



OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

ICO25 Consultation Team
Information Commissioner's Office

By e-mail

26 September 2022

Dear ICO25 Consultation Team

ICO 25 Consultation

I am aware that your consultation closed on 22 September. My Office was only able to provide a partial response to your online consultation owing to the constraints of space within your online questionnaire.

As discussed between our respective offices, there are some important areas that I would like to respond to more expansively as described in the plan 'The ICO's Purpose, Objectives and Performance Measures' and we have agreed it would be helpful if I record them formally here.

The following comments are relevant to Question 5. of your consultation:

The exponential development of biometric and surveillance technology has a direct impact on the use of personal data. However, all too often, legislative frameworks seeking to underpin its use by both public and private sectors have lagged behind the technologically possible, which has in the recent past resulted in the deployment of new technology before the legal, ethical and societal considerations have been fully understood. Sometimes this has invited formal legal challenge and it has certainly attracted questions and concern. For many organisations and sectors, the lack of specific guidance has inhibited planning and investment in new and emerging areas which has probably reduced the uptake of opportunities to

support investigations and prosecutions that are becoming increasingly available with new technology. While it would be difficult to compile reliable evidence of this particular ‘chilling effect’, anecdotal evidence strongly suggests that this is the case.

The Data Retention and Digital Information Bill seeks to reform the oversight landscape for biometrics and surveillance technology so far as it applies to policing and local authorities, and is based on the premise that public space surveillance is simply a subset of wider data protection and privacy. If Parliament accepts that premise, the ICO as the UK’s data protection authority will be expected to step in to fill the gap, not only where matters would otherwise fall to the Surveillance Camera Commissioner and compliance with the Surveillance Camera Code, but also where far wider gaps in the current arrangements have left the most prolific users of public space surveillance systems (transport, hospitals, universities and even central government) without specific regulation. It seems to me that the ICO will need to work quickly and proactively to identify the relevant and material uses of personal data in biometric surveillance and provide practical, timely advice on their lawfulness in light of requirements under the relevant legal framework. While the State’s use of biometric surveillance technology plainly engages individual data rights, it is well documented that some of the key issues giving rise to public trust and confidence considerations go beyond data protection and therefore, by extension, beyond the current remit of the ICO.

The ICO states that its purpose is to *empower you through information*, and two of the four ways in which it states it will achieve this are by *empowering your organisation to plan, invest, responsibly innovate and grow*, and *promoting openness and transparency by public bodies*. The acid test for this strategic ambition will of course be the extent to which these votive statements are corroborated by tangible, measurable evidence.

It is pleasing to hear of the ICO’s plans to produce guidance on biometrics for general processing under Part 2 of the Data Protection Act 2018 (DPA), which it is hoped will be of great use to both developers and users. Careful thought must also be given to putting in place guidance for specific data processing under Parts 3 and 4 (and also Schedule 14) in respect of both policing and law enforcement (the difference being important in this context). In all aspects of public space surveillance it will be important to ensure that those deploying new technology in order to prevent and detect crime and keep their staff, partners and the wider

UK safe have clear guidance to underpin these deployments in order that they can '*plan, invest, responsibly innovate and grow.*'

Biometric capability in its widest sense could revolutionise the investigation and prevention of crime and the prosecution of offenders. At the same time, the manner in which that technology is used could jeopardise our very model of policing. Its future regulation and oversight ought to reflect both its potential and its risk. If we are to get the most from biometric surveillance technology, it will need a *systemic* approach to regulation focusing on the integrity - of both technology and practice – along with clear standards for everything and everyone involved because, in a systemic setting, compromising part means compromising the whole.

There is a risk that if the ICO does not fulfil its purpose of identifying trends around new uses of personal information, and subsequently providing certainty around the use and sharing of related personal information, the *responsible innovation* it seeks to empower in the organisations under its regulation will be stunted. The importance of individuals being able to access and understand the applicable law and arrange their behaviour accordingly in order to comply or attract the appropriate penalty is a fundamental concept in the rule of law. Arguably this ability to access, understand and arrange their affairs accordingly is equally important in this field to organisations particularly if they are to be able to *plan, invest and innovate with confidence*, where there is a real risk of legal challenge against the use of innovative tools. This is particularly key in the increasingly linked fields of biometrics and surveillance camera technology.

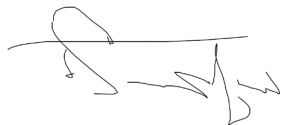
Of course, all of what is set out in ICO25 requires staff to do it, particularly where there are new areas to be understood before a decision can be made by ICO whether it is an issue for them to address in the first place. One of the behaviours in ICO25 is that, as an organisation, ICO is *curious*: this is an important trait to have, particularly if ICO is to get the grasp of issues in the way it states it will. Experience indicates the necessary resource simply does not exist, and that existing staff are already spread across more subject areas than capacity can accommodate. This leads to pressing subject areas being 'parked', with insufficient time to dedicate to considering some of the trending areas that fall within the data protection remit, and the expertise of the ICO not being available to users in the timely manner needed. The

ICO states the organisation wants to be *selective to be effective*, to enable the organisation to *fix things in ways which are timely and relevant*, and it needs to be sufficiently resourced to be able to get across the new policy areas that will fall to it, particularly those coming as a consequence of the abolition of the roles of the Biometrics and Surveillance Camera Commissioner.

It is vital that people have confidence in the relevant technology doing what it is supposed to, and that means the whole ecosystem of surveillance cameras and biometrics, not simply novel offshoots of it. More practically, it also means having equal confidence that the operators of those systems are doing what *they* are supposed to do; it means understanding the purposes for which the technology is being used, who authorised it and how they arrived at their decision that it was lawful and proportionate to do so in each case. And finally it means having clearly defined, published, accessible and intelligible policies publicly setting out the parameters, policies that will be regularly reviewed in light of experience.

Thank you for taking this addendum into consideration after your official closing. I and my Office stand ready to engage in any follow-up discussion that may be of assistance.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Fraser Sampson', written over a horizontal line.

Professor Fraser Sampson
Biometrics and Surveillance Camera Commissioner