



## Loyalty cards: The risks and rewards

Loyalty cards - with their numerous risks and few rewards - have really taken off. Can we trust that the commercial organisations that store our data will take good care of it? Cath Everett investigates and finds there's no such thing as a free lunch...

Today we are living in a database state. Despite growing fears of 'Big Brother' and the emergence of a surveillance society, it is not just the government that is merrily gathering increasing amounts of personal data on its citizens, and housing it in ever larger repositories for analytics and other purposes.

Commercial organisations of all stripes are also doing so as they try to build more detailed profiles of their customers in a bid to market and sell to them, thereby increasing their profitability.

Some information, such as names and addresses for example, are necessary for organisations to collect when taking hotel or flight bookings. Many companies also add to this data by purchasing information from third parties such as market research houses. The aim? To obtain a more rounded picture of their customer base in order to undertake so-called behaviour analytics.

Other increasingly common tools for data collection, however, include online profiling software, of which Amazon is a past master and, in the physical world, loyalty cards. Once a rarity, reward cards are now proliferating at an unprecedented rate. For what is often a minimal incentive, they encourage many consumers to hand over valuable intelligence about themselves and their behaviour, often without even reading the small print. As a result, many people are completely unaware of how their data is being used, and by whom.

Such cards are also, in some instances, money-earners. According to Adrian Pastor, principal security consultant at auditing and security testing firm Corsaire, between 10 and 20% of loyalty card points are never redeemed – particularly if time limits are applied – which means that companies simply "get the unspent money back tax-free".

The overall value of such cards, however, is best summed up by a statement on dunnhumby's website. The company is a specialist in database management and provider of behavioural analytics services, in which Tesco owns a majority stake. It states that the act of translating the insights "gleaned from terabytes of information (gained via its Clubcard loyalty card) into actionable marketing and retailing programmes" played "a key role in enabling Tesco to become one of the world's most successful retailers".

### Risks and rewards

So if the benefits to consumers are so apparently low and the benefits to companies so apparently high, why do people buy into such initiatives? Peter Gooch, senior manager at Deloitte's security and privacy team, believes that it "all boils down to risk and rewards".

"That's key as it depends on what people think they'll get back and whether they consider it's worth it. It also depends on the risk aversion of the individual concerned, combined with the reputation of the company. As a rule, the more eager a company is to get hold of information, the more rewards it will give", Gooch says.



Adrian Pastor, Corsaire



If retailers aren't looking after credit card data properly, they are even less likely to be looking after loyalty card information

Moreover, the average citizen does not think deeply about the privacy issues involved in such a situation as they are focussed on the rewards, not what they are 'trading in'. More worrying still, the average citizen also appears to inherently trust that organisations will handle their information responsibly.

As Mike Gillespie, director of information assurance at consultancy Advent IM, points out: "How many retailers have had to report some kind of credit card data breach in the last 12 months? If they're not looking after credit card data properly, how well are they likely to be looking after loyalty card information, which is considered less sensitive and is not covered under PCI DSS? One of the real concerns, of course, is identity theft."

Even in terms of credit card data breaches, it is unclear how many such incidents actually do take place in the UK because, unlike in places such as California, there is no legal obligation to report them. This situation is expected to change over the next few years, however, as the European Commission starts to turn its attention to such matters in the wake of growing negative publicity.

### Three's a crowd

One of the big areas of concern at present is data handling by third parties. Because managing and analysing vast amounts of customer information is a complex activity, many organisations hand over the data they have collected to specialists such as Dunnhumby and eLoyalty to do the job for them.

According to research undertaken by security research firm the Ponemon Institute, data breaches involving third party providers jumped to 44% of the total last year, up from 21% in 2005. They also cost more to deal with at around £140 (\$231) per compromised record compared with an average of £123 (\$202), with the biggest hit coming from lost business as customers went elsewhere.

As Deloitte's Gooch says: "Knowledge is power in the information age and so companies will

continue to try and obtain increasing amounts of information about their customers. You can't outsource risk, ultimately they still have responsibility. If things go wrong, it's them that will be blamed."

Moreover, James Mullock, head of the technology practice at lawyers Osborne Clarke, expects regulations and the enforcement of regulations around issues such as consent and selling on mailing lists to tighten up over the coming months.

