SUBMISSION TO THE INFORMATION COMMISSIONER'S OFFICE CONSULTATION FROM APPG ON DRONES

ON THE CCTV CODE OF PRACTICE

INTRODUCTION

'Where laws intersect with technology, as is strikingly the case with surveillance, the discrepancy between the pace of technological change and the pace of legal change requires lawmakers to consider carefully the risks that arise from the future development and application of technologies'[1]

1. This submission is concerned with the proposed amendments to the CCTV code of practice ('the Code.') The Code provides 'good practice advice' for those involved in operating CCTV and other 'surveillance camera devices' that view or record personal data, or records 'other information that relates to individuals'. The Code is concerned with application of Data Protection Act 1998 ('DPA') principles to those organisations processing personal data. It is voluntary, although designed to help data controllers comply with their legal obligations under the DPA.

2. The introduction to the Code states that it also 'reflects the wider the regulatory environment,' and refers generally to other obligations under the Freedom of Information Act 2012, Human Rights Act 1998 and Home Office Surveillance Camera Code of Practice ('SC Code'). The APPG notes that there is significant overlap with the SC Code issued under s30 Protection of Freedoms Act for (limited) designated authorities. The precise relationship with the SC Code (and respective remits and relationship between Surveillance Camera Commissioner and Information Commissioner) is difficult to negotiate[2]. The APPG acknowledges that overlap is inevitable: it is the consequence of applying different, existing regulatory regimes to the emerging technology. It would be helpful if the Code could clearly specify the areas of

[1] Wright, J (2013),Technology fuels surveillance harms. In Digital Surveillance: Why the Snoopers' Charter is the wrong approach: a call for targeted and accountable investigatory powers. Open Rights Group, page 52.

[2] The overview provided by the Roadmap on Surveillance February 2014 addresses this to an extent, covering overlaps with the Interception Commissioner too. It is suggested that the ICO may wish to reference the Roadmap in the Code.

overlap, extent and restrictions on application of each code (and Commissioners' powers and duties) with regard to the use of surveillance camera devices. This may reduce the risk that limitations and weaknesses in operation of the existing regulatory frameworks are obscured; or that summaries loose accuracy.[3]'

3. The APPG submission will focus on three questions:

   (a) how is the Code, and its proposed amendments, relevant to the use of unmanned aerial systems ('drones')[4] by Government departments, agents and other state bodies?;

   (b) does the Code, and its proposed amendments, adequately address issues raised by the use of surveillance drones (or drones with incidental surveillance capabilities)? In particular, is it appropriate to address the novel privacy issues raised by drones by amendment to the Code rather than by developing a distinct national policy on 'drones data'?; and

   (c) does the Code, and proposed amendments, adequately cover storage, sharing and use of any data obtained as a result of covert surveillance, via drones operated by or on behalf of Government departments or other state bodies?

4. The Code expressly addresses covert use of camera-carrying drones for the first time, acknowledging that 'new technologies mean new CCTV Code'[5]. The APPG welcomes this step and the opportunity to engage with the Information Commissioner's Office on the content of the Code, together with possible ways to supplement the important advice it offers.

[3] For example, the APPG notes that the draft Code is not entirely accurate in its broad assertion that 'any organisation using cameras to process personal data should follow the recommendations of this code. Note application to overt surveillance only, exemptions under DPA and APPG Submission to Home Office on Covert Surveillance which can be provided on request.

[4] See paragraph 11 for discussion on nomenclature

[5] ICO news blog 20 May 2014

BACKGROUND

5. The APPG was established in October 2012.[6] The APPG currently has five Officers, 20 official members, 10 civil society partners and a range of non-registered MPs and Lords members. The aim of the group is to examine the use of drones by governments for domestic and international, military and civilian purposes. The group uses Parliamentary processes to facilitate greater transparency and accountability on the development, deployment and use of drones. Parliamentarians in all parties have a key role to play in shaping and developing the policy on the use of drones, domestically, internationally and in the application of relevant scrutiny.

