data chaos

- a court case waiting to happen

Professor Merlin Stone

With a contribution from
Professor Martin Evans

Bristol Business School
University of the West of England
Frenchay Campus
Coldharbour Lane
Bristol BS16 1QY

UWE
BRISTOL

Bristol
Business School

Sponsored by

ACXIOM®

Contents

1   Executive Summary

The research for this report was carried out by Bristol Business School and sponsored by Acxiom. None of its content should be construed as offering legal advice.

There is increasing international focus on data protection. Although different countries have taken different stances, leading to an inconsistent set of rules, there is increasing pressure to work together to protect the rights of consumers as personal information crosses international borders. Data Protection under European legislation is particularly stringent.

This report shows that when it comes to managing customer data many companies still need to do a lot of work on quality. It also shows that senior management are not focusing enough on the issue of data quality.

The popularity of customer relationship management (CRM) lies behind these issues. CRM strategies usually involve a company gathering much more customer information from various sources, placing it in a central repository for segmentation, analysis and reuse. A 'single view of the customer' is a frequently cited aspiration of many CRM projects. But it is this very bringing together of information into a single database or several databases can potentially be at odds with the law.

The data chaos caused by the scramble for customer data has led many companies to be in direct contravention of these strict laws because they lack the rigorous processes required to keep them compliant. In most cases:

- There is no process for ensuring that the customer has full access to all personal data
- There is no process for reviewing, refreshing and discarding data on a regular basis.
- There is inadequate protection of data being transferred between countries with different data protection standards

Many companies are ignorant that they are breaking the law in this way.

However, the issue is broader than compliance with legislation. For while the threat of prosecution, fines or closure of a web site is very real, the loss of customer confidence and trust is more alarming.

This report shows what companies can do to improve the quality of their customer data and how it is used.

2   The Research

The research for this paper was carried out using a number of sources:

- Results of a Data Protection Questionnaire sent to key CRM representatives in over twenty blue chip companies and CRM strategists
- Customer Management Assessment scores (70 companies in many sectors were evaluated using QCi's Customer Management Assessment Tool. Degree of observance of best practice is as assessed by trained consultants, with scoring according to the extent and thoroughness of compliance.)
- Analysis of information on 'The Future of Retail Financial Services' collected by Pro-Log for IBM's Business Innovation Services, published in June 2001

These findings were supplemented by other sources, including analysis of published material.

3   Overview

Data protection and privacy issues are coming to the fore again in the age of the Web. Citizens are concerned about the use of data they give on the Web. This is reinforcing an old concern initially raised in classic direct marketing contexts (telephone, mail). These concerns were never really completely resolved, although the introduction of mail and telephone preference schemes, together with the improving control of major marketers over their direct mail and telemarketing activities have in general reduced the public attention focused on problems associated with errors and intrusiveness. However, the introduction of three new channels to the world of customer relationship management – interactive digital TV, mobile telephones and the web – have created the need to re-examine the extent to which companies are in control of their customer data. This is because these three new media have much greater potential for

intrusiveness and for gathering data from the customer than older media, and also for gathering it when the customer is not conscious of its gathering.

Whether citizens are surfing the Internet, using a mobile phone or exploring the interactive pages of digital television, they are producing data for the companies that supply them. They are also open to being targeted with commercial offers. The issues discussed in this report should be of interest to government, citizens/consumers, and companies, because in these new environments, the potential for customer data to be used illegally is much greater. How well are companies prepared for this new era of interactivity, when it comes to how they manage customer data? The answer as this report shows is – not very well. The reason - senior managers are not focusing on quality issues in customer data management.

So desperate are companies for better customer information that the overall spend on CRM projects has risen dramatically and is set to rise further. The Hewson Group estimated that in 2000 there was seventy percent growth of the European market (overall spend, including third party services - integration and implementation services from third parties or supporting technologies such as computer-telephony integration or data warehousing and analysis are excluded - was over $3bn in 2000). Further growth of one hundred percent or more is forecast for 2001 for application software and services direct from vendors including e-commerce, although they suggested that growth might be pegged back to seventy percent by the scarcity of implementation resource (of course, the slowing down of economic activity which has become apparent lately might also rein back growth).

