Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Written evidence submitted by The Information Commissioner (OSB0210)

Damian Collins MP
Chair
Joint Committee on Draft Online Safety Bill
House of Lords
London
SW1A 0PW

Our reference: ICO/O/ED/L/RFM/0314
By email to: jconlinesafetybill@parliament.uk

26 October 2021

Dear Chair,

RE: Follow up to ICO's oral evidence session

I recently provided oral evidence alongside my executive director Stephen Bonner on the aspects of the Online Safety Bill (the Bill) of interest to the ICO. Your committee also showed interest in hearing more about the ICO's experience of regulating digital and online service providers, and I agreed that I would write to provide more detail.

ICO interest in the Bill

Digital regulation cohesion

As noted during my oral evidence, the ICO recognises the clear links between regulatory remits as online activity – commercial and otherwise – expands. There are strong arguments for regulatory cross-awareness and collaboration where those links, if unaddressed, could lead to gaps in supervision. The ICO has enthusiastically and methodically begun to map those links and concern areas via both our bilateral relationships with other UK regulators active in the digital space. And, more formally, via the establishment and setting of a workplan for the Digital Regulation Cooperation Forum (DRCF) that brings together the ICO, Ofcom, the Competition and Markets Authority (CMA) and the Financial Conduct Authority (FCA).

The DRCF is a regulator-driven effort; and as such is non-legislative in its nature. I am on the record as having said that there are potential barriers to our cooperation and joint working as digital regulators. One way in which this could be addressed is via a duty in legislation to pay regard to one another's regimes. I believe that embedding this duty in our respective underpinning legislation would bolster confidence in the cohesiveness of the UK's digital regulatory system. Organisations would enjoy clarity on how regulators would be expected to treat a situation where there is interplay between regimes supervising the same organisation but from different regulatory angles.

Clarity on regime overlap

It is fair to say that when it comes to online regulation, the ICO has relatively greater experience due to the nature of how our data protection legislation works. In short, our law follows the personal data, regardless of where it is used. The medium-blind, platform-blind definition of personal data means that there is no ambiguity over the ICO's relevant interest in online activities that pivot on the processing of a person's information.

As I noted to the committee, the public have a history and expectation of the ICO being their complaint route when they encounter an issue with how their data has been used. This includes of course the public's concerns with how their data is used by online services. The ICO has had a number of previous high profile cases where we investigated the data processing practices of online services. However the larger proportion of our cases involving online services have been individual complaints that have not necessarily resulted in major fines or enforcement action. This does not in any way diminish the validity or significance of those complaints however. Every complaint upheld by the ICO is an important recourse outcome for a real individual. Our track record on data protection regulation online is therefore one of both high profile ecosystem-level investigations and one of reassurance for individuals who have grown used to coming to the ICO for recourse.

This cuts to the primary point of concern for the ICO in the Bill as currently framed. When it comes to matters relating to privacy and data protection in an online context, as covered by the Bill, I believe it is crucial that the ICO is clearly identified as the lead regulator for these concerns. The public have grown accustomed to the ICO having the capacity and power to engage on their behalf when an online data concern arises. I understand the desirability to wrap online issues up in the Bill in a neat way, with issues across all areas directed towards Ofcom. However, I believe the benefits of this approach would not outweigh the risks in creating a real or perceived separate oversight regime for data protection concerns arising in an online context only. We remain engaged with Government on this issue and are confident that a resolution will be forthcoming.

Audit powers

The committee was interested to hear more about the ICO's audit capabilities, which I described as granting me the ability to look under the bonnet of a data processing situation.

The ICO's audit powers are wide-ranging, are either consensual or compulsory, and may be deployed in an ex-post and ex-ante manner.

Ex-ante and ex-post audit

From an ex-ante perspective, this means that the ICO may examine the practical processing activities underlying a new data-centric service if we have sufficient concern that such processing would create risks. This allows the regulator to ask the right assurance questions at the outset of a plan to process personal data, and examine how that initial data is thus processed. This kind of intervention has a strong protective role in identifying risks and harms to which the public might otherwise suffer.

From an ex-post perspective, the ICO can often recommend audit activity as a complementary action to an enforcement notice. An ICO enforcement notice can demand steps are taken by an organisation to remedy their non-compliant data processing activities. However, without sufficient audit powers, the ICO would have to rely solely on assurances from that organisation that their practices had improved. Instead, the ICO can seek its own assurances that an enforcement notice has been complied with by directly auditing the current practices in an organisation.

The majority of the ICO's audit activity however takes place where we have concerns about ongoing data processing – often via individual complaints, breaches or media reports – but the threshold for taking immediate enforcement action has not been reached. In such cases, we can undertake an audit to evaluate the data protection compliance of an organisation; if our audit raises concerns then this may lead to a subsequent enforcement notice. The ICO's work on auditing data brokers' compliance both led to enforcement action arising from audit findings.

I believe the deployment of audit powers as a check against compliance with a notice to improve data practices, is an important examination tool for the ICO; whilst proactive audits based on concerns also provide a level of consistent assurance for the public that improvements have been made by an organisation to the extent expected by the independent regulator.