6. The level of Parliamentary interest in drones is increasing. To date, Parliamentarians have asked approximately 455 Parliamentary Questions on drones. There have been four debates in Parliament on the subject: two Westminster Hall debates on 6 November 2012 and 11 December 2012 (at the latter, the Minister for Defence Equipment, Support and Technology acknowledged that the debate demonstrated "the increasing interest among not only Members of the House but the public at large about the use of unmanned aerial vehicles"); a House of Commons Adjournment debate on 17 June 2013; and a House of Lords question for Short Debate on 25 June 2013. 3 Early Day Motions have been tabled by members of the APPG, including one on 18 June 2014.

7. The APPG notes that the RPAS Working Group is expected to hold a session dedicated to privacy this term. The House of Lords EU Select Committee has just launched an inquiry into civil use of drones. It is anticipated that EU level work will become increasingly important in considering the privacy aspects of drone use, following the European Commission Communication on 8 April calling for 'tough' new standards on privacy[7]. The APPG shares the Commission's concern that the risk that increased use of drones '*may raise serious and unique privacy and data*

[6] The Group is chaired by Tom Watson MP (Lab); the Vice Chairs are Zac Goldsmith MP (Con) and Baroness Stern (CB); the Treasurer is John Hemming MP (LD); and the Secretary is Dave Anderson MP (Lab). The Group is staffed by a human rights researcher, which is currently funded, primarily by the Joseph Rowntree Foundation. Please see entry on Parliamentary register.

[7] http://europa.eu/rapid/press-release_IP-14-384_en.htm

protection concerns in society and undermine the overall benefits of this innovative technology.'

8. Questions relating to drone use and the need for updated regulation have been raised in a diverse range of topics, from defence procurement to privacy. Four APPG peers, for example, recently tabled amendments to the Defence Reform Bill which included a proposed definition of 'drones': no legal definition currently exists.[8] Others have tabled amendments to the Immigration Bill that derived in part from concern that two former British citizens had been targeted by lethal drone[9]. Several parliamentarians have raised the question of domestic use of unmanned systems in the context of the broader debate on privacy and surveillance in the United Kingdom[10].

9. Members have asked a number of questions specifically about policies on data obtained by public bodies using drones, and whether there are any plans for further national regulation and/or guidance on the privacy aspects of civil drones. The APPG notes the Home Office Answer HC Deb 5 February 2014 c236 to Chair of the APPG in which Minister for Policing and Criminal Justice Damian Green said, '*there are no plans for further regulation of the use of unmanned aerial vehicles for surveillance purposes.'* However, an APPG Freedom of Information Act Request to Sussex police on the Aeryon Skyranger elicited this response: '*the trial will also be considering the need for a separate national policy in relation to data gathered by UAS.[11]'*

10. The ICO is invited to note that the Chair of the APPG sought the expert Advice of barristers Jemima Stratford QC and Tim Johnston 'In the Matter of State Surveillance' in January 2014[12] for APPG members. The front page Guardian article[13] on the Advice indicates a high level of public interest on the overlap between

[8] http://www.publications.parliament.uk/pa/bills/lbill/2013-2014/0060/amend/ml060-I.htm
[9] Bureau of Investigative Journalism (http://www.thebureauinvestigates.com/2013/02/27/former-british-citizens-killed-by-drone-strikes-after-passports-revoked/). Amendments tabled to cl 60: http://www.publications.parliament.uk/pa/bills/lbill/2013-2014/0084/amend/ml084-V.htm
[10] Roger Godsiff MP (Hansard, 10 September 2013 Column 650W), Nicholas Soames MP (16 May 2013 Column 343W), Lord Stoddart of Swindon (Hansard 6 Feb 2013 : Column WA62), Jim Shannon MP (Hansard 21 Jan 2013 : Column 65W), Caroline Lucas (Hansard 3 Sep 2013 : Column 339W)
[11] Letter from Sussex Police dated 2 May 2014
[12] Annex 1
[13] http://www.theguardian.com/uk-news/2014/jan/28/gchq-mass-surveillance-spying-law-lawyer

the surveillance debate and that concerning drone use[14]. The same team of experts have provided the APPG with a further Advice on use of *covert* surveillance drones in the United Kingdom. The Advice was submitted to the Home Office as part of the consultation on Covert Surveillance under RIPA and is available on request. Many of the points made in the Home Office Submission apply to use of overt surveillance drones. Indeed, it may not always be possible to distinguish between 'covert' and 'overt' use, with use on a single mission potentially covering both.