This vast outlay demonstrates the priority given to CRM by most companies. However, in the scramble to acquire more customers and to implement more and more data-driven applications to collect even more detailed customer data to help retain and develop them, 'data chaos' has ensued:

Data is being gleaned from the ever-increasing number of different channels without any secure process for maintaining that data to an appropriate quality standard. Often multi-channel strategies fail because what is right for one channel cannot be replicated across all the others.

Ownership of data is frequently spread across many different departments and business units, making management and responsibility for the integrity of the data as a whole almost impossible

Where senior management is focused on topics relating to customers, it is on classic CRM topics, such as customer retention, and not on customer data. This is despite the fact that that our work indicates that:

- The quality of customer data management is not strong
- Attention focused on customer data is not wasted.

The various studies we have seen about senior management priorities in related areas indicate that the main topics exercising senior management are these:

- Deregulation
- Competitive entry
- Merger and acquisition
- Risk
- E-business and (in some cases) wireless aspects
- CRM
- Marketing and sales efficiency
- Distribution channel uncertainties
- Long term shifts in demand patterns

In many cases, these issues are combined. For example, the impending further deregulation of the motor industry (the end of the European Union Block Exemption allowing motor manufacturers to specify that motor dealers deal solely in a single brand) is leading to a strong interest in CRM, e-business and a search for alternative distribution channels. The risk associated with changing climate patterns is causing property insurance companies to consider how to modify their CRM efforts to ensure that they do not attract too many customers with recently enhanced levels of risk. Competitive entry by e-banks is causing traditional banks to bolster their own e-operations, but also to focus their CRM efforts on customer retention and development. Retailers and airlines who have failed to address longer term shifts in demand

patterns are reconsidering their CRM efforts – in some cases enhancing them, but in others reducing them in favour of a stronger focus on the core offer.

Of course, management focus is not just a question of underlying forces. It is also directed by the efforts of companies marketing relevant products and services. For example, the enormous budgets dedicated by CRM software suppliers and their partners to advertising and exhibitions have undoubtedly helped sustain the salience of CRM. The same can be said for a variety of systems companies in relation to e-business. Publicity from major management consultancies and research companies reinforce the agenda, although at least in the latter case some (such as Gartner) are now focusing on reasons for failure.

Paradoxically, in some cases it is senior management's drive in other areas that is reducing compliance with data protection laws. Every new channel that is added, every merger or acquisition that takes place, means that different data sets are acquired or developed, often about the same or overlapping sets of customers. Old data sets may need to be combined with new ones. Indeed, the ability to manage the same set of customers more efficiently or to gain improved value is often cited as the reason for a merger or acquisition or for the development of a new (often electronic) channel. Where this is so, failure to comply with the law also implies failure to manage data properly – or at the very least risks alienating customers. These in turn raise doubts about whether a company will be able to achieve the proposed gains in areas such as:

- Marketing and sales efficiency
- Competitiveness
- Customer acquisition, retention and development
- Customer service.

However, all is not lost. Claire Forbes, the Corporate Communications Manager of the British Chartered Institute of Marketing, noted in mid-2001 that data protection legislation was, along with CRM, firmly in the top ten issues faced by marketers.

4   Resolving the problems

Total anonymity is almost impossible in today's society. Basic necessities in life such as earning a living, holding a bank account, driving a car, receiving medical treatment and schooling children all require giving out pieces of information about oneself. Successful CRM strategies rely on gathering this and more sophisticated information on current and potential customers. As Jacques Nasser, CEO of Ford put it "I want to know the coffee pot you use and the watch you wear to produce the right car for you", but the value of holding customer data has been recognised universally and those companies who do not understand their customers find themselves increasingly disadvantaged. Demand predictions are driven by the amount and quality of customer information held. Revenue and profit rely on accurate supply chain management based upon customer forecasts. Customer data is no longer a 'nice to have'; it is absolutely critical for commercial success.

However, consumers are becoming increasingly concerned about how personal information is used. They dislike being exposed to irrelevant advertising ('junk mail' and 'spam' e-mail being perfect examples of this). Whilst this phenomenon is annoying, the real issues that bother consumers are twofold:

- Who knows what about me? There is a real fear about repositories of personal information held without the individual's knowledge
- Could this information be used against me? For example, individuals do not want to become the victims of fraud, to be fired from their jobs or to be denied insurance based on a set of data held without their knowledge or permission

Any attempt to protect customer data has at its heart these two questions which together deal with the mutually dependent issues of privacy, security and trust.

