WANT TO TALK TO ME?

WHAT CUSTOMERS WANT IN EXCHANGE FOR THEIR PERSONAL INFORMATION

JUNE 2015

Royal Mail MarketReach

CONTENTS

EXECUTIVE SUMMARY

Royal Mail MarketReach conducted online surveys with customers and donors in seven key market sectors. The objective was to understand consumer attitudes towards providing organisations permission to hold and use their personal information.

This report summarises our research and provides an overview that should be useful for any marketers who collect, hold and use personal information.

Our findings reveal that trust is central to customers' willingness to provide data.

Firstly, people need to trust in the competence of an organisation to protect their information from loss or theft. People are worried about hacking, phishing and identity theft. Overall, 71% of our sample said they were concerned (47% very concerned, 24% fairly concerned) that a supplier could lose their contact details. It is an issue of data security.

Secondly, people need to trust the intent of an organisation in relation to the use of their data. They are particularly concerned that it will be passed on to third parties without their knowledge or understanding of why. They also want reassurances that the organisation will use their information to send more relevant communications, not just more. Here the primary issue is data privacy.

We found that there were certain influences that could help to predict where there might be greater or lesser challenges to gaining permission. For example:

- Older people, women and lower paid people were more resistant than others.
- Existing relationships matter. Respondents were more likely to give permission to the organisations they have a relationship with.
- Some sectors were also likely to have higher or lower levels of implicit trust regarding use of personal data.
- Surprisingly, trust related to the collecting and holding of data may be a very distinct issue from sector or even brand trust.

A key finding was that building trust regarding data security and privacy was a matter that could and should be undertaken before a formal request for permission. This is partly to build reassurance, and partly because many respondents stated that they did not fully read, understand or believe permission statements.

When we asked respondents what kind of information was most likely to get them to agree to the use of their personal information, a statement which focused on data privacy and security was most persuasive. But there were other factors that had value as well.

Offering the opportunity to have some control over the communications process was also influential. In the majority of our surveys, this was seen as the second most persuasive factor. Just making it clear that they could unsubscribe to marketing communications at any time generated a positive response with a sizeable number of respondents.

Offering a value exchange also had worth to a number of respondents. The appeal of this type of offer varied from sector to sector but was often close to the communications control results.

Clearly a range of approaches could and should be tested, and it may be that combining the different messages could be effective, particularly if the messaging begins in customer communications prior to a request for permission. However this research suggests that addressing concerns about data security and privacy is the crucial place to start.

INTRODUCTION

Technology can make many things happen. But there is a difference between what we want, and what we can do.[1]

The premise of 1 to 1 marketing is that relevant and timely messages can be sent to consumers; messages that benefit both the recipient and sender. Information technology allows this to happen – and personal, up to date and accurate data is the essential ingredient.

But is it what we, as individual customers, want?

The growing capability of 'Big Data' is being followed by increased concern about 'Big Brother'. In the European Union, a new regulation is in development that is designed to redefine the rights and responsibilities surrounding data collection and use.

The Data Protection Act 1998 is the current guide to the use of personal data in the UK. But European legislative bodies are creating a new data protection regulation – the General Data Protection Regulation (GDPR). Different draft versions of the regulation include more stringent operational requirements for organisations and new significant financial penalties for non-compliance.

Amongst the proposals are changes to the law which would set a higher standard for gaining the consent of the individual to use their personal information for marketing. This may involve providing much more information about what consent is being asked for, and making that information much more visible and accessible to the individual.

This may also mean the rules for getting permission from the individual will become stricter if companies want to send them marketing for different products and services, or to share their details with third parties. The law may also introduce stricter rules on creating profiles of customers.

It is important to emphasise that the proposed new legislation is not law yet.

1. Paraphrased from Bertrand de Jouvenal (des Ursins), 'Utopia for Practical Purposes,' Daedalus, Spring 1965, (as quoted by Maxwell H Norman, Dimensions of the Future, Holt Rineheart and Winston, 1974). Jouvenal (1903-1987) was a French philosopher, political economist, and futurist.

But the Information Commissioner's Office (ICO), the UK regulator for data protection law, is advising that now is a good time for businesses to conduct a review of how personal data is currently used in marketing. Understanding and responding to this is essential to the future of 1 to 1 marketing.