11. It should be made clear that the APPG is not opposed to civil use of drones by Government departments and state bodies. The Group recognises the value offered by drone technology, when used in compliance with domestic and international law[15]. A recent example of this appears to be imagery captured by a drone capture of the flooding in the Somerset Levels (although even this example raises privacy issues with regard to the incidental capture of private information)[16]. Rather, the Group is concerned that developments in drone technology may have outpaced the existing legal frameworks, which were not drafted with innovative technology or the current use of drones in mind. The primary concern is that 'shoe-horning' innovative use of unmanned platforms into older legal definitions risks leaving some privacy aspects unregulated.

NOMENCLATURE

12. The language and terminology that should be, applied to drone technology has become highly politicised. For simplicity, ease of reference and to enable the inclusion of both unmanned aerial and maritime vehicles, the APPG uses the term 'drone' notwithstanding this is not the preferred military or industry term 'remotely piloted air systems', the focus of which is to convey a message that there is a 'man in the loop'. The APPG does not use the term 'drone' in a pejorative sense. It is not right that the word 'drone' implies autonomy, or lethal use. The Group notes that the

[14] although the focus of the Advice was surveillance through intercepted material which may be available for the purposes of extra territorial lethal targeting by the United States

[15] The key human right here is the right to privacy enshrined in international human rights law and incorporated into the domestic legal framework under the Human Rights Act 1998: Article 8 European Convention on Human Rights.

[16] 'UK flooding: special drone captures 360 image of Somerset under water', The Telegraph, 03 February 2014

Government itself, in its responses to Parliamentary Questions, uses a variety of terms to describe this technology including 'remotely piloted aircraft system', 'remotely piloted air systems', 'unmanned aerial vehicles' and 'drones'[17]. The APPG considers insistence that all drones should be called 'remotely piloted aircraft systems' is not helpful in a civil context.

13. The APPG welcomes the identification of four types of drone by the Royal United Services Institute (RUSI) also used by the Defence Committee[18]. The ICO is invited to adopt this model and consider the surveillance capabilities of each type of drone distinctly. They are:

    (a) 'nano' with low resolution image capture such as the Black Hornet;

    (b) 'miniature' offering short range surveillance using small basic sensors such as Desert Hawk;

    (c) 'tactical' a long range endurance drone with medium quality imaging such as the Watchkeeper; and

    (d) 'strategic' large surveillance drone with high resolution synthetic aperture radar and long range electro optical infrared sensors that can cover 100,000km2 per day.

14. The APPG notes that ultimately the Air Navigation Order 2009 will need to be updated to ensure that drones, and the extensive support systems required to support operation, are properly defined. This may help ensure 'drones' are covered in existing regimes which regulate drone use pending comprehensive review; and that the unique features of unmanned systems are not ignored by treating them as if they are traditional manned aircraft. In turn, this may also facilitate the ICO, Home Office and other Governmental departments as they attempt to give proper and distinct consideration to the novel issues that arise in relation to

[17] For example PM used term 'drone' in Ministerial Statement on European Council 6 January 2014: http://www.theyworkforyou.com/wms/?id=2014-01-06a.6WS.1&s=Cameron+drone#g6WS.2

[18] From evidence provided by RUSI to the Defence Committee on 25 October 2013 on Remotely Piloted Air Systems; see Defence Committee report at paragraph 11

drone technology as it develops and is used in increasingly diverse ways.

15. Notwithstanding these observations, the APPG is keen to ensure that the debate on nomenclature does not distract from the substantive issues set out below.