5   Current Trends in Data Protection

The Internet has brought new focus to the issues surrounding the protection of data. Never before has there been such freedom of access to an immense amount of personal information on a global scale. Countries such as the US who value their open society and personal

freedoms and find any bent towards totalitarianism deplorable are being forced to rethink how to deal with the balance between privacy and freedom of information. By contrast, Europe, which spent twenty years bashing out the finer details of the EU's 1995 Data Protection Directive, are beginning to realise that their ability to legislate is being outstripped by the speed of technology and that some form of self regulation is desirable. Table 1 gives a quick overview of the two different approaches to data protection.

The success of a business depends upon the trust of its customers. Individuals will not choose to do business with companies they do not trust. Trust cannot be won unless privacy is respected and security is assured. Respecting privacy and protecting personal data mean much more than mere adherence to laws and regulations. A company must put in place the standards and disciplines required to meet customer expectations; it must practice the art of self-regulation. Those companies that harness their understanding of their customers' data protection requirements will demonstrate integrity to their customers. Their customers will have confidence that their privacy is protected and their transactions are secure. Treating people the way they want to be treated can give companies a significant competitive edge.

In the US there are no statutory rules. Codes of practice exist within the industries but little is known about their effectiveness. There is also some sector-specific legislation. But data protection laws are not the decisive factor when it comes to consumer trust in data protection. World-wide, about 12 million people stopped buying over the net because of privacy concerns and that resulted according to Gartner Research in a loss of $12 billion in e-commerce, according to a Financial Times Article (February 28, 2001). A Westin/Harris research report done in 1999 for IBM shows that customers trusted their banks and health insurance companies, but only 10% of German, 13% of UK and 21% of US customers trusted web companies an the way they handle personal data.

Jennifer Barrett, Chief Privacy Officer of Acxiom, says "If companies are merely making investments to comply with privacy laws and regulations, they are missing a huge opportunity if they do not recognise it as a dual investment in building trust, increasing customer loyalty, and creating a competitive edge. The most forward-looking, customer-centric companies recognise that compliance with the law and the related communications is a platform for entering into a

positive dialog with the customer about how the company treats their personal information, honours their preferences, and cares enough to listen."

Opting in separately to all the possible uses of customer information would be virtually impossible. So, this makes it very important to be a trustworthy business. No matter what a company promises, if it deceives customers or uses information about them incompetently, it will pay in the court of public opinion and eventually in revenue and profit. This suggests short and general notices are more likely to work, the more complex the relationship. However, resolicitation of important permissions (e.g. to use particular communications media, to promote major product areas) may be worth considering.

There is also a big difference between the business-to-business and business-to-consumer environments. Companies in the former are entrusted with complex and sensitive information about their client companies and about many individual managers in these companies. This means that business-to-business companies need to work particularly hard to maintain high standards in the management of customer data.

In the business-to-consumer area, there has been consumer uproar about the data-gathering practices of online companies such as DoubleClick and Toysmart.com. DoubleClick planned to combine the names and addresses of consumers with their Web surfing and shopping habits. They planned to use cookies to track individuals without those individuals knowing they were being watched. Public outrage forced the company to rethink its practices. It hired a chief privacy officer, shelved its master data-collection plans and invited an external auditor in to look at its business practices. In another case, Toysmart, the online toy retailer filed for bankruptcy and wanted to sell its extensive list of consumer information as an asset. Again, public outrage forced them to reconsider the sale. The fear of such public relations disasters has meant that companies are trying harder to comply with the new rules. There has also been a bipartisan push in the US to see federal laws passed on privacy protection.

Table 1: Data Protection Trends in the US and Europe

	United States	Europe
State-Regulation	• Federal law protecting the citizens of the US against the collection, processing and use of data by the government is comprehensive and relatively restrictive • No federal law for commercial data protection passed, but with increasing examples of abuse of personal data, increasing pressure is now being brought to bear on the government to do so • Thousands of individual pieces of privacy law being created by individual states in response to local concerns (e.g. in 1999,over 7000 pieces of state legislation on data protection & privacy were made state law)	• Data Protection Directive created in 1995 • Individual countries of EU have own laws in compliance with Data Protection Directive. For example, the UK Data Protection Act 1998
Self-Regulation	• Long history of industrial self-regulation • Series of codes of practice within industry, but no ultimate means of enforcement. Little evidence as to how effective the self-regulation is • Non-profit privacy groups are finding alternative ways to protect data (e.g. The Privacy Foundation based in Denver is testing a tool to identify surveillance tags too small to see) • Safe harbour agreement between US and EU	• Much legislation cannot match emerging technology (especially anarchic nature of the Internet) • Self-regulation becoming increasing prevalent e.g. FEDMA has created a series of codes of practice which set standards for data protection (encouraged and supported by the Directive)