In recognition of this need, we have conducted an extensive programme of research. We undertook seven separate online surveys, interviewing a total of 6,923 individuals. Each survey focused on the views of customers in a specific sector. These sectors were Telecommunications, Insurance, Retail, Retail Banking, Credit Cards, Energy and Charities.

In each survey, we asked customers about their attitudes and behaviours regarding the collection and use of their personal information by providers in that sector. Whilst the objectives remained the same in each survey, there were variations in specific questions as appropriate, and we modified some questions based on the insights we gained from survey to survey.

Unsurprisingly, views regarding the collection of information differed from sector to sector. But there was also a high level of consistency. This summary focuses on the issues at the heart of all the sectors we researched. These findings should be relevant to all organisations that want to hold and use personal data, not just in those sectors we have explored.

This is not, however, a 'Data Permissions Instruction Manual' that attempts to provide a simplistic and definitive guide to preparing for possible future legislation changes. Rather, it provides validated insights regarding the consumer's views of the issue of data privacy and security as a whole. It identifies and clarifies customer resistance, and shows how the right messages can overcome this.

Perhaps most importantly, it identifies content that organisations can use in communications programmes now, which will help to increase the propensity of customers to give permission in the future. We hope this will stimulate your thinking, and give you a foundation on which to build your own permissions strategy.

OUR RESEARCH

We conducted seven online quantitative surveys. The aim was to understand how customers (or donors) in different sectors felt about the use of their personal information by organisations, both in general and in their specific sector.

Each survey was independent of the others, and no respondents took part in more than one survey. All respondents were over the age of 18, and each sample was weighted to be nationally representative by gender and age.*

Details of the individual samples and fieldwork are as follows:

Telecommunications

- 1,000 customers of telecommunication companies who were sole or joint bill payers for at least two telecommunications services.

Insurance

- 1,000 customers who personally held an insurance policy and were involved in the decision about which policy to buy.

Retail

- 1,000 customers who had shopped for non-food items in the last 12 months.

Retail Banking

- 1,000 customers who held a current account with a retail bank.

Credit Cards

- 876 customers who currently had credit cards.

Energy

- 1,044 customers who were responsible for paying the household gas/electric bills.

Charities

- 1,002 donors who had given to charity in the last 12 months (excluding those who only donated via collection tin).

* Royal Mail MarketReach, Want to talk to me?, FastMap, 2014. Fieldwork conducted Telecommunications: November 2014, Insurance: November 2014, Retail: October 2014, Retail Banking: August 2014, Credit Cards: July 2014, Energy: May 2014, Charities: March 2014.

WANT TO TALK TO ME?

In June 2010, The Direct Marketing Association (DMA) published its first Data Tracking Study.[2] In it, Chris Combemale, Executive Director wrote:

"*Understanding why consumers are quick to withdraw the privilege of using their data for marketing purposes from brands is not terribly complicated… According to the findings of the report, simple trust in the brand is by far the most compelling reason that consumers cite for their willingness to hand over their details.*"

In the years since then, millions of us have provided more and more personal information to companies; to online retailers, bank apps, social networks, location-based voucher systems, and more.

But despite this, our latest research indicates that whatever the consumer is doing, his or her attitudes haven't changed.

Trust – or rather, lack of trust – is the central issue that database marketing must overcome.

This apparent paradox of customers giving information despite concerns could arguably continue indefinitely. And perhaps that is why there has been limited action from organisations in response to the DMA's comments five years ago.

But new legislation is on its way. And trust – in Non-Governmental Organisations, in businesses and in the media – is in decline.[3] So it is essential that, rather than just identifying the problem, organisations dig deeper into what this really means and how it can be addressed.

And the place to start is trust.

2. Data Tracking Study, DMA, June 2010.
3. Endelman Trust Barometer, Global results, 2015.

DIMENSIONS OF TRUST: COMPETENCE AND INTENT

The components of trust are defined in many ways. In his abstract 'Halo Effect in Trust', Professor R.C. Natarajan[4] provides a short resume of three decades of research and theory regarding these components. He concludes that there are dimensions under 'Goodwill Trust' and those under 'Competence Trust'. Don Peppers of the Peppers & Rogers Group[5] (and others) suggest a variant on this: in essence, trust in any organisation is determined by the viewer's perception of its intent and its competence.

This model is useful in defining the barriers that consumers have when considering the use of their personal details.