EVIDENCE ON DRONE SURVEILLANCE

16. The APPG has been hampered by the notable paucity of facts in the public domain on state use of surveillance drones (or drones with surveillance capabilities) in the United Kingdom. Meaningful consultation on the Code is difficult without disclosure from Government Departments and other state bodies on past and existing trials, use and proposed use for drones. The ICO is well placed to appreciate that lack of relevant information inhibits oversight and by parliamentarians, and prevents informed public debate.

17. The APPG considers that one primary obstacle to parliamentarians accessing reliable and comprehensive information on drone use by the state is that neither the Home Office, nor any other Government Department, collates the information centrally[19]. The Rt Honourable Damian Green MP explained the position of the Home Office to APPG Chair Tom Watson MP[20]: there is no central collation of information on civilian use of drones. Use of drones is regarded as an operational matter for each chief constable or, presumably, other relevant governmental bodies.

18. The ICO may wish to advise the Home Office on the best way to collate and publish information on civil drone use to promote transparency. This would be welcomed by APPG members and the public, and may help the ICO in formulating relevant policy. The ICO is also well placed to collate and share additional information about data controllers using drones. Part III of the DPA deals with notification by data controllers. Particulars for registration could,

[19] There is no requirement on police forces to report the trialling, acquisition or use of drones: hansard 6 Feb 2013, c62WA

[20] Hansard December 31 October c540W

for example, be extended to include details of type of drone, technical specifications, purpose and geographical area.

19. The absence of any system by which information on drone use is maintained centrally - and made available for scrutiny by members of parliament - is perhaps especially pertinent given the absence of overarching policy guidance from the Home Office on current and planned use of drones by state bodies, officials and others carrying out work for or on behalf of the Department. The APPG considers that guidance on both aspects (operation and use of data), must incorporate analysis of the emerging technical capabilities of surveillance drones. The use of camera, radar, interception or any other surveillance equipment on the drones will define, to some extent, how drones will be used once authorised. The RPAS Working Group is unwilling to share information about its work with the APPG or public, although it is understood that the Group is working toward the development of a 'consistent message' on civil drone use[21].

20. The APPG invites the ICO to note that none of the police forces subject to FOIAs served by the APPG Researcher, which include express request for details of the laws and policies pursuant to which drones were operated, made mention of any of the domestic legislation or any human rights considerations referred to by the Home Office in response to Parliamentary Questions.[22]

21. The ICO may know that the Department for Environment and Rural Affairs ('DEFRA') has recently introduced guidance for staff specifically on the data protection aspects of drone use.[23] Specific guidance has been issued even though DEFRA is not acquiring or using drones directly, or receiving video imagery from drones. The answer helpfully identifies which bodies operate drones and pass data to DEFRA, as well as the types of drone used: two fixed wing Quest 200 vehicles, Flysense Ebee fixed wing, Trimble Gatewing,

[21] The Working Group has refused to disclose information on its current and planned work in an APPG FOIA, June 2014 . However Paul Cremin gave a presentation to the Royal Aeronautical Society on 10 June advising that the Working Group were working to provide a consistent message which would (i) inform RPAS related policies (ii) identify cross-government joined up synergies and opportunities and (iii) identify and address barriers and support the industry

[22] FOIAs sent 2012-2013 so the APPG acknowledges FOIAs sent now may elicit an updated response

[23] House of Commons Debate 20 March column 697W

DJI S800 Spreading Wings, Swinglet and Albotix X6 Hexacopter. The APPG welcomes the lead taken by DEFRA.

22. The APPG acknowledges that the present dearth of information on civil drone use for surveillance may be in part because commercial operators and state bodies are still carrying out basic civil drone trials. The APPG was informed by Gerry Corbett, UAS Lead in the CAA, at a meeting on 25 June he was not satisfied that 'detect and avoid' sensors for drones flown out of the line of sight were sufficiently advanced for safe use. However there is no reason why the public and parliamentarians cannot know which trials are being carried out and why, how the trials are funded and the outcome of each trial as it is completed. The current practice of withholding relevant information impedes scrutiny and the role of Parliament in developing and assessing policy on civil drone use, including the Code and other relevant Guidance. It may also impede the work of the ICO in trying to draft as comprehensive and relevant a Code as possible, and fill any gaps identified.