6   How do customers feel about this?

Research carried out by Professor Martin Evans at Bristol Business School indicates that privacy is an issue for some customers, with physical privacy (the intrusion of direct marketing into their homes) representing an annoyance and information privacy (relating to the information available on consumers) representing a more substantial worry. In terms of the latter, respondents' level of knowledge varies substantially. People react in different ways. For example, some are pragmatic and recognise that the provision of personal details may improve targeting. However, those who feel particularly strongly attempt to minimise the information held on them, and rarely, if ever, provide direct marketers with personal details or request communications from them.

Interestingly, privacy concerns feature most strongly when respondents perceive that they are targeted with irrelevant marketing communications. The emotive response to this can vary from a general annoyance to overt concerns, and the strongest reaction is to actively withdraw from direct marketing communications. Direct mailers do not like the term 'junk mail'. It applies to mail that is perceived by the recipient as being uninteresting or irrelevant.

The Bristol research showed that there are several dimensions to the relevance issue. The four variations being; interest, timeliness, repetition and the information processing effect. Relevance can only be achieved through improvements in targeting; improvements that require the use of personal data on individuals by companies. Control is an important consideration for consumers. Indeed, control issues underpin concerns with regard to both privacy and relevance and, as such, must be taken seriously. Here are some examples of what consumers said to the Bristol researchers:

- '...I would prefer it if I didn't see anything in the post unless I had specifically requested it' (Female, 25-34).
- '…Personally, if I've got something that I want to do financially, I would look into it and go to my own people. I would search them out myself rather than look at something that came through on the carpet because generally you just pick it up and throw it away.' (Female, 25-44)

- '…It's just annoying to be sent things that you are not interested in. Even more annoying when they phone you up….If you wanted something you would go and find out about it.' (Female, 45-54).

## 7   How to improve the quality of customer data management

Data quality has always posed problems. Incorrect or incomplete data leads to internal frustrations, inaccurate marketing campaigns, incorrect segmentation, etc. Our research shows that the majority of CRM managers feel that there still needs to be significant improvements in the quality of data management. Despite spending considerable sums of money on CRM software and the resource to implement it, most of them stated that there have been few major improvements to the quality of customer data in the last few years. However, until now this has, for the best part, been an internal issue. Worse than this, they risk damaging publicity leading to a lack of trust by customers.

Trust is the foundation for maintaining good customer relationships. It was clear from our expert survey (the details of which are presented in the Appendix) that the retention of best customers is the top priority for most companies (acquisition of new customers, though rated highly, is not considered to be as important to the success of the business). It is not surprising then, that when the respondents were asked to state their priorities in marketing, customer service and related areas, we saw an emphasis on those activities which involved developing the relationship and trust of the customer. For example, ensuring security of customer data and ensuring the customers' rights to privacy were cited as key concerns.

Issues of security, privacy and trust are growing in importance, particularly with the coming of age of the Internet. Companies that will succeed over the next decade will be those capable not only of understanding that are their best customers, but nurturing that relationship and providing those customers with the comfort that their data will be used with integrity. This can only be achieved by taking a holistic approach to the processes and procedures for good data management. Most companies need to take a close look at how customer information flows into the company, how it is managed internally and how it is passed out of the company. They also need to look at the processes that focus on the customer experience. The customer must be allowed full access to their information should they require it and the company should

frequently check that the customer is comfortable with how their personal information is being used. Figure 2 illustrates this flow of data and poses some key questions that a company wishing to follow best practice customer data management should ask itself.