INTENT

Determining intent is a primitive capability that guides our behaviour: it's the need to identify friend or foe. If someone asks us to do something, our first response – what Kahneman,[6] would call 'fast' thinking – is based on the level of embedded trust we have regarding their intentions. If we feel at this gut level their intent is good, then we may do what they ask without hesitation or consideration.

4. '**Halo Effect in Trust**', Professor R.C. Natarajan, Indian Institute of Management Indore, May 27 2008.
5. '**It's About Competence and Intent. Trust Me**.', Don Pepper, Peppers and Rogers Group. Peppers is a business executive, author, keynote speaker, and a founding partner of Peppers & Rogers Group, a customer-centric management consulting firm. He is considered by many to have created the modern concept of Customer Relationship Management.
6. '**Thinking, Fast and Slow**', Daniel Kahneman, Macmillan Books, 2011. Kahneman illustrates how we use two forms of thinking; System 1 or fast thinking is our first response and is fast, automatic, instinctive and emotional. System 2 is slower, more considered and more logical.

So a consumer who has complete trust in an organisation might give permission to use his or her personal information without thinking about it.

But as noted earlier, trust in organisations is generally not strong at the moment.

Our survey illustrated this. We asked respondents 'How concerned, if at all, would you be that an organisation would do any of the following after you had given them your contact details?' and listed amongst the options, was the statement: 'Not keep to their promise in their permission statement'. Across all of the studies, 52% of respondents said they were very concerned about this, and another 30% said they were fairly concerned.

So if trust at this basic level is lacking, then individuals consider – using 'slow' thinking – what the motive for asking for information is. They think about why a company wants their personal information.

In our research we asked respondents to indicate if the statement 'I understand why a provider needs my information' was applicable to them. Only 27% thought so.

So, lacking both trust and comprehension, consumers worry that an organisation's motives for gathering the information might be self-serving rather than in their own best interests.

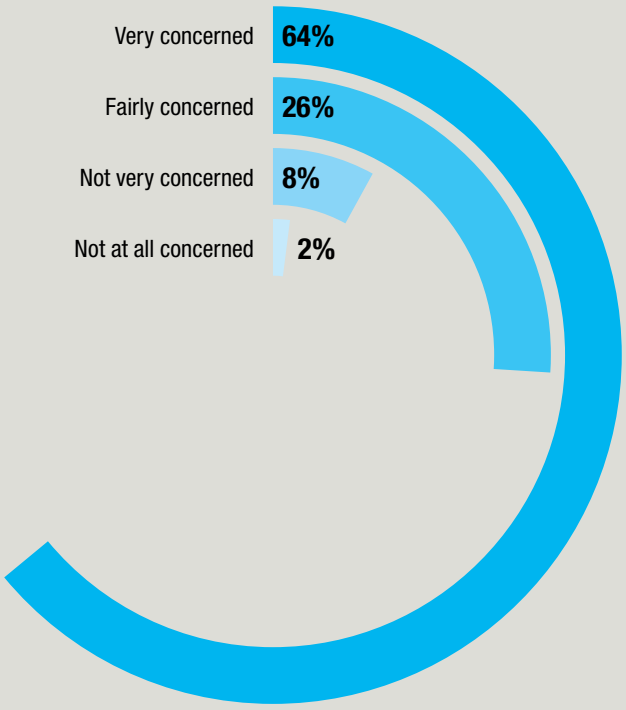
This expressed itself in two primary concerns: 'pass(ing) on my information to third parties', and 'contacting me too often'.

PASSING ON MY DETAILS TO THIRD PARTIES

One of the other options we put forward as part of the question 'How concerned, if at all, would you be that an organisation would do any of the following after you had given them your contact details?' was 'Pass on my details to third parties'. The percentage of people and the intensity of feeling (the proportion saying 'very' concerned rather than 'fairly' concerned), were both high.

Q: How concerned, if at all, would you be that an organisation would do any of the following after you had given them your contact details?

A: Pass on my details to another organisation.



Base: 6,923 All Permissions respondents.

Clearly the vast majority of people dislike the idea that a company they have chosen to engage with will use their information as a commodity to be sold, traded or passed on to other unknown organisations.

This concern may arise because passing a customer's information on is seen to be putting their personal information at risk in the hands of less competent organisations. It may simply be seen as unfair; why should the company financially benefit from something they had been given for free (and in a deal which they did not transparently tell the customer about)? But it may be more basic than this.

