Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

ICO response to OFCOM consultation on Draft Initial Obligations Code. Submitted 30 July 2010.

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998, the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications Regulations. He is independent from government and promotes access to official information and the protection of personal information. The comments provided by his office in response to this consultation are focussed on ensuring that any approach to tackling the problem of online infringements of copyright is compliant with data protection legislation and is compatible with the rights of individual subscribers.

The points we make focus only on those areas that are of direct relevance to our role.

We welcome the requirement to provide a statement of compliance (3.5.6 and 4.5 of the code) and the intention to ensure that a copyright owner gives assurances to Ofcom that data protection law has been satisfied before submitting their first Copyright Infringement Report (CIR). This provision is a reminder to the copyright owner of their obligations under the DPA and should help to focus their attention on complying with the Act but the statement of compliance will not of course, provide an indemnity for the copyright owner if they have breached Data Protection law. The same goes for ISPs undertaking subscriber identification.

However, it is important for all those subject to the Code to remember that regardless of their duties under the Code, compliance with the DPA98 and PECR is a legal requirement – the existence of a statement of compliance and the fact that a quality assurance process exists is not enough to guarantee that compliance. We would like to be assured that there will be sufficient scrutiny of these statements and that rigorous processes will be in place to check that all parties subject to the Code are fulfilling their data protection obligations.

We would expect that statements of compliance with data protection laws should be more than simply a bland assertion that a company is complying with the law. They should instead set out in detail the measures in place and the analysis undertaken to demonstrate that the rights holder or the ISP is adopting practices that place privacy at the centre of their efforts to comply with the Code. Our experience shows us that transparency and openness can often assist in protecting individuals' privacy so we wonder how far the rights holders and ISPs might be encouraged to demonstrate their commitment to upholding information rights by making public the steps they are taking in this regard.

Rights holders will need to be reminded that they will remain responsible for the information gathering processes of those acting on their behalf as data processors. Even where no such controller-processor relationship exists, holding personal data collected unlawfully outside the UK might still raise issues of compliance with UK law insofar as it is held by a data controller established in the UK.

The Quality Assurance process does appear to allow for OFCOM to intervene but we wonder how far the data protection elements of the report might be opened up to audit by the ICO and how far the report as a whole might be scrutinised for compliance on an ongoing basis.

We recognise the benefits of the proposed system but it stands or falls on the willingness of all parties to engage in meaningful debate over whether the factors included in a statement of compliance are sufficient to protect the rights, freedoms and legitimate interests of individuals. We would welcome further involvement in this aspect of the Code.

The 'data quality' principles of data protection require that personal data is kept accurate and up to date. This is especially important in the context of identifying subscribers following receipt of a CIR. Poor practice in gathering information about potential infringers and poor standards in terms of linking a CIR to a subscriber is likely to lead to unjustified intrusions into the private lives of individuals who are not responsible for any copyright infringement. Clearly, the process by which an ISP links a report to a subscriber will be crucial in terms of fulfilling the fairness requirement of the first data protection principle – processing personal data to inform someone in error is unlikely to be fair and we would expect ISPs to take a cautious approach.

In previous responses to consultations on this issue, we have pointed out the importance of recognising that the data used throughout the reporting and notification process is likely to be personal data insofar as it relates to an individual subscriber. The consultation document makes it clear that in order to take legal action against those infringing their rights, copyright holders will often seek to relate the IP address allocated to the uploader to an actual person and physical UK address. While we welcome the safeguards brought about via the need to seek a court order, this does not remove the need for careful consideration of data protection issues.

In June 2007 the Article 29 Working Party, an advisory committee composed of the European national data protection supervisory authorities, agreed an opinion on the concept of personal data which established that in many contexts IP addresses are personal data and should be treated as such. This view is consistent with the guidance issued by the Information Commissioner on 'Determining What is Personal Data'.

It should be clear that where IP addresses collected by a rights holder are combined with the customer details held by the ISP with the aim of establishing whether copyright has been breached by a particular individual then the IP address is being used to learn record and decide something about a particular individual. It is therefore equally clear that the IP address is personal data. The Data Protection Act 1998 (DPA98) and the Privacy and Electronic Communications Regulations 2003 (PECR) are engaged

It is apparent therefore that the use of personal data to identify and prosecute infringers will rely on the processing of personal data and the ICO's aim in entering this debate is to ensure recognition that any response to the problem of illicit sharing should be proportionate and lawful and have proper regard to the rights of individuals.

We have said before that simply because privacy legislation is engaged does not mean rights holders cannot act to protect their legitimate interests. The DPA98 does not prevent the disclosure of personal data where to do so is fair, lawful there is a sound basis for making the disclosure. Certainly, where a court orders the disclosure of personal data to a rights holder, the DPA98 would not prevent this disclosure being made.

However, as a data protection authority we must point out the privacy risks of unfettered sharing of data where no justification for the sharing is apparent; we must do this even as we argue that the legislation we enforce does not preclude legitimate disclosures. We would argue that users have a reasonable expectation of privacy in the context of whether their ISP should disclose data to third parties even while we recognise that the 'reasonableness' of this expectation changes according to time, technology and context. A 'serial' uploader who is well aware of the illicit nature of his activities clearly has limited scope for arguing that his rights have been infringed in the event that a rights holder links his IP address with illicit activity and his ISP complies with a reasonable request from that rights holder. But large scale intrusion into the private lives of users is not a fair or proportionate response. To avoid such disproportionate intrusion we would welcome the opportunity to engage with OFCOM, rights holders and ISPs to provide direction on how best to comply with their obligations as set out in the Code while also complying with the legislation enforced by the Information Commissioner.