said at [27]: *' Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.'* The kind of data that can be collated by RPAS clearly has even greater implications for private life than the communications intercept data at issue in *Digital Rights Ireland*.

20. It would be difficult to codify privacy protections beyond controls over data collection and retention. However, the APPG Officers consider this would be a valuable exercise and should be considered in relation to RPAS specifically.

21. It is as yet unclear what justification would be relied upon for the incursion upon privacy rights. In the case of the Data Retention Directive, as struck down by the CJEU in *Digital Rights Ireland*, and in relation to the use of RPAS for surveillance, the justification of national security/ the prevention of crime etc. can be relied upon. However, the APPG understands that the use of RPAS for far wider purposes is being considered, including but not limited to 'mapping and commercial purposes' (not defined). This makes it especially important that questions of whether any interference with private life can be justified by such activities and what sorts of safeguards can be brought into place to minimise any interference, be addressed *ex ante* and not simply on a case-by-case, presumably *post hoc*, basis.

Lack of specific provision in relation to RPAS

22. The current legislative framework does not specifically mention RPAS, nor were RPAS under consideration at the time when the legislation was drafted. This is equally true of the EU legislation referred to above as of the domestic legislation to which the APPG can speak, namely the UK's Regulation of Investigatory Powers Act 2000 ('**RIPA**') Data Protection Act 1998 ('**DPA**') and Protection of Freedoms Act 2012 ('**PFA'**).

23. The 1995 Directive, and the DPA in the UK, apply to any 'processing' of data collected by an RPAS, which is 'personal data'. 'Personal data', according to the 1995 Directive means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The DPA definition is slightly different, but essential amounts to the same thing – namely that 'personal information' is information which relates to an individual who can be identified by that data or by any other information in the possession (or likely to come into the possession) of the data controller. 'Processing' includes the use or disclosure of that data by transmission.

24. It is clear that the use of RPAS has the potential to involve the processing of personal data. However, the 1995 Directive and DPA are ill-equipped in several ways to deal with the specific issues thrown up by the use of RPAS. The question of the right to information and to access to personal data is dealt with separately below. However, also of concern are the following points:

    (i) the lack of specificity about the lengths of time for which data can be stored;

    (ii) the lack of clarity to date as to the purposes for which data collected by RPAS can be used;

    (iii) the lack of distinction between different types of data and lack of specificity regarding the particular types of data that can be collected by RPAS;

(iv) the potential for 'automated processing' and the consequences of that.

25. RIPA applies in addition to the DPA, whenever surveillance activities take place. RPAS can be used for surveillance purposes and, setting aside potential privacy concerns outlined above, there is no reason in principle why data obtained from RPAS should be treated differently from data obtained from any other form of surveillance. However, RIPA does not provide for how long data obtained via surveillance may be retained. Nor are there any restrictions on the use to which such data may be put. Issues such as these would ordinarily be governed by the DPA. The Secretary of State is entitled to remove data gathered by the security services from the scope of the DPA. To the extent, therefore, that RPAS are to be used by or on behalf of security services, there would be very little regulation of retention and use of surveillance data. That is very different to the position in respect of data obtained via interception of communications, which is subject to a separate legislative framework.

26. Whilst limits to the Trilateral study are recognised, the final recommendations may wish to give general advice on the need to treat intelligence-gathering operations distinctly and with particular care. Consideration should be given to banning commercial intelligence gathering missions, and the need for warrants (or other independent authorisation) for use of drones for surveillance purposes by or on behalf of government bodies. Additional restrictions and requirements on surveillance drones may ease the path for mainstream commercial use.

Right to be informed and of access to personal data

27. The right of access to personal data raises novel issues in relation to the collection of data by RPAS.

28. The DPA and the 1995 Directive provide the right to be informed by any data controller that data is being processed and the right to access to that information.

29. It is not obvious how the operator of an RPAS will warn potential data-subjects that their personal data may be processed. It is not clear that the suggestion in the Policy Recommendations that a 'transparency protocol' requiring, *inter alia*, signs to be placed stating that an RPAS patrol is to

take place will suffice to meet these concerns. In particular, since RPAS have the potential to view inside a person's home (or certainly inside their garden), people may become a data-subject without seeing such a sign. It is also unrealistic to suggest that signage could allow individuals to 'opt out' by 'choosing not to enter the particular area'. First, the very nature of data collection by RPAS may be too wide to make this a viable option for people. Second, individuals may already be in the area and therefore not pass signage at the 'entry' to the relevant area.

30. Whilst a code of transparency would be welcome, the APPG's view is that core safeguards should exist in hard, rather than soft law. In particular, the APPG submits that an individual cannot consent to have data collected about him or herself without knowing the precise level of data collection that is to be undertaken. The use of RPAS raise particular concerns in this regard, given their potential to collect biometric and thermal imagery. Provisions relating to the provision of information to potential data-subjects therefore need to be mandatory and should be placed in primary legislation.

31. Similar specific issues arise in relation to access to data. When seeking to access the data, the data-subject needs to be aware of the level and type of data available – biometric etc. Further, how will a request for access to data be treated when it is difficult to ascertain the identity of the data-subject in imaging, or when releasing images will inevitably implicate the privacy rights of other data-subjects? Consideration needs to be given to these issues, and the fundamental question addressed head-on: should the operation of RPAS should be prohibited to any extent where the right of access to personal data cannot be achieved.

32. In addition to the draft recommendations, the APPG suggests the following measures are considered to help address these issues:

    (i) requiring a 'licence' plate for drones issued by the aviation authority responsible for licensing;

    (ii) requiring an electronic signal which identifies the operator, mission, and data collection carried out by the drone;

    (iii) requiring 'data collection statements' as part of the proposed privacy impact assessment that must detail the data collected, how

it will be used, whether and for how long it will be retained and whether it is being sold or shared to (identified) third parties.

Enforcement

33. The APPG is concerned about the adequacy of the existing legal framework to ensure that the existing rights identified above can be enforced by individuals. The soft measures proposed will undoubtedly contribute to the monitoring and understanding of drone use by commercial operators by operators, civil aviation authorities and data protection agencies. However, the APPG is not satisfied that existing mechanisms for enforcing breaches are adequate, given increasing use of RPAS and EC Roadmap for integration into civil air space. For example, in the UK, it is considered that the ICO is likely to need an increased remit and resources to uphold information and privacy rights in this context: see APPG submission on CCTV Code.

34. It would be helpful if the recommendations could clarify obligations and expectations on Member States here, together with areas for further work and review. The problems identified by the APPG at a national level underscore the need for 'tough' new standards to regulate civil drones, as identified by the Commission in April. Legislation should contain appropriate guarantees and safeguards for all fundamental rights. Detailed soft laws and codes of practice are then welcome to supplement this. With the caveats set out above, the APPG invites further consideration of a multi-layered approach to address the complex privacy implications of civil drones, combining 'top down' legislation at both EU and national level with detailed 'bottom down' privacy and human rights impact assessments.