23. Notwithstanding these limitations, the APPG is aware of the following key facts relevant to this consultation:

    (i) at least 11 state bodies have been authorised to use drones in the United Kingdom according to an APPG FOIA;[24]

    (ii) at least two Government Departments appear to have used drones to gather data (either directly or indirectly). The Department of Transport revealed that the Home and Environment Departments had made presentations to the Working Group on the use they have made of drones[25];

    (iii) there have been a number of ad hoc reports of police and fire services using or trialling drones for

[24] According to an APPG FOIA to the Civil Aviation Authority dated 3 September 2013: Hampshire Fire and Rescue; West Midlands Fire Service; Staffordshire Police; Health and Safety Laboratory; Scottish Environment Protection Agency; Merseyside Police; Essex Police; National Policing Improvement Agency; Police Service of Northern Ireland; BBC (Natural History Unit) and BBC (Research/Development).[24] Note bodies not susceptible to FOIA which may not be listed.

[25] House of Commons Debate 11 Feb 2014 column 525, PQ by APPG Chair. Note Home Office have subsequently made guarded denials that (a) it employs drones: House of Commons Debate 25 Feb 2013 column 292 and (b) it uses data collected from drones to monitor or develop policies: House of Commons Debate 19 March 2013 column 607W

surveillance operations, which have been confirmed in APPG FOIAs. FOIAs have revealed police use includes 'crime scene investigations'[26];

(iv) one police force, Staffordshire, uses a drone for occasional security sweeps and search and rescue;[27]

(v) one police force, Sussex, is currently running a trial[28] to 'monitor a wide area from the sky' in Sussex and Surrey funded by the Association of Chief Police Officers ('ACPO')[29]. The drone used, Aeryon Skyranger, includes high resolution cameras, an integrated imaging payload and software to enable field and office image processing including an integrated tool for 3D visualisation. It can produce real-time digital imagery to any device[30];

(vi) another police force, Kent, has hosted some trial drone flights as part of the 2 Seas project to assess system performance;[31]

(vii) the Northern Ireland Policing Board ('PSNI') have approved purchase of '3 types' of drone to 'support policing' in Northern Ireland. This appears to have started on 13 June 2013[32];

(viii) there are a number of current research projects and development programs, such as those run by Research Councils UK and the ASTRAEA consortium, on a range of potential civil uses which that include

[26] See FOIA from Staffordshire Police which also mentions road collisions and V music festival; Wiltshire Police made use of a drone (UAV) during the Summer Solstice at Stonehenge in 2009; Derbyshire Police used a drone to Red, White and Blue Festival at Codnor.
[27] HL Deb 25 March 2014 c94W
[28] HL Deb 25 March 2014 c94 : a formal date for the trail is in the near future
[29] http://www.uasvision.com/2014/03/13/police-deploy-uas-around-londons-gatwick-airport/
[30] http://www.aeryon.com/products/avs/aeryon-skyranger.html
[31] HL Deb 25 March 2014 c94: Kent are planning to host an event about 2 Seas in July
[32] Response to APPG FOIA from PSNI received 29 July 2013. PSNI declined to answer questions on the number and nature of flights undertaken. Note M15 has primacy over PSNI in national security matters, although there is no publically available information on surveillance drones being available for use by the intelligence services Letters from JA Harris dated 5 March and 10 April to APPG give some information on training of pilots and policy to follow the same standards and processes as CCTV such as destruction after 28 days. Exceptionally the PSNI made reference to Article 8 right to privacy and Data Protection Act. Media reports include: http://www.independent.ie/irish-news/drones-to-work-with-8000-police-at-northern-ireland-g8-summit-29190426.html

security and surveillance. These appear to have some included flights in shared air space[33];

(ix) DEFRA have made use of drones for used unmanned aerial vehicles to support work on flood defence[34];

SCOPE OF DPA AND APPLICATION OF CODE TO OVERT SURVEILLANCE DRONES

24. Under s1(1) the DPA is concerned with the 'processing' of 'personal data.' 'Personal data' means 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 the data by transmission. 'Sensitive' personal information includes personal data consisting of information as to the racial or ethnic origin, political opinions or religious beliefs of the subject, or the alleged commission by him of any offence.

