

# You have permission to talk to my wife

**Jennifer Kirkby** looks at the minefield that is the Data Protection Act and suggests some ways in which organisations can overcome the problems it poses in dealings with their customers

**M**arriage vows are a deeply emotional commitment to care, share and endow our partners with all worldly goods. So it can come as quite a shock when call centre agents impudently imply we are defrauding our nearest and dearest. Welcome to the world of the 1998 Data Protection Act (DPA), where only individuals exist, and companies are

the arbiters of our information; unless they have a permission infrastructure. In theory data protection is a godsend, in practice it's causing grief.

Take the wife who queries the household electricity bill, and cannot get any information because the account is in her husband's name. How does she feel? Infuriated - her next call is to move the energy account to another supplier.

Or the lady who asks for the final payment needed for a joint mortgage endowment and is told the policy is in her husband's name; never mind that the direct debit goes to a joint account, she cannot have payment details. How does she feel? Vengeful - the company need never ask for her insurance business again.

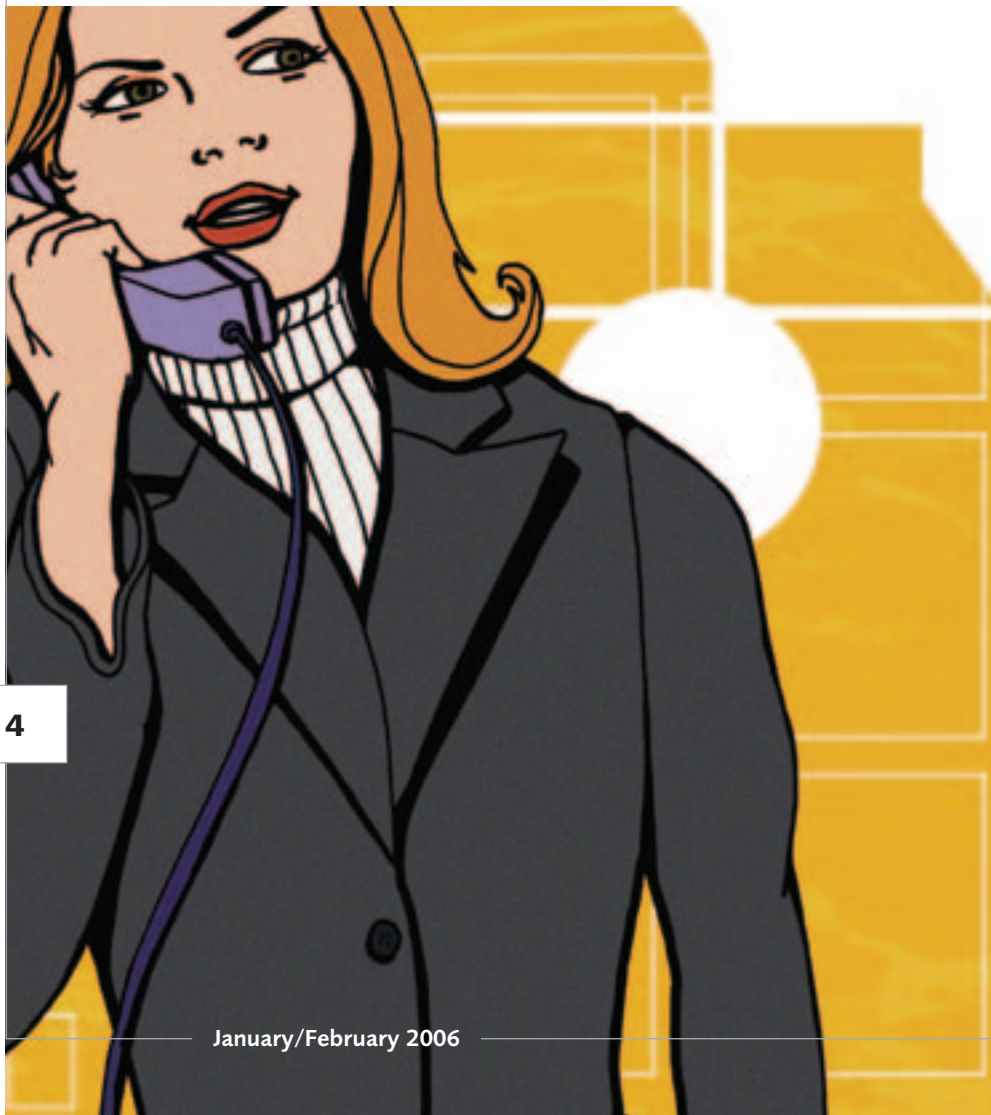
Or the father who cannot lock down his underage son's mobile phone to stop pornography downloads, because the contract is in the child's name. How does he feel? Irate - he ensures the whole family cancels every contract they have with that supplier.