Scope of audit power

The wide-ranging nature of the audit powers means that the ICO can:

- Enter a physical premises where data is being processed;
- Expect to be assisted by staff on site in premises to help identify the data processing activity to be assessed;
- Seek explanations from staff on what information or documents are and how they relate to the data processing activity being assessed;
- Examine not just information but the equipment which processes that information;
- Examine the processing of data in remote locations outside an organisation's own premises, e.g. data held on a cloud server;
- Invoke an urgency provision when the need to audit a data processing situation is time-sensitive to protecting individuals from data risks.

Benefits of an audit

Whilst an audit is a formal regulatory activity, consensual audits are a useful tool which the ICO can provide upon request to certain organisations' processing activities. As well as providing a supervision role and a public protection role, audits have spin-off advantages for both the ICO and those organisations assessed:

- An ICO audit can help raise awareness in an organisation of the importance of data protection, cyber security and general information security and the need to account for the risks arising in those areas. This can have an important galvanising effect for embedding good practices into the future.

- Submitting to a consensual ICO audit indicates that an organisation recognises its data protection obligations and has an active interest in benchmarking its data processing activities against both baseline compliance and best practice.
- Collaboration between the ICO's audit staff and an organisation's data innovators can lead to pragmatic and novel understandings of the data protection implications of a new technology or new business model, with an opportunity to make privacy-friendly alternative choices.
- Close engagement on an audit enriches the ICO's subject matter expertise and allows for more effective and quicker reaction by the ICO if something goes wrong in future.

Oversight and due process

The ICO's audit powers are deployed via formal assessment notices; the format and content of the notices are laid down in legislation in the Data Protection Act 2018. This includes a requirement for the ICO to be specific about the concerns it has about the data processing being undertaken and provides a number of important exemptions such as for legally privileged material. This provides organisations with a level of certainty and clarity over how they are being supervised by the regulator.

Like other ICO notices, an organisation served with an assessment notice may appeal the notice via the Information Tribunal. ICO audits can occasionally be urgent in nature, and thus an appeal to an assessment notice may introduce a critical delay to the audit process. However in the case of an urgent or 'no notice' ICO assessment notice, we may still go ahead with an urgent audit even if an appeal has been lodged and prior to it being heard.

The ICO recognises the public interest, by both individuals and other similar organisations, in audit outcomes. The ICO adopts a transparency by default approach to its audit work, with post-audit reports proactively published on our website. Where audit activity is particularly high profile, such as our work examining charity fundraising practices and political party campaigning, we work to make our findings accessible and relevant and proactively notify interested parties such as parliamentary committees.

Relevance to online regulation

Online activity has advanced rapidly in recent years, and every regulator is working hard to keep pace with ever-evolving technologies. Audit powers have been beneficial to the ICO in this online context by allowing us to scrutinise in real time the data processing in a new technology or business model. The ICO's understanding of the often complex web of data relationships in an online business model has been greatly enriched by our in-situ audit activity. This includes having an audited organisation's staff talk us through the data life cycle in a way that allows us to map those processes to the established lexicon of data protection legislation.

Despite the novel technology involved, audit scrutiny often reveals that the underlying data protection risks in online services are no different to those risks found offline. Poorly protected back door access to information; lack of staff awareness of data protection obligations; and failure to slow

down a new product deployment until data concerns are properly mitigated – these risks may now arise in a cloud processing context rather than an organisation's own local server room.

The ICO's breach reporting statistics back this finding up, with most breaches – across both high tech and low tech organisations – still falling into the three scenarios identified above. Organisations still require regular reminders to address these basic risks; not doing so can have serious detrimental effects on the public. The ability to audit online organisations, and to challenge their staff to explain to the ICO how the data risks we identify during an audit have been accounted for, is crucial for public trust in the data protection credentials of online services.

It will be important for the coherence of, and confidence in, the UK's online regulation regime that all regulators have sufficient powers within their own necessary contexts to properly identify for themselves in a first-hand manner the risks within supervised organisations. Whilst the audit powers in the Data Protection Act suit the ICO's needs from a data protection perspective, other regulatory regimes will have different needs in terms of how they go about securing that first hand assurance.

End to end encryption

During my oral evidence, the committee were interested in the role that end to end encryption (E2EE) can play in online services. The ICO has been thinking carefully about E2EE from our particular regulatory perspective. To assist others in their own understanding, the ICO has produced a policy position paper setting out our views on E2EE. This does not form binding regulatory guidance and has no formal status in any specific case we may examine. However it does set out our initial starting point on how we think about E2EE within our regulatory remit.

I think this represents a useful proactive regulatory intervention, to provide a starting position for others that can then evolve and adjust over time as others articulate their own positions and seek greater clarity on the ICO's view. This paper is currently being finalised and I will send to the committee once completed.

Yours sincerely,

Elizabeth Denham CBE
UK Information Commissioner

27 October 2021