25. The APPG notes that drone surveillance would involve processing personal and sensitive personal data, and that disclosing or sharing that data after it has been obtained should also fall within the scope of the DPA. The ICO is invited to make reference to this.

26. The draft Code extends beyond CCTV use to 'other surveillance camera devices.' The APPG would welcome a definition of those other devices covered. In particular, does the Code cover sensors using portions of the electromagnetic spectrum other than light? The APPG notes that common technology for 'Intelligence Surveillance and Reconnaissance ('ISR') by drone includes use of thermal, infrared and other electromagnetic sensors.

27. At the European Commission workshop on Privacy and Drones (at which the APPG presented, as did Hannah McCausland from the ICO) Professor Paul De Hert correctly emphasised that unmanned aircraft systems were much more than 'flying cameras'. They operate in a 3D space, can access space not otherwise available, and can carry out persistent surveillance using range of

[33] http://www.rcuk.ac.uk/RCUK-prod/assets/documents/submissions/UAVinquiry.pdf
[34] Hansard 25 Feb 2013 Column 284W

electromagnetic sensors. Surveillance capabilities can be directed towards various functions including imagery, 3D modeling, scene management, real-time situational awareness and security patrol.[35]

28. Professor De Hert explained that drone surveillance impacts on 4 aspects of privacy: bodily (biometric data), communications (interception) location and personal data. The APPG agrees. The Group would welcome an analysis of how the ICO considers the DPA and Code applies to each of the 4 aspects of privacy identified. The APPG considers, in line with Professor De Hert's analysis, that the Code does not cover all aspects of ISR and privacy relevant to drone surveillance. The Code's remit is probably limited to overt use of camera-carrying drones insofar as the DPA applies to the particular operation at hand. Section 7.3 of the Code states that drones are 'capable of visual recording.' This should be elaborated, with regard to the 4 types of surveillance drone, 4 aspects of privacy affected and diverse sensors and functions.

29. It is important that these limitations in application of the Code are clearly identified and illustrated by theoretical example in the absence of relevant case work. The APPG hopes that the ICO will make sure that the Code cannot be held out by others as a complete response to the privacy implications of emerging drone technology.

RIGHT OF ACCESS

30. The APPG notes the rights (i) to be informed by any data controller that personal data is being processed and (ii) to access that information under s7 DPA. Surveillance drones raise novel issues which need specific advice in the Code. It is not at all clear how a drone operator might remotely 'warn' his various data subjects that he is processing their personal data. Without advice from the ICO, a data controller might be tempted to ignor this statutory requirement.

[35] FOIA Sussex Police 2 May 2014

31. It is suggested that the ICO may wish to consider prohibitions when the right of access is unworkable, colour coding, notices in public places and use of the ICO and other websites to identify the data controller, drone, surveillance capabilities, area of operation, purpose, policies in place with regard to data and best point of contact. Detailed advice, following consultation with specialist lawyers and technicians is advisable. Where possible, the aerospace industry should be encouraged to develop technologies, such as facial redaction and automatic deletion, with a view making sure processing of personal data is kept to a minimum.

32. The APPG notes the additional requirements of s12 DPA: 'rights in relation to automated decision-making.' A data subject is entitled to ask the data controller to ensure no relevant decision affecting the individual is based on processing personal data 'by automatic means.' As degrees of automation increase within use of unmanned systems, this section may need consideration.