## The problem areas

The problem of data protection versus family ties crosses all industries - can a husband sign for his wife's parcel delivery - but most problems occur in the following sectors; Energy; Telecommunications; Education; Financial Services; Health; Legal.

Expectations and the degree of 'personal' information, mean that occurrences at the top of the list cause more indignant anger and fewer disclosure complaints, than those at the bottom; few husbands complain when wives obtain details of the electricity bill. But disclosure of even the existence of a sexually transmitted disease test is venturing on to very dodgy ground - legally and morally.

It is a particular issue for married couples, because gender is easily determined on the telephone. Other pairings likely to run into trouble in the most mundane of circumstances are: parents and ▶



PERMISSION TO TALK: WHAT TO DO NEXT

Currently, 75% of companies have no information security and use policy. More organisations should use compliance to build not destroy relationships. The big question is always what is the business case - the answer must be to look at the detrimental effects on company image, customer loyalty and retention. A good place to start would be with one of the data protection assessments on offer by experts. Actions could include:

- Make sure that contracts name all owners - you may need to prompt. Ask for authorised users as well. This is principal one of the DPA. Gather this information on application forms. Currently running contracts should be updated - a good reason to contact customers and benefit from refreshed data whilst educating on the growing cost and problem of identity theft.
- Manage expectations, alert people to the service as well as the direct marketing aspects of data protection, the issues, and your policy on permissions. Say, if you have a blanket ban, and make it easy for people to give authority or change names to suit their requirements. This will cut the cost of customer attrition.

- Think through normal contract usage in your industry - do people tend to act as individuals or family units? Remember, behaviourally, men hate using the telephone. What are customers' expectations? How sensitive is the data. Build this knowledge into application and service processes - it's all part of the customer experience and will build the loyalty premium.
- Think through likely situations where people will try to illegally obtain data in your industry - quite often the same points as normal usage - and then put in place relevant safeguards. Ensure staff are trained to spot tell tale signs - some financial services companies are even inviting customers to attend such courses. Use the services of DPA advisors. A more effective way to protect.
- Mother's maiden name, dates of birth and address are all factual information that anyone can find out. Value based security checks - favourite colours or car - work better. If you offer people a choice of security questions look at secure ways of changing it. One man has a mother with the maiden name 'Bedford School', because he opted to use his first school, but the company mistakenly used the

default maiden name option; now he cannot change the question or the answer.

- Look for evidence of implicit permission e.g. is there a direct debit from a joint account; has regular contact or transactions been made by the same person. Asking 'if the account holder is there', is open to abuse.
- Are you actually giving out personal information?
- Change the way the situation is handled by staff. The tone and attitude of 'I cannot tell you that' is guaranteed to give offence. Don't blame the DPA; it's not true. Explain the situation and why the information cannot be given; give secure options for providing a service such as contacting the account holder at a known contact. Have out of hours help lines. This builds trust.
- Although many problems come from inbound telephone calls, there are also issues with letters, email and even personal visits. One medical company realised it should not use branded envelopes to notify patients of test results - family members asked questions.

underage children, children and elderly parents, common law partnerships, and even secretary and bosses.

The DPA, supported by the Human Rights Act, and intertwined with contract law, is a shield to protect us from those who pry into our affairs for personal gain and steal our identity - including the UK Government. Used with flair and imagination it's an asset to customer relations. But its leaden interpretation by over cautious companies leads to poor service by opening a Pandora's Box of emotions. The anger I unleashed when I asked consumers about their experiences was vitriolic. It is time organisations provided a proactive and comprehensive permission infrastructure based on the DPA's eight principles.

