

TRANSPARENCY: SEEING IT THROUGH

Christopher Graham 28.09.11

Today is International Right to Know Day. To mark the occasion, as United Kingdom Information Commissioner, I want to offer a view on the state of information rights here in the UK: the right to know and the right to privacy. I want to set out how the Information Commissioner's Office – the ICO - is already a key player in delivering an effective Right to Know; that our responsibility for both the right to know and the right to privacy equips us to assess where the public interest lies; and that the ICO can and should be an essential partner in delivering the much trumpeted transparency agenda – in seeing it through to practical reality.

Information is the currency of democracy. Whoever first said that, Thomas Jefferson or Ralph Nader, was stating an important truth. Freedom of Information widens and informs public debate. It can contribute to the development and execution of policy generally, as well as in specific high priority areas such as health and safety or the environment. The right to know underpins the accountability of public servants. It exposes waste and drives efficiency. It opens up possibilities for different approaches to service delivery. It's certainly a challenge, but then it's meant to be.

The Information Commissioner's Office has a Mission: to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. We enforce the Freedom of Information Act, the Environmental Information Regulations, and INSPIRe, the regulations concerning spatial datasets for the development and monitoring of environmental policy and practice. That's all about the right to know. But we also enforce the Data Protection Act and the Privacy and Electronic Communications Regulations. That's the right to stay in control of your personal information and require those who process your data to be transparent about what they are doing with it.

Transparency involves the right to know, tempered by the right to privacy. And that's the business we're in, here at the ICO. So, naturally, the ICO is already very much involved in delivering transparency.

What do we do to assert the right to know? There are our Decision Notices under the Freedom of Information Act, ordering public authorities to publish specific information requested under the Act. Some very significant rights, rights that perhaps we now take for granted, were won by the operation of the Act. For example, it's now routine to access the MOT pass/fail data by car manufacturer and model. But it took a ruling by the Information Commissioner in 2009 to put that vital information into the public domain. Recent decisions have concerned the salaries of some senior civil servants who had previously declined to allow their details to be published. We ruled that the public interest required publication. We also ruled that cabinet materials about the Hillsborough football stadium disaster should be made public. Again, we judged it was in the public interest.

Then there are the Publication Schemes under the Freedom of Information Act. These specify the classes of information that public authorities should be publishing proactively. If they don't, they are in breach of the law and the Information Commissioner can take enforcement action.

We publish guidance through statutory codes of practice. We recently published our Data Sharing Code of Practice. This shows how organisations can legitimately share data in appropriate circumstances, provided they have thought through the privacy implications. Many people think that data protection exists just to stop people doing things. Our Code shows that that's just plain wrong.

We also take action in cases of the unlawful disclosure of personal information, often involving blagging information from unsuspecting staff. We believe there needs to be a stronger deterrent to the unlawful trade in personal data, however acquired. The matter

is urgent, not least, as the previous government pointed out as long ago as 2006, to build public confidence in transparency and open data. If you want to reassure the public that datasets can be published and data shared without endangering legitimate expectations of privacy, you have to demonstrate that there are effective sanctions against misuse. It's a highly profitable business. We have to make it not worth the blaggers' while.

Just now, there's a lot happening on the right to know front. There's a drive for greater accountability. The government is consulting on their transparency strategy, 'Making Open Data Real'. The Open Data initiative is about accessing information in usable, mashable formats, making it possible to analyse, compare and create. And next there's to be a process of post legislative scrutiny of the Freedom of Information Act. After almost seven years experience, how's it all going?

The ICO welcomes the emphasis on greater transparency in public policy, and we certainly support the direction of travel. New technologies enable a bolder approach to the right to know. In fact, they demand it. It is vital that the freedom of information regime responds to the new demand for information online – and, in particular, the demands of those who can innovate with data. Web 2.0 demands a 2.0 freedom of Information regime – and an ICO 2.0 as well, for that matter.

But the right to know isn't just about the proactive publication of datasets and other structured data. The disclosure of unstructured information (emails, memos, reports, policy documents) is also vitally important in delivering accountability and holding public authorities to account. In other words, transparency is not just about what the authorities choose to reveal to citizens; but what citizens have a right to ask to see, and the authorities may have an obligation to publish, depending on the circumstances, however inconvenient that may be.

It follows that it is also vital that this unstructured information is subject to proper records management. And the citizen's ability to obtain information and hold public authorities to account mustn't be weakened as models of service delivery change. Contracting out and the involvement of new providers from the private sector, charities or the third sector generally must reduce neither the citizen's right to know nor the accountability of public services. Transparency and accountability are supposed to be transforming public services. It would be perverse if the transformation of public services resulted in less transparency and less accountability.

We also need to ensure that there is no gap between the right to know rhetoric and the reality of a 'don't tell 'em' mentality that all too frequently frustrates the citizen.