EXEMPTIONS

33. The APPG notes the broad exemptions to the DPA which, it is understood, are generously interpreted by the ICO. The first is national security (s28) A certificate by a Minister is conclusive evidence that the exemption is required for 'the purpose of safeguarding national security.' It is not clear whether there is any restriction on processing, use, retention or sharing of data obtained by surveillance drone once such a certificate is issued.

34. If there is no restriction on processing and use of data falling within a DPA exemption, the APPG has been advised this is likely to amount to a disproportionate interference with the individual's right to privacy: it cannot be held by a public body without restriction[36]. The Advice received by the APPG on the security exemption provided for by s28 DPA, whilst give in the context of covert surveillance, also applies to overt surveillance. If it is the ICO's view that the Data Protection principles should be applied in any event, on a voluntary basis, this should be clearly stated in the Code. This would be consistent with the view that the DPA

[36] Annex 1 of APPG Submission to Home Office on Covert Surveillance

principles represent a 'default' position. Either way, the Code presents an opportunity to at least address shortfalls in connection with retention and sharing of data falling within the remit of the Code.

35. Where data is not covered by the Code, the ICO is invited to make alternative provision, and highlight this need to other relevant authorities[37] and the public, to ensure that drones data is only gathered or shared for a lawful purpose and retained (if at all) for the minimum period possible by all. This would be consistent with the ICO's role and responsibility for promoting and enforcing the Data Protection Act and principles.[38] It is anticipated that the ICO may take a lead role in the introduction of new regulation and guidance in order to fill gaps in the Code and existing surveillance regulation.

36. The APPG suggests that use of exemption certificates (i.e. application of s28 DPA) under s28 should also be reviewed by the ICO[39] if possible. As House debates on the Justice and Security Act demonstrate, the APPG notes diverse use of the term 'national security' and would welcome guidance from the ICO on the scope of s28 insofar as it is or may be applied to use of unmanned (or other) aircraft with surveillance capabilities. The Home Office may benefit from the independent advice of the ICO in this respect.

37. The ICO is invited to pay particular attention to the RPAS Working Group's focus on the increasing shared use of 'RPAS' operations and data between different government departments and bodies[40]. This practice may demand a separate ICO policy or guidance on the sharing of data obtained from surveillance drones (or other aircraft) so that, for example, data obtained for border policing in populated areas can only be shared with GCHQ in defined circumstances and directed towards activities that are lawful in the UK[41].

---

[37] Including the Home Office, Surveillance Camera Commissioner, Interceptions Commissioner, Chief Surveillance Commissioner, Intelligence Services Commissioner and (possibly) the Biometrics Commissioner
[38] Surveillance Roadmap p5 on role of the ICO
[39] HC Deb 10 April 2014 c362: no comment by Home Office on use of s28 exemptions
[40] Paul Cremin's presentation to RAS 10 June
[41] Jemima Stratford's Advice January 2014 on sharing of data for the purpose of unlawful targeted killing abroad

38. S29 provides an exemption for processing personal data for inter alia the prevention or detection of a crime. The increasingly advanced technical capabilities of surveillance drones - which can persist over densely populated areas for long periods in a semi-covert manner - raise new questions. For example, the Aeryon Skyranger drone trialed by Sussex police is aimed at airport security but used more widely in both Sussex and neighbouring Surrey.

39. The Skyranger includes a camera with thermal imaging payload designed for night time tactical surveillance[42]. The camera produces high resolution imagery which can probably identify individuals (at least when combined with other data). This raises the question: does s29 apply to detection of any crime as a result of general observation during the trial? For example, if a camera and ANPR system identifies a car jumping a red light, what will happen to that data? Or could a suspicion that an individual might be planning a crime in any circumstances justify persistent surveillance over a well-attended London mosque at Friday prayer time, if frequented by that individual? What threshold or procedure applies to use of advanced airborne cameras for crime detection in these circumstances, including the incidental processing of data? These are difficult questions. They demand comprehensive assessment and review.