Figure 1: An Overview of Customer Data Management
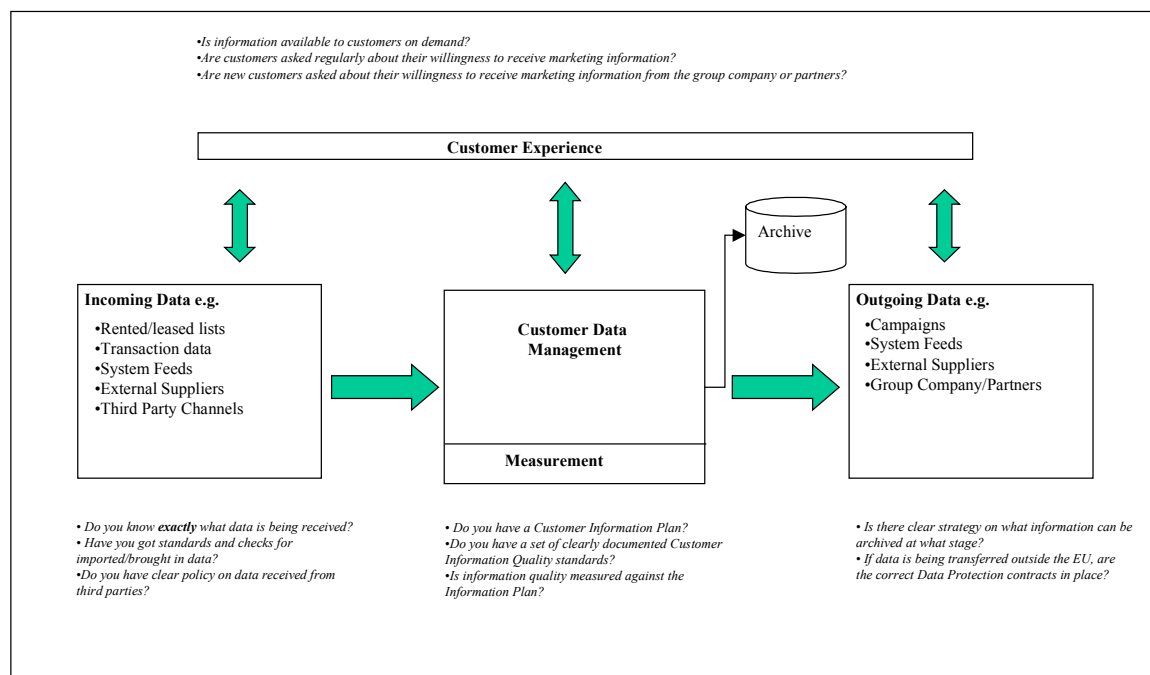
7.1 Managing the Customer Experience

The Customer Experience begins with the acquisition of data (even at the prospect stage – when they have yet to become customers) and continues until the company no longer holds any personal data on that individual.

The customer should be made aware of what information is being recorded about them. There should be complete visibility at the point of capture.
Companies are weak in recording declarations made to customers when customer data is captured. Our research shows that even blue chip companies with good internal customer management processes have poor knowledge of exactly under which declaration data from a given customer is held. Many companies do not even record declarations made to customers when they capture customer data. If a company does not know, it should refresh the

declaration by sending the data to customers and asking them to sign a new declaration, or it should restart its data collection process with clear separation between old and new data.

The *type* of data gathered must be relevant. In an Internet bank that wanted to be seen as a market leader in customer service, the CRM team felt that there was no such thing as 'irrelevant' data, and that any information gathered about a customer, via whichever channel, should be kept for future analysis.

The customer should be made aware if personal information is to be used for purposes other than that for which it was collected

This has fundamental implications for any CRM programme. Most CRM databases were designed with a wider use of combined data in mind. Customers should be informed of these wider uses at the point of data capture, or consent should be obtained subsequently. Companies must therefore ensure that they monitor the use of customer data and seek permission when the use is outside the original remit for acquiring the information.

Many companies are also poor at maintaining up-to-date records for marketing purposes. While most are diligent about canvassing new customers with regard to their willingness to receive marketing information from groups and partners, very few of them regularly check to ensure the opt-out clause is up to date. Companies should consider putting a process in place that can, at regular intervals, automatically check that a customer is happy to continue receiving marketing literature.

