

---

# Editorial

*Journal of Database Marketing & Customer Strategy Management* (2007) **15**, 1–3.  
doi:10.1057/palgrave.dbm.3250072

A departure, this volume.

It is a tradition for each Editorial to reflect upon the papers that are published in the current issue. Nothing wrong with that: it situates what is being written about in a broader context; and that can be helpful where, on occasion, the train of editorial thought that links the content of each volume is a little obscure.

This issue, however, I would like to look outside the contents, and to consider a topic we will be returning to with a special edition later in the volume. That is the whole question of data security and data protection.

It is presently very topical in the United Kingdom. If one reads the newspapers, one can hardly escape the issue. The government, in the guise of its taxation arm, the Revenue and Customs division, decided to send two CDs, containing the personal and banking details of 25 million individuals, from one department to another.

The CDs went missing. After extensive inquiries, the most likely outcome is that they have simply been lost. However, there is an outside chance that they have fallen into the hands of criminals, which could eventually prove catastrophic both for the government and for the individuals whose details have been lost.

As always, the main headline story has driven many more such stories out of the woodwork, and the general public is aware that the government has routinely been losing or misplacing their personal details.

This is important for two reasons. First, because it feeds into a growing paranoia about identity theft and misuse of personal

data. Second, because it comes at a time when the government's main initiative to protect the public from identity theft is the idea of creating a single national super-database, linked to ID cards.

There is already much opposition to this idea, though it is often confused. The government proposal is actually made up of two distinct ideas: the ID card, and the idea that failure to carry it would be a crime in its own right, and the database.

Critics of the latter proposal have pounced upon the loss of data as being a strong argument for not going ahead with a new database. The government, with remarkable chutzpah, has argued back that this loss of personal information is a very strong argument FOR such a database.

One can just about see their point. After all, if ID fraud is likely to be more prevalent, better, perhaps, to entrust its safety to a national body with theoretically unlimited resources to develop security measures. Although that is not how the public has seen it. The government response sounds remarkably like: 'we have just lost a load of your data: so to make things safer for you, please entrust us with even more of your data'.

If one discounts the fact that a great deal of public angst is based on irrationality, there is a more basic disagreement in play here, between management and technicians. Having worked on countless systems developments over the years, it has always struck me as odd, sometimes amusing, that those who sponsor IT projects talk in terms of '100 per cent', zero errors, and blue skies perfect outcomes. Meanwhile, those who

have to make it happen — those of us who know just how badly wrong any system can go — talk about reducing risk and mitigating adverse consequences.

The government are talking like managers: many of the more thoughtful critics are IT specialists.

So far, this may appear like a storm in a UK teacup. But it is adding to a debate about data that is worldwide.

The history of data protection has been slow and patchy. In Europe, it began with the concepts now embodied in Data Protection law. This set limits to what organisations might do with personal data that they hold about individuals. In the US, the approach has been rather to rely on individual rights to privacy. The end result is not altogether dissimilar — but has meant that Europe and the United States do not altogether see eye to eye when it comes to protecting data.

To begin with (in the UK), data protection was taken with a pinch of salt. It was new law. It had few teeth. So I have not been surprised to find myself asked very closely by the Directors of some (very respectable) companies what would be the costs of breaking the law vs the costs of making the IT systems compliant. My sense is that for some companies, in the end, it was perfectly rational to prefer illegality to compliance.

In recent years, that has begun to change. The penalties for noncompliance are greater in some parts of Europe, and the trend is toward increasing those penalties — not being more lenient. The US has had the Enron affair, and other issues around company transparency. Although this has not directly resulted in new data protection law, it did lead to much tighter legislation on corporate compliance in general — the Sarbanes–Oxley Act — which has fed back into issues of data protection.

Back in the UK, a trend that has been visible for the last few years is that of some companies — especially in the public sector

— finally getting their act together and then over-reacting. In many cases, data protection has become a means to protect the organisation itself from what it sees as customer intrusion.

Which brings us back to identity theft, ID cards and public disquiet. Issue 15/3 of the *Journal of Database Marketing and Customer Strategy Management* is going to look in depth at some of the implications of the above. This, however, is to focus on the problem. The reverse of this is a series of trends that are only just beginning to make themselves felt in embryonic form: in some instances as humour of the ‘it’ll never happen here’ variety.

That is that the public are waking up to the fact that data and data protection is an important issue. Further, that it has been legislated around for years with little true consumer input. The point of view has been that of the legalist, not the individual data subject.

A protective framework has been put in place. But it is not clear that it suits those it is meant to protect. A couple of months ago, one respected marketing newsletter printed a spoof letter from a customer to their bank. The joke lay in the idea that a fed-up customer might turn the tables and start to set out terms and conditions by which they expected the bank to trade with them. Very witty.

Except: this IS the way that companies need to be thinking. From the US, there are already well-established moves from the customer side to collect personal data and charge companies for using it. Within the ‘geek’ community, there is much debate about constructing software that will force companies to identify themselves to customers before they do any trading with them. The coming wave seems to be an abrupt reversal of the last 20 or 30 years of database marketing.

This has been about companies collecting personal information and laws being passed to regulate that. The next wave is beginning

to look like individuals managing their own personal data, and issuing permissions to companies to make use of it.

Science Fiction? Oddly, the first glimmerings of this could be seen in one of those works of '60's free thinking — 'The Third Wave', by Alvin Toffler. It had many, many predictions about the effect that technology would have on our lives. Some now appear ridiculous: but some are merely delayed. In the '60's, the presumption was that technology as change driver would be impacting society tomorrow. In the end, the impact did not come tomorrow. Or the day after tomorrow. Rather, to extend the metaphor, it has come eventually, about a

week or so later than predicted. But nonetheless, it is coming.

My suspicion is that many data controllers believe that they have seen the worst of the changes. Government has spoken. Laws have been passed. A new era is upon us, and it is manageable.

In fact, we have merely dipped our toes into the waters of change. The top-down revolution has happened: the bottom-up one is about to begin. And most companies are seriously under-prepared for it.

JOHN OZIMEK  
Managing Editor