40. S32 provides a broad exemption for journalism, where the processing of data is undertaken with a view to the publication of any journalistic material, and the data controller reasonably believes publication would be in the public interest. The APPG is concerned about how this exemption might be used in practice, noting the conviction this week of Andy Coulson. The privacy implications of an organization such as News International being licensed to use a civil drone for 'journalistic material' may be profound. The APPG suggests that the ICO build on their relationship with the Civil Aviation Authority and request monthly update on which bodies have been licensed to use civil drones under the Air Navigation Order 2009. Use of drones by group and purpose, including the media, should be kept under close review.

[42] http://www.aeryon.com/products/payloads/thermal-imaging-flir.html

ENFORCEMENT

41. The DPA provides for some enforcement measures, including enforcement notices (s40) and monetary penalties (s55). It is understood that the primary function of the ICO is to provide advice and support rather than enforcement, which appears to be reserved for 'serious' cases. Fines of up to £500,000 are for serious breached of the DPA (or Privacy and Electronic Communications Regulations). As civil drones are used more frequently, APPG members may expect to see increased use of s41A assessment notices served on data controllers. This will help the ICO determine whether the DPA principles are being properly observed by data controllers using drones in civil airspace for the first time. It may also be necessary to carry out a comprehensive review of the privacy implications of drones operating in the UK; and assess the effectiveness of the revised Code.

42. It is suggested that the ICO add a section in the Code on enforcement measures, including use of s41A notices, which may be applied to innovative uses of new technology including drones.

CONCLUSION

43. The draft Code is a welcome start in considering the complex privacy implications of use of drones in civil airspace in the UK. However, a revised Code cannot be seen as a substitute for (i) comprehensive review of the privacy implications of drones and (ii) overarching national regulation and/or a policy on collection, storage and use of 'drones data.' It appears form the FOIA from Sussex Police on 2 May that such a policy is now under consideration. The APPG supports this initiative.

44. It is anticipated that civil use of drones including many camera-carrying drones may significantly add to the workload ICO. The APPG is likely to support an increased remit, with increased funding, for the ICO so that the ICO can supplement the Code and proactively review and regulate increased use of surveillance drones, continuing to uphold information and privacy rights. Pending new regulation, (probably initiated by the European

Commission) the APPG encourages the ICO to appoint a specialist drones or UAS officer to devise a new national policy on collection and use of data obtained via surveillance drones, actively advise and regulate data controllers, and liaise with public bodies about relevant responsibilities. The APPG would welcome increased dialogue with the ICO on this.

45. The APPG notes that the Defence Committee's report, published 25 March 2014, calls on the Ministry of Defence (MOD) to formulate and set out its policy on the military use of remotely piloted aircraft systems (RPAS) no later than September 2014.[43] Many points made in the Defence Committee Report on the need for transparency, accountability and a clear policy apply equally to civilian use of drones in the United Kingdom. The APPG hopes that the ICO will encourage the Home Office to adopt this model and publish a high level overarching policy on use of drones and drones data, including for those used for surveillance, within the same time frame.

46. The APPG Submission on Covert Surveillance suggested that the Home Office voluntarily report to parliament on civil use of drones by departments, public bodies and agencies. This recommendation is repeated: it should apply to use of covert, overt and combination surveillance drones. It is hoped that the ICO may support the APPG's request.

47. The ICO is also well placed to advise the Home Office on disclosing information on civil drone use, and to directly seek additional material from data controllers. It is hoped that as much material as possible will be available for publication or through Freedom of Information Act requests. This would significantly increase public confidence in Government use and oversight of this new technology.

[43] http://www.parliament.uk/business/committees/committees-a-z/commons-select/defence-committee/news/remote-control-rpas-substantive/.

This submission is made by the following named officers, on behalf of the All Party Parliamentary Group on drones:

Chair: Tom Watson MP (Lab);

Vice Chairs: Baroness Stern (CB); Zac Goldsmith (Con);

Treasurer: John Hemming MP (LD);

Secretary: David Anderson MP (Lab).

For any further information, please contact the APPG's Researcher Anna Thomas on anna.thomas@parliament.uk