Public bodies proclaiming pro-active transparency shouldn't be so coy about revealing what individual citizens may want to know.

Organisations promoting accountability need to be better at processing day-to-day information requests.

And public authorities using Twitter and Facebook to engage with citizens cannot complain when citizens use the same new media to submit FOI requests.

There's a key role for the ICO's statutory Publication Schemes to play in delivering transparency, even under current, un-enhanced FOI legislation. Today, I am announcing how we intend to revise our approach to Publication Schemes in the light of developments in the transparency and open data agenda. We are launching a consultation on how the ICO could improve the existing approach to Publication Schemes. We will want feedback, not just from Public Authorities but from members of the public as well. Our questions will include: What further classes of information or further detail can be included in Publication Schemes? How should Publication Schemes evolve in the light of web 2.0? Is our approach of one model scheme and sector based guidance appropriate?

Of course, we will, the while, continue to promote and monitor compliance with the requirements of the existing statutory Publication Scheme framework, taking regulatory action as appropriate.

What of the interface between competing rights? Which takes precedence: the right to know? Or the right to privacy? How is the balance to be struck? Just saying there's a balance to be struck between different rights - the right to know or the right to privacy - or different policy imperatives, for example, national security - just saying there's a balance, doesn't itself strike the balance. The decisive factor must always be a sober assessment of the competing interests, both public and private. And these have to be assessed on a case by case basis.

As I said earlier, there's a common assumption about data protection - and it's wrong. Too often the assumption is that the Data Protection Act is there to stop things happening. In fact, it's there to enable positive developments to happen, but to happen with due attention to relevant privacy considerations.

There's certainly a public interest in privacy for individuals as well as in transparency around public information. But privacy shouldn't always be claimed as a barrier to transparency, accountability or open data. The ICO will continue to issue and update guidance about privacy risks to help public bodies make the right decisions. We are also developing a Code of Practice on anonymisation under section 51 of the Data Protection Act, and we will publish broader guidance on key privacy principles that apply to dataset disclosures.

We welcome the approach of the recent O'Hara report which argued for better decision making processes around dataset disclosures involving privacy risks. Here you're going to see an ICO operating as educator and enabler as well as enforcer. And we've already taken steps to beef up our research and technical knowledge, as the report recommends.

So we're doing our bit to respond to the challenges of transparency and Web 2.0. We can be effective partners in delivering the benefits, and we are engaging with different Whitehall Departments and the devolved administrations.

What is needed is a joined up and consistent approach to the different strands of transparency policy across government. There is perhaps a good case to be made for a co-ordinated "National Information Policy". My opposite number in Australia, for example, has a role, defined in legislation, to develop such a national approach.

On local government Publication Schemes, we plan to have amended guidance in place by the end of the year. Since the ICO Publication Scheme vehicle is there already, it shouldn't be necessary to develop additional non-ICO codes, whether advisory or statutory. More codes doesn't necessarily mean more compliance. And more codes can mean more muddle.

Finally, there's the Protection of Freedoms Bill which is making its stately progress through Parliament. It's important that the new law delivers the promised benefits of strengthened safeguards for information rights.

The proposals to delete the DNA profile and fingerprints of those who have not been convicted and are of no ongoing interest to the police are welcome and meet long standing concerns. But the associated information about these people held on the Police National Computer should be deleted too.

Additional regulation of Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) is also welcome, but the current proposals are limited in coverage, both sectoral and territorial, in a way that doesn't reflect how widely this surveillance technology is used - and there are no new sanctions for non compliance. The Data Protection Act will still apply to images of individuals whatever the sector and wherever

in the UK they are held. It is therefore essential that the proposed Secretary of State's Code and the new Surveillance Camera Commissioner properly complement the ICO's existing regulatory regime.

The Bill includes measures designed to ensure a better balance in criminal vetting arrangements, but there is nothing in the Bill about filtering out old minor convictions from vetting checks, as recommended by the Government's own adviser. Furthermore changes to the vetting regime may mean more enforced subject access, the practice whereby prospective employers require applicants to exercise their rights as 'data subjects' to access their own data and show the employer the results. There is already a long standing and urgent need to trigger provisions to make this practice unlawful. It's no good exempting citizens from checks if the boss can get round this by unfairly exploiting the citizen's own right of access to police information

It is also vital that the amendments in the Bill that add new rights of access to datasets under the Freedom of Information Act are clear and straightforward, both to implement and enforce.

And, I am determined that the improvements to the arrangements for safeguarding the independence of the Information Commissioner's Office are also enacted.

So, on this International Right to Know Day, I believe that an active and independent ICO can help to make a practical reality of the transparency agenda. Not just supporting the direction of travel, but helping to reach a common goal. Delivering a Right to Know 2.0. The reality, not just the rhetoric. The difference between seeing it through - and seeing through it.