



Information Commissioner's Office

The Information Commissioner's response to the transparency section of the Home Office business plan

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) welcomes the opportunity to comment on the transparency section of the Home Office business plan. In this response we have focused on the broad issues of promoting transparency and the need to consider data protection and privacy implications rather than providing detailed comments on the proposed input and impact indicators.

Right to data

The Information Commissioner welcomes the government's proposals to create a new 'right to data' and the proactive steps many government departments have already taken to identify and publish datasets. He will be responding in more detail to the government's proposals once legislation has been published. The Commissioner believes that publication schemes, as set out in section 19 of the Freedom of Information Act, are an important mechanism for implementing a 'right to data'. The Commissioner plans to consult with government departments about revising the definition document for central government publication schemes during 2011. Departments are advised to start thinking about possible ways publications schemes could be revised.

The Information Commissioner also wishes to stress the importance of considering privacy impact assessments for the disclosure of datasets that may contain or relate to personal data. In some cases there will be a risk that disclosure may lead to direct or indirect identification of individuals. In many cases privacy friendly solutions can be found that still offer key transparency benefits. This may include techniques such as using blocks and zone on maps rather than "pins", providing partial postcode data or applying statistical techniques to area level statistics. Government departments should also

consider a joined up approach to the risks of identification via data aggregation of several datasets.

Crime data

The Information Commissioner supports the Home Office's commitment to provide greater transparency on local criminal activity and anti-social behaviour. Using techniques such as crime mapping can be an effective means of letting people know what crimes are taking place in their local area but care needs to be taken as this can potentially have an impact on the privacy of individuals such as victims or witnesses. The ICO is pleased to have had the opportunity to provide advice to the Home Office about the privacy implications of the crime mapping project and that our advice has been incorporated into many of the safeguards that have been put in place. It will be important that this initiative is reviewed to ensure that the privacy safeguards are effective in practice.

The Home Office has given a commitment in the business plan to release data proactively at the lowest level of aggregation appropriate for each dataset. The publication of crime data online, whether through crime mapping or the release of raw data sets, is a fairly new development and technological advances have meant that it is developing rapidly and the impact that the release of crime data may have on an individual's privacy has not been properly explored as yet. While welcoming greater transparency, we think care needs to be taken as this can potentially have an impact on the privacy of individuals such as victims or witnesses and in turn engage concerns about compliance with the Data Protection Act and Human Rights Act. We encourage the use of privacy friendly options that reduce the risks of identifying individuals, for example by providing partial postcode data and banding together certain categories of crime, rather than identifying crime locations at places owned or occupied by individuals.

It is not yet apparent how the release of detailed crime data could be exploited and indeed what the public perception is or will be once it is seen how the information can be re-used. Undertaking a privacy impact assessment will help resolve such concerns. There is also very little evidence about public sensitivity and attitudes to privacy in respect of the publication of data about crime. Therefore we would encourage the Home Office to work with victims groups and others to develop a clearer picture of public sensitivity and perceived privacy risk in this area.