dataprotectionlaw&policy
STRATEGIC ANALYSIS BY DATAGUIDANCE
APRIL 2014 VOLUME 11 ISSUE 4

Best foot forward: challenges & opportunities of Big Data

In the privacy sphere, how to protect the 'data' in 'Big Data' has been hanging over privacy professionals' minds since the concept of Big Data first came into the equation. While industry experts and observers continue to debate on whether data truly is the new oil, companies must seize every opportunity presented by Big Data and tackle the unforeseen data protection challenges with minimum disruption to their commercial activities, but how? Mike Bradford, Founder & Director Regulatory Strategies Ltd, shares his thoughts on how to strategise your business in the age of Big Data.

I attended a conference recently in London run by a major IT company. I'll not mention names.

As with anyone running their own consultancy I like to keep myself up to date with both legal and practical developments around data and as it was a 'freebie' I didn't see any reason for not doubling up an a client visit to the City and a chance to become an expert on what seems to have become the in-phrase, Big Data.

I even did some background reading before the conference - and some personal research among clients - to gauge their views on the subject. And then something totally unforeseen happened. They were a speaker short. Or more accurately - and thankfully - a member of a discussion panel short. And yes, I was there - wrong place, wrong time.

I was ushered through the delegates - fortunately it wasn't a sell out - and took my place at the 'top table'. And then, much to my horror, was asked to provide some initial views on the subject.

Perhaps because I didn't know much about it meant that I could say exactly what I thought - and what I suspect each and every passenger on the proverbial Clapham omnibus thinks about it!

What on earth is this phenomenon of Big Data? How does it impact me? Who has my data and what are they doing with it? Frankly it all sounds a bit suspicious.

Having got over my initial shock at being offered this 'hospital pass' I then moved into 'professional' mode and, in what I hope was a measured, assured and (reasonably!) coherent manner shared my views with an audience who I'm sure knew far more about Big Data than I ever will.

Good data and privacy protection doesn't operate in a vacuum. Regulators must protect consumer interests - and as we know only too well in Europe there is a conflict between those that balance legitimate business interests and consumer rights with those that almost regulate privacy for privacy's sake.

And I fear where this will end up for those countries, like the UK, that have enjoyed a balanced approach though data protection legislation pre-dating even the current data protection directive.

But we are where we are in Europe. For those countries operating on a similar data protection framework to the current directive there is still time to avoid what may become a straightjacket, with stifled innovation and reduced consumer choice as unintended consequences.

And of course there is a natural tension between technological innovation and in particular data flows over the web and data protection.

Potentially every body of law in every country could apply to activities carried on via the internet - there is a fundamental conflict between two ideals at work. The very essence of the internet is that it facilitates the free exchange of information. Conversely, the sole raison d'être of data protection legislation is to ensure that the exchange of information is strictly controlled and regulated. An encouraging start!

My view on what data protection means to me as an individual is quite simple:

"To me good privacy provides a framework of protection to give me the confidence to make informed decisions and lifestyle choices as to how I use and to whom I disclose my information for my benefit as a consumer; and ensures transparency over the legitimate uses and disclosures of my personal information in respect of my rights, obligations and protection as a citizen."

And then we have new 'flavour of the month' - Big Data. Frankly people don't understand Big Data. What does it mean? It conjures up visions of 'Big Brother.' And against that, to make it work both for businesses and consumers we need to build confidence now to win over what is a very sceptical audience. And that might be a big ask in some geographies.

But Big Data as a concept isn't new. It simply means optimising the use of available data for a particular activity. And the more data we can put into the pot, the more optimal our offering will be - or so we think.

We are all concerned about the security of our data, especially over the internet. And privacy and

information rights awareness is high globally.

Data protection law is all about personal data. So can we anonymise the data? But the pragmatic UK position of anonymisation - where businesses need only prove that there is only a remote risk of re-identification - is not shared across the EU and certainly the new EU regulation is likely to tighten up on this and the requirements tends to be that re-identification is no longer possible. Germany is a good example of this.

So we can't bank on being able to rely on anonymisation taking us outside our DP obligations.

Data protection law and regulator expectations go to the heart of Big Data. And things will get more challenging as EU law moves up to take its place alongside our more strategic legal 'must do's' like competition and anti-trust laws.

Don't approach Big Data in isolation. It should be part of our holistic approach to privacy and data protection as we prepare for what lies ahead.

The commercial upside is that businesses which embed data protection in their culture and psyche are increasingly using this as a competitive differentiator.

Big Data - and compliance with what consumers expect from their data - puts a premium on:

- developing methods to verify the authenticity and trustworthiness of data
- more focus on how our analytics teams interact with, mine and understand that data
- creating technical mechanisms to minimise the impact of Big Data use on the privacy of individuals - the regulatory controls are a given

Transparency, choice and proportionality are the critical tests at the moment. And openness - especially with automated decisions using my data in background. What if it's incorrect or out of date - both requirements of current data protection law? Consumers hate - and will react to - loss of control. Avoid surprises.

Don't approach Big Data in isolation. It should be part of our holistic approach to privacy and data protection as we prepare for what lies ahead.

Regulators see increasing amounts of personal information as meaning increased risks to individuals and the need to raise the privacy protection bar. And this is driving EU data protection changes where technology and procedural safeguards have lagged behind innovative uses of data.

It is better to build in protection rather than bolt it on as an afterthought. And there are different transparency and consent challenges for exploiting legacy databases for new purposes versus newly collected data.

Maybe there's a difference here in public versus private sectors - with the former, use of personal data for new purposes and impacts on the individual are likely to be highly sensitive and the EU Article 29 Working Party (WP29) recommendation of 'free, specific, informed and unambiguous opt-in consent' would be required; with the latter a clear notice and consent could be proportionate.

The WP29 recommends people who are given access to their profiles and organisations should disclose their decision criteria. Seems fair to me for the big win of optimising our Big Data opportunities.

When advising clients on 'Big Data' my 'best practice' model really only reflects what I'd expect as a consumer and citizen:

- work with the regulator and expect different levels of support and appetite - one size will not fit all
- be totally transparent and use very clear notification clauses and privacy statements, explaining any less visible technologies like cookies
- decide on an opt-in or opt-out strategy - remember you want to be able to reuse the data and it is a false positive to think that the more data you have the more powerful the solution - it is only as powerful as the consumer deems it to be
- only use predictive data – it must be adequate, relevant and not excessive
- build in quality checks around accuracy
- establish retention periods - quality and recency of data is preferable to a huge decaying data pool
- observe the consumers' rights – encourage accessibility and with careful relationship-building the consumer is your best method of enriching your database through interaction and updating their details and preferences
- security - must be at the top of your priority list
- cross-border considerations - don't forget that one regulator's support may not be shared out-of-country

We have a huge opportunity - but one that is on the cusp of being lost though mismanagement of messages and lack of clear protections and safeguards.

Mike Bradford Founder & Director
Regulatory Strategies Ltd
mike.bradford@regulatorystrategies.co.uk

CECILE PARK PUBLISHING
Data Protection Law & Policy is published monthly by Cecile Park Publishing Limited
17 The Timber Yard, Drysdale Street,
London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093