Companies must be able to track customer data and allow their customers to access it if they wish

The capability to track customer data as it is used and stored in different parts of the organisation is critical if data is to be protected. Data is often moved to more centralised repositories so as to get a 'single view of the customer' – said to be essential for the customer to experience consistent treatment by all parts of the company. In our survey we asked CRM managers, CRM consultants and other relevant experts whether their companies could quickly and accurately recognise a customer at any of their contact channels and access complete and up-to-date information for that customer. With a few notable exceptions, most respondents had to agree that it was currently impossible in their organisation or those of their clients,

despite a declared aspiration to one day attain the holy grail of a 'single customer view'. However, a single customer view has implications for data protection. To comply with legislation, a company must maintain high quality records of the source of all the data it holds about its customers. Real-time updates of customer information across all channels make data extremely difficult to track.

Most of the respondents to our questionnaire on data protection (See Appendix) stated that they had problems with keeping track of the source of the data, especially with inbound e-mails. At the same time, most of our expert respondents saw achieving a single view of the customer as being a priority. We wonder whether a sense of reality needs to dawn. A 'less fragmented view' rather than a 'single customer view' might be easier and less costly to manage, whilst having the added benefit of allowing better management of the data and therefore compliance with the Data Protection Act. This is especially important given that there are constant pressures which cause "re-fragmentation" of the customer view in many of the industries which are big users of customer data, such as financial services, utilities, telecommunications, travel and leisure. These pressures include mergers and acquisitions, launch of new ventures targeted at existing customers, and proliferation of channels of distribution and communication for managing the same set of customers.

7.2 Managing Customer Data Internally

In Figure 2, Bar 1 shows how comprehensively the industries surveyed understand the requirements of the Data Protection legislation in all the countries in which they have customers. By contrast, Bars 2, 3 and 4 reveal the extent of customer data management processes in place to manage customer data:

- Bar 2 shows the existence of a Customer Information Plan covering information value, acquisition priorities, information Management and usage
- Bar 3 reveals the extent of clearly documented Customer Information Quality standards that apply to customer related data
- Bar 4 shows the degree to which the information quality is formally measured against the Information Plan with measures being stored and used to monitor improvement

Data Protection: Understanding versus Activity
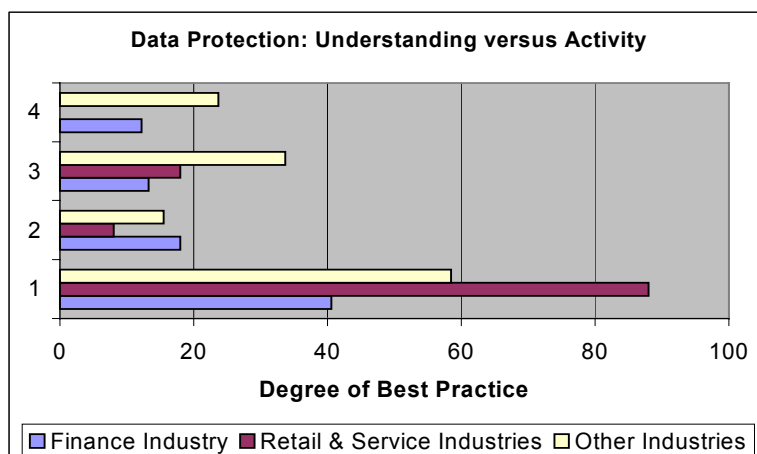
Figure 2: Data Protection: Understanding versus Activity [Source: QCi's CMAT Scores]

While overall understanding is quite good, it is worrying to note that though the understanding of the law in financial services industries is better than in other industries, it is still not very good. Also, despite an understanding of what is required, companies are neglecting to put in place the practices and processes they need in order to be able to manage their customer data to the standards expected by the legislation. This suggests that companies need to introduce a number of disciplines, suggested below.

Internal data audits should be undertaken at regular intervals

An internal data audit is one way for a company to understand how well it is managing customer information. This will reveal:

- The amount of data kept on individuals
- Where the data has come from (and where it has been across the organisation)
- The consistency and accuracy of that data across different channels and data bases
- The relevancy of the data (e.g. Has excessive data such as 'hobbies' been recorded for an individual?)
- How long the data had been kept
- Whether the data should still be kept (i.e. Is the original purpose for collecting the data still valid?)
- Whether the data has been processed in accordance with the individual's rights

- How secure the data is (i.e. Is it open to internal/external fraud?)

