

# Data sharing in the insurance industry: an overview

The UK insurance industry recently came under fire with claims that they share customer details with personal injury firms. This was triggered by the Former Justice Secretary Jack Straw writing an article in *The Times* in June 2011, stating that insurers regularly refer their clients to personal injury lawyers without permission. Straw wrote that Phil Riley, one of his constituents, had been contacted by compensation lawyers after being involved in a minor road accident, although never authorising disclosure of his mobile number, or any other data. Mike Bradford, Director of Regulatory Strategies, discusses how data sharing takes place in the industry.

27th June 2011. The day started as usual with the 'Today' programme gently stirring me from my slumbers. Jack Straw was being interviewed around something a constituent had raised with him about being contacted by compensation lawyers following a minor road accident. So it transpired that the insurance company had sold his data to an accident management company without the constituent's consent.

At this point, my data protection instincts took hold - I was wide awake and Section 55 of the UK Data Protection Act 1998 (DPA) was whirring through my mind. A cut and dried case of a Section 55 breach if I'd ever heard of one.

The data had clearly been disclosed by the insurance company and obtained unlawfully by the accident management company - and any subsequent recipients. Multiple criminal offences for the Information Commissioner's Office (ICO) to address - they'll have a field day!

Just as I thought it couldn't get worse, the spokesperson for the Association of British Insurers (ABI) said that it was common practice across the industry and, quite unbelievably, that if insurers didn't do it, others would - recovery firms, garages, credit companies, the other insurance company involved and 'even the police' (although the Association of Chief Police Officers (ACPO) subsequently refuted this claim). So that's alright then.

Even more ironic is that the likely come-back from someone using the services of an accident management company is an inflated insurance claim - the phrase 'biting the hand that feeds it' springs to mind!

The following day, Axa unilaterally declared that it had voluntarily banned referral fees - the practice of accepting fees from personal injury lawyers when putting their customers in touch with them to pursue 'valid claims' - and also said that it had never sold customer data.

So following the ICO issuing the UK's first statutory code of practice on data sharing on 11 May, we have a perfect example of data sharing in practice that contravenes all that good data sharing should stand for. Indeed, back in the June issue of *Data Protection Law & Policy*, I wrote an article on credit data sharing and laid out my own expectations of how my data should be used in this context: '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.'

The insurance example is a clear breach of the Act, but perhaps worse than that is the total disregard for what individuals would expect from any organisation that holds their data.

In its defence, the insurance sector faces significant challenges, in particular around the levels of fraudulent claims. Since 2006, the work of the Insurance Fraud Bureau (IFB) with UK insurers and police forces has led to the prosecution of many organised insurance fraud gangs but there is still a huge issue that affects all of us - and which we are all literally paying for in our premiums.

In July this year, ABI members set up a national Insurance Fraud Register to combat rising levels of fraud across all lines, estimated at £2 billion a year reported to increase insurance premiums by on average £44 per individual policy holder.

This database, currently in a six-month pilot phase, should be fully operational next year and will enable insurers to share data on known fraudsters enabling them to identify anyone who fails to declare a previous fraudulent insurance claim.

I would argue that this both complies (or should comply if operated correctly, typically with appropriate notification wording prior to a search of the database being carried out and the relevant purpose provisions around data being shared for fraud prevention being in place) with the DPA, and should also not offend any privacy sensibilities of individuals, either on a personal or public-interest level.

The Motor Insurance Database (MID) is another example of data sharing in this sector that has been operating successfully for many years. The UK has one of the worst records in Western Europe for

uninsured driving with an estimated one in 20 cars on the road being driven without the correct insurance. MID now holds details on all UK insured drivers, covering over 25 million motor insurance policies, 30 million private vehicles and four million commercial vehicles.

MID is a tool for insurance companies and the Police to identify the insurance company of a particular vehicle and receives over 75,000 enquiries a day from the police. The general public can also make enquiries.

On a cross-insurance line basis, the Claims and Underwriting Exchange (CUE) is a central database of motor, home and personal injury / industrial illness incidents reported to insurance companies, which may or may not give rise to a claim.

CUE is managed by not-for-profit company Insurance Database Services Limited (IDSL) on behalf of its member organisations including all major insurers and many self-insured organisations, such as local authorities, passenger carriers and transport companies.

The database is reported to hold over 32 million claims records comprising information supplied by the policyholders or claimants on their application or claim form, together with other data relating to the incident or claim.

To my mind, this level of data sharing is a different proposition to that referred to earlier about sharing know fraudulent claims. Here, there is no suggestion that the claim may be fraudulent and insurers and their actuaries will use the database as a means of detecting what may be a fraudulent claim due to similarities or material inconsistencies with previous information submitted by that individual, or volumes and types of claims from that

**The insurance example is a clear breach of the Act, but perhaps worse than that is the total disregard for what individuals would expect from any organisation that holds their data**

individual, or potentially that individual's family or associates.

Here I would certainly expect to be told that any claims' data I provide may be shared with other insurers for the purposes of assessing any future claims and the prevention and detection of fraud. I would expect the transparency bar to be higher than in the case of known fraudulent data sharing as much for confidence and openness - this is the model that the sharing of credit data is predicated on in the UK, namely notification at the point of application.

I would therefore argue that the Schedule 2 Paragraph 1 condition of 'consent' should be applied for transparency as much as compliance with the DPA, although there could be grounds for pointing to Paragraphs 2 and 6, namely it being a contractual requirement and/or in the legitimate interests of the data controller. This latter condition would although refer more to the database search rather than the sharing of any claims data which is by definition of less immediate benefit to the company disclosing the data than the company obtaining it on the subsequent search.

There is also another data protection challenge here in that claims' forms may contain details of third parties, for example accident witnesses. The 'consent' requirement cannot easily be fulfilled here and the other Schedule 2 conditions become even less appropriate.

And to compound the issue it is not unknown for 'witnesses' to appear on a number of claims albeit apparently being made by different individuals and it is this - the 'serial witness' - that is indicative of the potential fraud.

Whether a clause on the claim form putting the responsibility for notifying any witnesses named that

their data may be shared is sufficient could be highly debatable on the grounds of proportionality.

So, there you have it. Some examples of data sharing in the insurance sector. And on the most part fulfilling both individual and public benefit criteria, and complying with the letter and spirit of the DPA.

And there are equally examples of compliant cross-sector data sharing, including fraudulent insurance data, operated by the credit reference agencies and CIFAS - fraudsters tend not to limit themselves to a single sector and someone submitting a fraudulent credit application is as likely to make a suspicious insurance claim.

Indeed, maybe the insurance industry needs to push its data sharing boundaries even further as the credit sector has done - with the agreement of the ICO - throughout the customer lifecycle from identifying prospects, risk assessment, customer management and claims processing.

Anyway, I wonder what will be the next John Humphries interview that makes me sub-consciously flick through the DPA as I stir from a night's slumber?!

**Mike Bradford** Founder and Director  
Regulatory Strategies  
[mike.bradford@regulatorystrategies.co.uk](mailto:mike.bradford@regulatorystrategies.co.uk)