Ultimately, passing on personal information could appear to be a betrayal of our basic beliefs about privacy.

It's important to fully consider this point: however concerned a consumer might be about a chosen supplier using their data for its own marketing, they are more concerned about its decision to share it with others.

So failing to protect an individual's privacy is a key issue that degrades the intent component of trust for an organisation. This suggests that those organisations which do not pass on consumers' personal information should say so in a clear, impactful manner. If information is passed on for legitimate reasons only, then it is worth considering testing a 'transparent' approach which explains to whom and why this is being done (e.g. keeping insurance premiums down by preventing fraud).

CONTACTING ME TOO OFTEN

An additional concern was that if a respondent gave an organisation their contact details, it would 'contact me too often'. 43% of respondents were very concerned about this, and 40% were fairly concerned.

This suggests that respondents feel that providing contact details would not lead to more relevant, timely and appropriate communications; just more of them.

This is understandable since some companies have employed direct communications simply as an 'always on' channel to drive short-term gain. Arguably, the low cost of digital communications has worsened this. It's clear that in a more protective data regulation environment, the consumer will need to be convinced that when a company asks for his or her contact details, it intends to use it sensitively and in a mutually beneficial manner. It will be the quality, not the quantity, of communications that will ultimately obtain and maintain consent.

COMPETENCE

The second half of the trust equation is competence. In this context, this relates directly to the belief that an organisation is capable of holding personal information securely.

Reports of online data security breaches from governmental and commercial organisations are regularly in the news.

And it's not just personal data. Sony is hacked, and private emails and films are stolen.[7] Kaspersky Labs has uncovered a phishing scam whereby 'an Eastern European hacker ring is stealing an estimated $1 billion from banks by infecting computers with malware and siphoning money'.[8]

And as the Snowden affair illustrates, even governments are not able to protect their most confidential data. It can feel that any time an individual provides personal information or even touches the digital world, a mark is left somewhere that criminals can hack and abuse.

Closer to home, our research suggests that 1 in 4 of us believe we have been the victim of some form of data security issue.

In our surveys we asked respondents 'In the past 12 months have you experienced any of the following personal data security issues?' 26% said yes and listed problems ranging from unrecognised payments on their accounts to notifications by the supplier of a data breach.

But concern about data security is a magnitude greater than the actual experience of it. 71% of our sample said they were either fairly or very concerned (47% very concerned, 24% fairly concerned) that an organisation could lose their contact details.

7. '**Hollywood in crisis mode over Sony Scandal**' – CNBC, 11 December 2014.
8. '**Bank Security Is So Bad That a Simple Phishing Scam Can Cost $1 Billion**', Kate Knibbs, 16 February 2015.

In a data-sharing world, data security is evolving from a purely operational matter to one that has an essential marketing role. This point may seem obvious, but its implications are both surprising and important.

Telling customers about the secure systems used to hold consumer data is of value. In some of the surveys, we asked about the confidence supplied by a website that appeared to have good security controls, and this received an extremely positive response. So if you hold data securely, say so.

Trust – as defined in its component parts of intent and competence – is the primary factor that continues to inform consumer attitudes towards providing permission to hold and use their data. Given this, understanding and managing the trust your customers have in your organisation is perhaps the most urgent task for companies to address.

THE DATA TRUST LANDSCAPE

Trust is at the core of the personal information issue, and this research has identified three external factors that provide a set of expectations of where this trust is to be found. These factors are: consumer based, sector based, and relationship based.

CONSUMER BASED FACTORS

Across all sectors, our survey samples were nationally representative by gender and age. We found that roughly 30% of our respondents had a gross (before tax) household income of under £20K, 46% had £20-£50K, and 14% had over £50K (similar to TGI data), with 10% not answering the question.

