EVIDENCE SESSION ON SOCIAL MEDIA DATA AND REAL-TIME ANALYTICS

Thank you for your letter of 9 July which requested that the Ministry of Justice provides a response to a number of questions that arose during your Committee’s recent evidence session on social media data and real-time analytics with Ed Vaizey MP, Minister of State at DCMS.

The Committee’s questions are set out in bold text below, followed by a response on each point.

Under the Data Protection Act a breach of section 55, which is unlawfully obtaining disclosure of personal information, is currently an offence but is backed up only by a fine. It is not a criminal offence and there is no prison sentence attached to that. Do you think it should be? (Q213)

The Government takes the protection of individuals’ personal data very seriously. Since taking up my role as Minister of State for Justice and Civil Liberties, I am reviewing the sanctions available for breaches of the Data Protection Act 1998, including whether to introduce custodial penalties for breaches of section 55.

The Information Commissioner has alerted this Committee to the fact that a credit reference agency has been buying social media sites. Are the Government concerned about that? Do they see a privacy issue there, or do they believe action should be taken when ownership changes so that the users of those sites know who the owner is and that it might be used for different purposes from those they originally envisaged? (Q212)

I am not familiar with this particular case so it would not be appropriate for me to comment on the specific details or whether the credit reference agency or social media sites involved are compliant with the Data Protection Act 1998. However, it should be noted that all organisations that wish to process personal data in the UK...
have to comply with the eight data protection principles in the Data Protection Act 1998. The principles include the requirement that personal data is processed fairly and lawfully. The second data protection principle states that 'personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'. In practical terms this means that organisations must, amongst other things, be clear from the outset about why they are collecting personal data and what they intend to do with it and make sure that if they plan to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

The Information Commissioner told us that once data has been anonymised, the data loses data protection rights. But there is potential for data to be re-identified. Is the Government of the opinion that re-identified data should have the same rights as unanonymised data? (Q215)

Personal data can be defined as any data that relates to a living individual who can be identified from that data or from that data and other information that might be in the possession of the data controller. If re-identified data meets the definition of personal data, it would be subject to the same legal protections in the Data Protection Act 1998.

The Government submission seemed to be unsupportive of the proposals for EU data protection regulation. Could you explain what your submission to this inquiry meant by "the insistence [of the] proposals on explicit consent is likely to lead to a 'trivialisation' of the experience for data subjects"? Can you explain why the Government considers that explicit consent would not provide greater protection for individuals?

Individuals are sharing data on an unprecedented scale. It is therefore essential that we provide for strong data subject rights to protect against abuse of personal data. However, we do need to strike a balance and, while this should not be abused, data controllers can have a legitimate interest to process data.

We would therefore be in favour of retaining the 'freely given, specific and informed' formulation for personal data in the current Data Protection Directive and reserving 'explicit consent' for sensitive personal data. Consent should be attainable for data controllers.

Our concern is that explicit consent would not necessarily provide greater protection for individuals. This is related to the fact that this is likely to result in 'tick box fatigue' as it is likely to require numerous opt-in mechanisms on websites. This could lead to individuals opting in as a matter of routine even in cases where their privacy would be better served by opting out, rendering the concept meaningless. There is also a risk that the additional bureaucracy might frustrate users and prevent vulnerable individuals in particular from accessing services.
Should the re-identification of anonymised data be made a criminal act? If so, what sanctions should be introduced?

Re-identification of anonymised data may contravene a criminal offence at the moment. Much would depend on the particular facts. Section 55 of the Data Protection Act 1998 refers to the 'unlawful obtaining etc of personal data' and makes it a criminal offence for a person to 'knowingly or recklessly obtain information without the consent of the data controller'. This could be by deception or by accessing personal data on a computer for individual's own purposes when they know, or ought to know, that they do not have the consent to do so.

To what extent the S55 offence would apply to the re-identification of anonymised data would depend on the context and particular facts. If an individual uses a position of trust to re-identify a person by piecing together information that is not publicly or knowingly (or ought to have known) that they did not have consent to do this, then s55 is likely to apply. However, if the data sets are publicly available and a member of the public pieces together information to identify an individual, the issue of a lack of consent would unlikely to be relevant as they are publicly available anyway.

A person found guilty of a criminal offence under s55 DPA on summary conviction is liable for a fine not exceeding the statutory maximum of £5000 or an unlimited fine on indictment. Given this, we do not believe there is a need to introduce a further criminal offence in these circumstances.

I hope this provides the Committee with the information they were looking for.

SIMON HUGHES