The subject of consent, for example, is mandated under the Data Protection Act (DPA) - the key legislation in this arena - and involves companies using devices such as opt out tick-boxes. One of the key problems here is that such boxes are often not very visible, nor do they make it very clear what marketing information will be shared with whom.

However, while such areas may "not have been that well enforced" to date, according to Mullock, the appointment of Christopher Graham, new Information Commissioner and former head of the Advertising Standards Authority (ASA), is expected to change the situation - particularly if, as is widely rumoured, the Information Commissioner's Office (ICO) also receives stronger enforcement powers.

'Graham comes from the ASA, which has traditionally enforced against the issue of consent the most. So he's aware of the issues, which are about things like not having clear enough tick boxes or none [at all], and having adequate contracts with suppliers in place', Mullock explains.

“

**Knowledge is power in the information age and so companies will continue to try and obtain increasing amounts of information about their customers**



Peter Gooch, Deloitte



Another ICO requirement that is also likely to start rising up the agenda, meanwhile, is for organisations to start undertaking privacy impact assessments - or risk management initiatives- at the commencement of any personal data project This is not best practice is. in reality, rarely followed today.

'Very few companies are doing it. Partly it's about lack of awareness, but such activities also take time and money and people, want the maximum return for the minimum investment', says Advent IM's Gillespie. Nonetheless, he believes it crucial that chief information and chief security officers start 'thinking honestly' about whether they have fulfilled all of their obligations under the DPA.

"Has their organisation conducted a privacy impact assessment? When was the last time they did a formal data handling audit? Do they have a formal data classification strategy or even know what data they have?" Gillespie asks. "Just because organisations have a DPA policy and are sending back their return to the ICO once a year doesn't mean that they're handling their data in the way they should be."

### **Take it back**

Such concerns, particularly in the privacy arena, are starting to give rise to alternative means of dealing with the situation, in an online sense at least. Doc Searls, a fellow at the Berkman Center for Internet and Society at Harvard University, for example, is heading up a community driven project in the area of Vendor Relation Management (VRM - <http://projectvrm.org>).

VRM involves flipping the concept of Customer Relationship Management (CRM) on its head by creating a standards-based frame-work, out of which online tools and services can be developed, to enable consumers to take back control of their own personal information.

**"VRM is a framework and mindset for looking at the tools, applications and technical models to help individuals initiate transactions on their own terms".**

*Adriana Lukas*

The aim is to provide people with the means of managing which authorised third parties, whether vendors or friends, have access to their personal data. Another goal is to enable consumers to analyse their online transactions in order to help them manage their expenditure. for example, or to articulate their preferences to vendors more clearly.

If the vision becomes reality, it would ultimately mean that numerous private or public sector organisations would no longer need huge amounts of (often inaccurate) information about individuals in massive databases that they spend time and money on trying to manage, protect and analyse.

Instead it would be up to individuals themselves to provide authorised third parties with selective data in order to either undertake relevant transactions, or to interact with them during the product design process for example. Individuals would also provide third parties with any changes to that data - such as a new name or address via alerts or feeds - but could likewise remove them from their authorised list should any abuse take place.

Adriana Lukas, who has set up an open source project called Mine!, which is attempting to put into practice the principles articulated by Doc Searls, explains: "It's about the user-driven web. So VRM is a framework and mindset for looking at the tools, applications and technical models to help individuals initiate transactions on their own terms. It's about redressing the current balance of power."

Lead developer Alec Mullett aims to have beta code available by the end of August, and Lukas is also working on the all-important user interface with various others. The aim is also to develop a REST-based application programming interface for organisations to write applications. services and plug-ins to download Mine! programmes to. How data storage should be undertaken however, is still under discussion.

One possibility involves holding encrypted information in distributed fashion around the cloud, while another involves capitalising on ideas currently employed by systems such as Opera Unite. Opera Unite is a service that turns the Opera web browser into a web server to enable file-sharing and streaming.

Lukas concludes: 'It's the flip side of CRM. We expect the first users to be mainly developers and social web people that will use it for themselves and develop it further. But over time we also expect it to develop like blogging and twittering which means that once people start doing it, companies will have to follow and learn how to deal with the changes it brings too.'