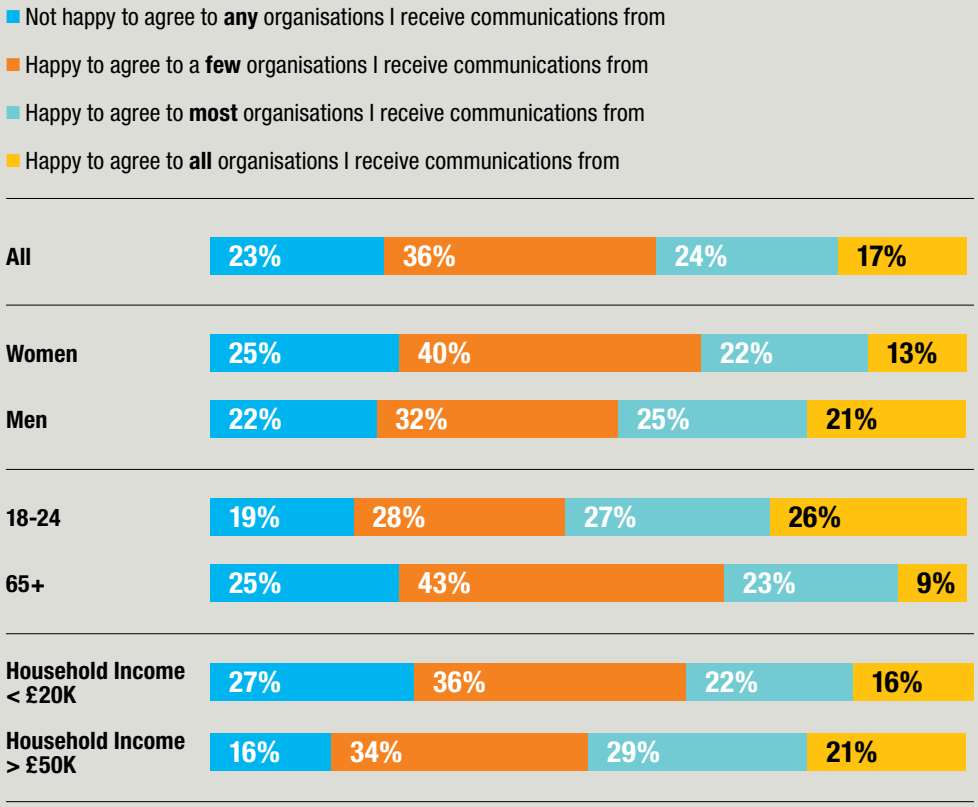
And across a wide range of questions, we could see that these factors showed a strong correlation with attitudes and behaviours.

In its simplest terms, the patterns of response could be defined as follows:

- Older people were more cautious, careful, and concerned about the use of their data than younger people.
- Women wanted more reassurance and messages of security and were generally more reluctant to allow companies to hold and use their information than men.
- Higher paid people were more confident, more willing to allow companies to use their data, and less concerned than our least well-paid segment.

This pattern was consistent across the surveys.

Q: If the organisations that currently send you information about products and services contacted you to ask you if you were happy to stay on their mailing list, what would your response be?



Base: 6,923 All Permissions respondents. Numbers don't add up to 100% due to weighting.

Clearly, these figures show tendencies only. Every sub-group has representatives in each of the four answers.

Various theories can explain the differences in these findings. They include digital natives vs. digital immigrants, baby boomers vs. millennials and traditional gender differences in relation to risk-taking.

It may be simply experience. Younger people may be more familiar with giving their details to lots of organisations (apps, for example) and see it as normal in today's world. Wealthier people may have purchased more products and services that have asked for permission, and therefore normalised the behaviour more than others. They may also have interacted with more upmarket organisations that tend to work harder to reassure and satisfy their wealthy customers.

Interestingly, 32% of respondents who had experienced a data security issue – and these were significantly more likely to be male, younger (under 35), and higher earners – stated that they would be happy to leave their personal data with all the organisations they receive communications from. This is in contrast to only 17% for the sample as a whole and only 13% of those who have not experienced a problem.

SECTOR BASED FACTORS

While trust can be conceived on a macro level, it also operates on a micro level. For example, a B2B organisation may be viewed as generally trustworthy. The quality and quantity of the work supplied, its ability to hit deadlines and its responsiveness to changes may all be good and build a general image of trustworthiness. But it may have a particular behaviour that is not satisfactory; reconciling invoices, for example. So measuring its trustworthiness as a brand (rather than at a component level) may obscure particular problems.

We believe this is certainly the case within the B2C personal data arena, as we shall see below.

When recruiting respondents for our surveys we screened on the basis of behaviours that were relevant for that study e.g. bill payers of energy or current account customers. Many of our respondents had the appropriate qualifications to be included in many if not all of the surveys.