Through such an audit, companies discover the full extent of the customer data they hold and the quality of that data. When companies undertake an audit, they usually discover that they are holding far more data than they thought, at far lower quality. The data is rarely concentrated on one database, except in relatively simple businesses (e.g. single product or single channel). If, as a result of doing an audit, a company becomes compliant (or nearly compliant) with the new Act, a year later it may well have become non-compliant. This is likely to be because another customer database has been set up that is not properly tied to the first and has records that overlap with it. The chances are that either or both customer records are incorrect, but the company will not know which.

Internal principles for managing data must be set

To attain high quality data management, it may help if data privacy guidelines and principles to be set and published and communicated to relevant parties – particularly to those members of staff who have customer-facing roles. Business practice can then be evaluated against these privacy guidelines and principles to ensure continuity of quality. They might include:
- Published quality guidelines for all imported data
- Clear policy with third party channels regarding the customer information they provide
- Documented customer information quality principles that apply to customer-related data. These principles should be set using a Customer Information Plan that covers information value acquisition priorities, information management and usage.

Enlisting staff help to improve data quality

With increasingly complex systems interfaces to contend with, the employees' contribution to the quality of customer data management can be great. There are a number of steps a company can take to ensure that the employees' contribution is maximised:

- Staff can be given incentives and sanctions to ensure the information quality on the customer database. Bar 1 in Figure 3 shows how many companies surveyed subscribed to this way of thinking. In none of the sectors was the score over 26%. Interestingly, it is in the Finance Industry (where mistakes can be extremely costly and where staff are typically given

financial incentives to produce the desired result), that is the worst culprit, scoring an average of only 8.9%.

- Our research also shows that there is a problem with the way that customer information is being recorded. Bar 2 on Figure 3 shows how frequently core customer information is clearly documented in a way that can be understood by non-systems staff. All industries, it would appear, have a problem with this, since none scored higher than 32%.

- Minimise keeping of records on paper. In our questionnaire to CRM managers, we discovered that there are a large number of companies whose customer-facing staff keep some records on paper. This puts the quality of customer data at risk, and should be minimised.

- Regular checks should be made on key customer/prospect records to validate their existence. Bar 3 on Figure 3 shows how frequently this practice is undertaken within the different industries.

There must be a clear archiving strategy

Figure 3 shows that, with the exception of the Retail & Service Industries, most companies do not have a coherent and well-managed archiving strategy. Data should not be stored for longer than its purpose requires. It effectively has a shelf life. Even with a clear strategy on what information can be archived at what stage, there needs to be a mechanism in place to alert the company that the information has gone out of date and either needs to be deleted or refreshed (with the customer's permission).

Figure 3: Archiving strategy [Source: QCi's CMAT scores]
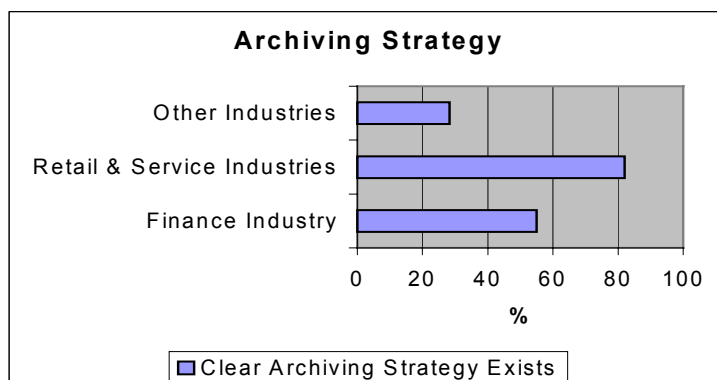
Summarising the results from using the CMAT data gives a stark picture.

- Only 15% of companies have clear and published data standards for imported data
- Only 26% comply fully with the terms of list rental agreements.
- Only 30% consistently store the source of their customer data on the customer database, for each new record added
- Only 17% could demonstrate complete understanding of data protection legislation
- Only 7% have comprehensive and clear customer information quality standards
- Only 7% give proper incentives to relevant staff concerning customer information quality
- Only 10% document core customer information in such a way that relevant non-systems people can understand it
- Only 7% formally validate customer records once a year or more often
- Only 20% have a clear policy for archiving customer information.

Building an infrastructure to avoid problems

Most companies' problems with compliance with data protection laws arise from not paying close attention to their data infrastructure – the processes by which customer data is gathered, maintained and supplemented, and the systems on which they are held. It is now possible to ensure that data gathered from and used by different channels, products and subsidiaries is unified and maintained to high quality standards.

