Transparent Government, Not Transparent Citizens:

A Report on Privacy and Transparency for the Cabinet Office

Kieron O'Hara

Intelligence, Agents, Multimedia Group
School of Electronics and Computer Science
University of Southampton
Highfield
Southampton SO17 1BJ
United Kingdom
kmo@ecs.soton.ac.uk

Executive summary and recommendations

In December 2010, I was asked by the Minister for the Cabinet Office to conduct a review about the issues for privacy that were raised by the Coalition government's transparency programme. During the review period, experts in government, civil society activists, academics and many others were consulted to try to reconcile the desire for open government with the privacy of individual citizens (who may be data subjects in datasets about government activity). Those who were kind enough to help the review are acknowledged at the end of the report.

The review reached the following conclusions.

- Privacy is extremely important to transparency. The political legitimacy of a transparency programme will depend crucially on its ability to retain public confidence. Privacy protection should therefore be embedded in any transparency programme, rather than bolted on as an afterthought.
- Privacy and transparency are compatible, as long as the former is carefully protected and considered at every stage.
- Under the current transparency regime, in which public data is specifically understood not to include personal data, most data releases will not raise privacy concerns. However, some will, especially as we move toward a more demand-driven scheme.
- Discussion about deanonymisation has been driven largely by legal considerations, with a consequent neglect of the input of the technical community.
- There are no complete legal or technical fixes to the deanonymisation problem. We should continue to anonymise sensitive data, being initially cautious about releasing such data under the Open Government Licence while we continue to take steps to manage and research the risks of deanonymisation. Further investigation to determine the level of risk would be very welcome.
- There should be a focus on procedures to output an auditable debate trail. Transparency about transparency – metatransparency – is essential for preserving trust and confidence.

Fourteen recommendations are made which are intended to implement these conclusions without making too strong a claim on resources.

1. **Represent privacy interests on the Transparency Board.**
2. **Use disclosure, query and access controls selectively.**
3. **Include the technical paradigm.**
4. **Move toward a demand-driven regime.**
5. **Create a data asset register.**
6. **Create sector transparency panels.**
7. **A procedure for pre-release screening of data to ensure respect for privacy.**
8. **Extend the research base and maintain an accurate threat model.**
9. **Create a guidance product to disseminate best practice and current research in transparency.**
10. **Keep the efficacy of control in the new paradigm under review.**
11. **Maintain existing procedures for identifying harms and remedies.**
12. **Use data.gov.uk to raise awareness of data protection responsibilities.**
13. **Investigate the Vulnerability of Anonymised Databases.**
14. **Be transparent about the use of anonymisation techniques**

The grounds for these conclusions and recommendations are given in the body of the report, and the recommendations elaborated in detail in the final section.