2014. Ofcom then plans to publish a consultation in Q1 of 2015 setting out any proposals for changes to its policy and a final statement in early Q3.

Manana Shrimpling, solicitor, Osborne Clarke, Bristol

Big data and data protection paper from ICO

Sue Gold

Journal of Direct, Data and Digital Marketing Practice (2014) **16**, 135–137.
doi:10.1057/dddmp.2014.69

Who: Information Commissioner

Where: United Kingdom

When: 27 July 2014

Law stated as at: 7 August 2014

What happened

Different privacy risks

The Information Commissioner's Office (ICO) published a 50-page paper on 27 July entitled 'Big data and data protection'. The paper gives an overview of the privacy issues that arise from using big data and suggests how to comply with the Data Protection Act 1998. The ICO states that the paper's aim is to ensure that the different privacy risks of big data are considered alongside its benefits. It emphasizes that the 'benefits cannot simply be traded with privacy rights'.

Setting the scope

The paper invited comments by 12 September 2014 and asked for feedback on three specific questions:

- whether the paper reflects all the relevant issues;
- whether the ICO should produce further guidance documents and, if so, what they should cover; and
- whether there are any other practical measures and tools needed to address the issues in addition to those already contained in the paper.

Focus on transparency

The paper focuses in particular on the importance of transparency. It emphasizes that, where big data involves personal data, then data protection laws still apply and should not be seen as a barrier to progress, but as a stimulus to 'develop innovative approaches to informing and engaging with the public'.

ICO conclusions on big data

Definitions

The ICO references the Gartner definition of big data, although it emphasizes that there is no fixed meaning. Big data is defined, the paper says, by volume, variety and velocity (the three Vs). Big data typically

uses extensive amounts of data from a variety of sources and can be analysed in real time. Sources of data include metadata from internet searches, payment transactions, social media postings and mobile phone location data. Issues can arise when combining data from different sources when data is sourced externally.

Fairness

Fairness is a key data protection requirement. Organizations need to be transparent when they collect data and the ‘complexity of big data analytics is not an excuse for failing to obtain consent when required’. Individuals should be informed about the purposes, implications and benefits of processing their personal data in a big data context. There is a danger, the paper says, that algorithms may be used to perpetuate stereotyping or bias, for example, customers’ ‘likes’, purchase and search histories being used for targeted advertising. Data quality can also be an issue.

Consumers ignore privacy notices

The paper recognizes the challenges in providing notice about use of data. The fact that people very often do not read privacy notices does not necessarily mean they are unconcerned about how their data will be used. Often individuals will not even know their data is being used as big data uses observed, derived and inferred, rather than provided data.

Consent

The paper references research which shows users may want to give consent to different uses of data throughout the relationship (graduated), rather than being asked to consent at the beginning, and will often want to receive a benefit in return for data. In addition, the benefits of big data should be explained, but consent does not mean people ‘trade all their privacy rights’.

Repurposing data

Personal data is often collected for one purpose and then analysed for a completely different purpose. Individuals should be made aware of this intended use. If the new use is incompatible with the original purpose, then consent may be needed to use the data.

Data minimization and retention

Big data often features using personal data in a way which may not be compatible with the data protection requirements to minimize data use and ensure use of data is not excessive. Big data is not an excuse to stockpile data or keep it for longer than needed.

Security

This is always a key requirement and a proper assessment of risk should be carried out. The collection and retention of large volumes of data (often in the cloud) could potentially, if ‘uncontrolled’, increase the risk of a security breach, but big data can also be used to improve information security. The paper concludes that, while there is a potential for increased risk, this can be mitigated by applying normal security procedures and using big data in security analytics.

Ethics

Organizations adopting an ethical approach to big data are more likely to be complying with data protection laws and they may gain a competitive advantage by being seen to be ‘responsible and trustworthy custodians of customer data’.

Anonymization

Consider if personal data is really needed in a big data project or whether it can be anonymized. The ICO states that the issue is not about eliminating the risk of re-identification altogether, but whether it can be mitigated so it is no longer significant.

Privacy Impact Assessments (PIAs) Subject access

Carry out a PIA to consider how the processing could affect privacy.

Design systems to facilitate easy access to data in the event of subject access requests.

Why this matters**Regulatory attention**

Big data is clearly on the radar for regulators and the fact that the ICO has issued a 50-page report indicates its importance. The paper, however, is on the whole balanced and recognizes that big data is not always bad (as the media sometimes suggests) and that privacy and big data can be compatible by going back to basic privacy principles.

Existing practices apply

Many of the points and issues raised in the paper are not new, but reinforce the fact that the existing privacy rules continue to apply. One area that may be challenging to apply in practice will be getting consent where required and coming up with innovative means for notification.

Announcing the publication of the report, Steve Wood, the ICO's head of policy delivery, said, 'What we're saying in this report is that many of the challenges of compliance can be overcome by being open about what you're doing. Organizations need to think of innovative ways to tell customers what they want to do and what they're hoping to achieve. Big data can work within the established data protection principles ... established in UK and EU law [which] are flexible enough to cover big data. Applying those principles involves asking all the questions that anyone undertaking big data ought to be asking. Big data is not a game that is played by different rules'.

Sue Gold, consultant, Osborne Clarke, London

CAP top tips for affiliate marketers (and PhonepayPlus pipes up, too)

Anna Williams

Journal of Direct, Data and Digital Marketing Practice (2014) **16**, 137–140.
doi:10.1057/dddmp.2014.70

Who: Committee of Advertising Practice (CAP)

Where: United Kingdom

When: 10 July 2014

Law stated as at: 5 August 2014

What happened**Performance-based commission**

'Affiliate marketing' is a method of performance-based marketing where a third party (the 'affiliate') is rewarded by a brand for new customers attracted to the brand as a result of the affiliate's marketing efforts. Affiliates will often be rewarded on the basis of a commission for the sales that result from their efforts.