8   Conclusions

Customers have a right to expect companies to manage their data professionally. This is not just a marketing question – financial issues are at stake too. Fraud is the most obvious risk, but there are other financial risks e.g. the recent case in which many customers of an insurance company were asked to return demutualisation bonuses because they were not qualified to receive them but had done so because of data problems. It is therefore important for companies to review the extent to which their own practices match best practice, and to establish strategies and targets to improve their practice.

9 Appendix – expert opinion

Respondents were asked the question, "In terms of your company's priorities in marketing, customer service and related areas, how would you score the following (score 5 for top priority, 4 for very important, 3 for quite important, 2 for not very important, 1 for not important at all)?". The answers are given in Table 2, ranked by priority.

Table 2: Business priorities

	Mean	Standard deviation	% Agreeing or agreeing strongly
Retaining our best customers	4.14	0.99	78
Ensuring security of customer data	4.05	0.90	70
Improving quality of CRM	4.05	0.79	70
Developing our relationship with existing customers	4.05	0.84	65
Ensuring our customers' rights to privacy	3.91	0.97	65
Acquiring new customers	3.73	0.88	74
Improving the quality of customer data	3.68	1.04	57
Compliance with Data Protection Act regulation to provide data to individual customers on demand	3.68	0.95	43
Implementing e-business	3.64	1.05	61
Coping with shifts in demand patterns	3.59	0.85	52
Making customer management more cost effective	3.41	1.18	43
Coping with structural change – deregulation, mergers and acquisitions, competitive entry	3.27	0.94	39
Coping with changing patterns of customer risk	3.09	1.15	39
Coping with distribution channel uncertainties	2.90	1.07	30

The table shows that data security and protection issues are important, being 2 among the top 5. However, our analysis of CMAT scores shows how far companies are from achieving their desires. An inspection of the standard deviation column shows that although coping with different kinds of change was less of an issue, the higher standard deviations indicate less of a consensus.

A second set of questions was asked, concerning the current status. Respondents were asked to state their degree of agreement with the statements below, using 5 to indicate agreeing strongly, 4 agreeing, 3 for neither agree nor disagree, 2 for disagreeing, 1 for strongly disagreeing. In Table 3, these are ranked in order of agreement, so the statements at the top of the list are the ones that most respondents agreed with. Note that the strongest positive consensus was about the need to improve the quality of customer data. Note too the agreement concerning the distribution of customer data on different databases, despite the general disagreement about sceptical statements about single view of customers.

Table 3: Current status

	Mean	Standard deviation
We still need to make significant improvements to the quality of our customer data	3.76	1.48
We always ask our new customers about their willingness to receive marketing information from our group company and from our partners	3.62	1.24
We still have a long way to go when it comes to identifying the preferences of our customers for communication with particular media	3.52	0.93
The customer data that results from our customer's transactions with different business units is held on separate databases	3.48	1.50
Our company has made major improvements to the quality of its customer data in the last few years	3.43	1.12
We have found It difficult to keep to our normal data quality standards when dealing with inbound e-mails	3.40	1.10
The addition of new channels of communication and distribution means that my company is finding it difficult to bring all its data about customers together	3.38	1.43
Members of staff who deal with customers still keep some of their records on paper	3.38	1.47
Our company maintains a high quality record of the source of all data it holds about customers	3.19	1.03
We still have a long way to go when it comes to identifying the interests of our customers in particular products or services	3.19	1.08
Our company can quickly and accurately recognise a customer at any of our contact channels and access complete and up to date information for that customer	3.05	1.40
Our company knows exactly under which data protection declaration it holds data from any given customer	3.00	1.18
Our company's policy is to ask our customers regularly about their willingness to receive marketing information from us, so as to ensure that our Data Protection Act opt-out and customer preference information is up to date	2.75	1.21
We do not believe that it would be cost-effective to develop a single view of the customer	2.33	1.11
My company does not believe that a "single view of the customer" – in the sense of having a comprehensive, rapidly updated view of all its interactions with a given customer – is really achievable	2.29	1.15

Acxiom Limited
Counting House
53 Tooley Street
London SE1 2QN
Tel: +44 (0)207 526 5100
Fax: +44 (0)207 526 5200
E-Mail: enquiries@acxiom.co.uk