**The law (is not an ass)**

Companies misinterpret the law. If you believe many contact centre staff, the DPA does not allow the disclosure of any information, in any circumstances, to anyone,

other than the person they deem to be the account holder (few know if a male with the right password is really the male account holder). This is incorrect. The DPA not only accommodates but encourages good customer service. It actually says data requested by a third party should be handled fairly and securely, with relevant safeguards in place to ensure only legitimate disclosure.

The act urges the use of sound judgement, but with 55% of organisations suffering from at least one malicious security breach in any one year, blanket bans tend to be imposed. It is too risky and costly to empower staff with judgement (a problem exacerbated by culturally different off-shore operations). Incompetence is then covered with bad practice when the ban is blamed on the DPA. Others, realising the detrimental effect on customer experience, handle third party requests with care and a comprehensive permission infrastructure. These conflicting approaches

confuse customers and exacerbate anger with the blanket ban laggards.

**Customer action**

Of course, customers should protect themselves by ensuring accounts are in joint names and giving suppliers permission to talk to authorised users. But many people don't do this, because:

1. Emotionally they see themselves as part of a family group and linked.
2. Not every supplier has a blanket ban and expectations differ.
3. It is time consuming, difficult to do, and not helped by suppliers being reactive to enforcement, rather than proactive to service.
4. People do not know the law and don't know there is a problem until it really hits. People are used to opt-ins/outs for direct mail but few think about third party permissions for usage.

If customers thought they would be incon-

veniented or really understood the dangers then they might do something - but it is really up to suppliers to be proactive.

### Company inaction

The rationale for the blanket ban is the very obvious cost of compensation for damage and distress; this overrides the more intangible cost of customer annoyance. Yet this hidden cost could be vastly decreased through awareness of the benefits of protection. Knowing your suppliers have your interests at heart helps a relationship - thinking they are covering their own backsides at your expense does not. Companies should alert people to stories of:

- Separated and divorced spouses getting details of accounts for improved settlements.
- The spouse who uncovers an affair through an innocent query on a credit card hotel transaction.
- Address information given away to a violent, estranged partner leading to an attack and as has been known, murder or 'honour' killing.
- The growing crime of identity theft.

During the research for this report, men were far more responsive to the first two stories and women the latter! The irony of a blanket ban is that it doesn't protect from these events. If someone wants to illegally obtain personal information - known as blagging - they will. Even the uninitiated know that it merely takes the right gender voice and knowledge of security information - one 30 year old woman setting up her mother's mobile phone security was told she had a very young voice for 70, but the security was still set up. Using the appropriate email address is even easier, as is a letter. Proper, thought through safeguards would be better protection.



The DPA, supported by the Human Rights Act, and intertwined with contract law, is a shield to protect us from those who pry into our affairs for personal gain and steal our identity – including the UK Government. Used with flair and imagination it's an asset to customer relations. But its leaden interpretation by over cautious companies leads to poor service by opening a Pandora's Box of emotions

A permission service should cover contract usage and direct marketing; you should know both who you can talk to and who can talk to you. Technology is vital, and can be a barrier as it must be robust enough to record and ensure the right permissions at all touchpoints and support reliable identity authentication - speed and accuracy are crucial.

However, for many customers this is the hallmark of an efficient company; blanket bans give the wrong corporate image and thoroughly annoy those whose marriage vows still mean something. **CM**

### AUTHOR INFORMATION

Jennifer Kirkby is Strategy & Business Analyst for the Customer Management Community and Director of White Waves. She is an analyst and practitioner in 'state of the art' marketing and customer management practices. She was formerly CRM Research Director for Gartner UK Ltd and has been described by peers as "one of the leading independent CRM analysts and writers in EMEA"  
 Contact Details Tel - +44 (0)1943 878046  
 Mobile - +44 (0) 7740 740816  
 Jennifer.kirkby@white-waves.com



The Vanguard Method enables organisations to change from command and control to a systems approach to the design and management of work.

John Seddon, Vanguard's leader, translated the Toyota system – whose results are legendary – for service organisations – improving service, reducing costs and transforming morale.

## The Vanguard Method



To find out how the Vanguard Method could transform your organisation, call John Seddon on 01280 822255 or visit: [www.lean-service.com](http://www.lean-service.com)