Being asked about specific brands in a sector as part of the screening process meant that when respondents answered the first general question – about receiving information from 'any organisation' – their minds were firmly on that specific sector. So we saw a sector effect, as shown in the graph below illustrating the answers in the Telecoms and Retail Banking surveys.

Q: If the organisations that currently send you information about products and services contacted you to ask you if you were happy to stay on their mailing list, what would your response be?

Base: All Permission respondents 6,923, Telecoms 1,000, Retail Banks 1,000 current account customers.

With the sector image in their mind, it's not surprising to see that people in the retail banking survey were much less open to receiving communications, than people in the telecoms survey. Given the battering that banking has taken in the media since 2008, it is fairly safe to say that trust in the retail bank brands versus the trust in brands in other sectors may be low.

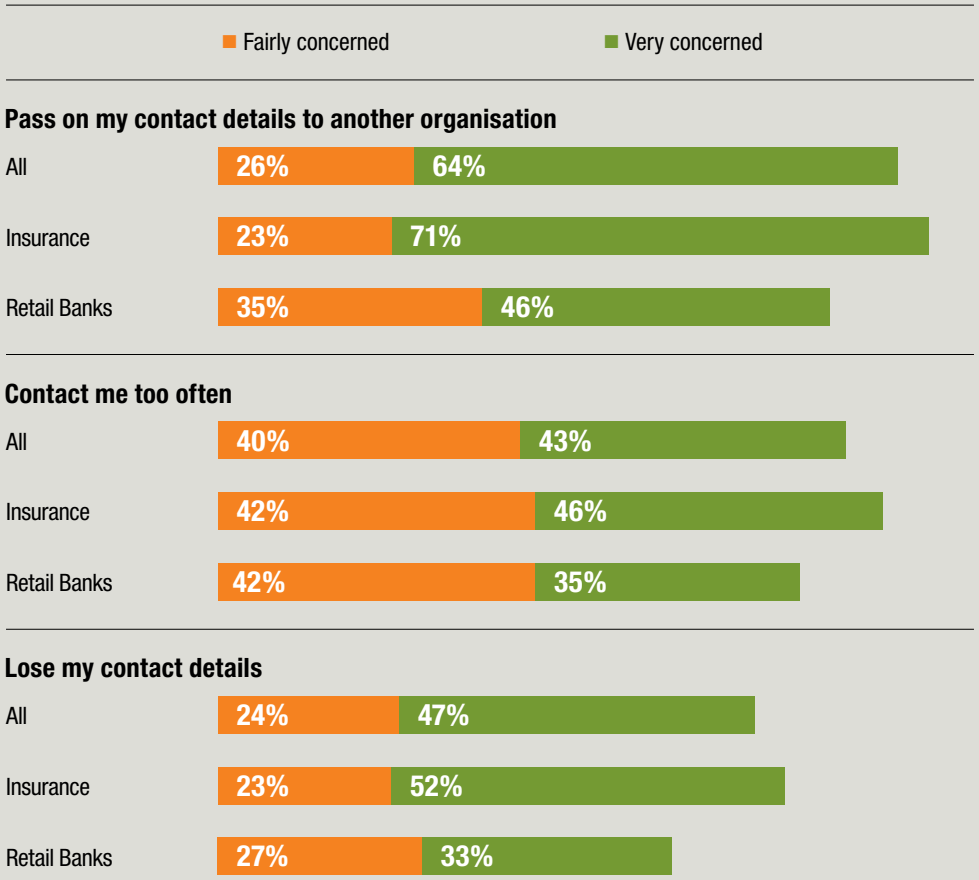
But when asked about specific concerns – a bank losing their data, passing it on to other organisations, or even contacting them too often – the banks tended to be assessed better than the average across the sectors.

It may be that perceptions of banks as a sector generally, and perceptions of banks regarding the use of data specifically, are not identical. We suggest that it may be important for brand marketers to measure trust in individual components, e.g. value, service, accuracy, and trust to hold data – in order to assess the environment for permissions requests.

In this context, our findings opposite must be seen as relevant not to the sectors overall, but to the perceptions of the specific sectors, in terms of their use of personal data.

The chart opposite illustrates how two different financial service sectors generate very different levels of concern regarding data privacy and security.

Q: How concerned, if at all, would you be that an organisation would do any of the following after you had given them your contact details?



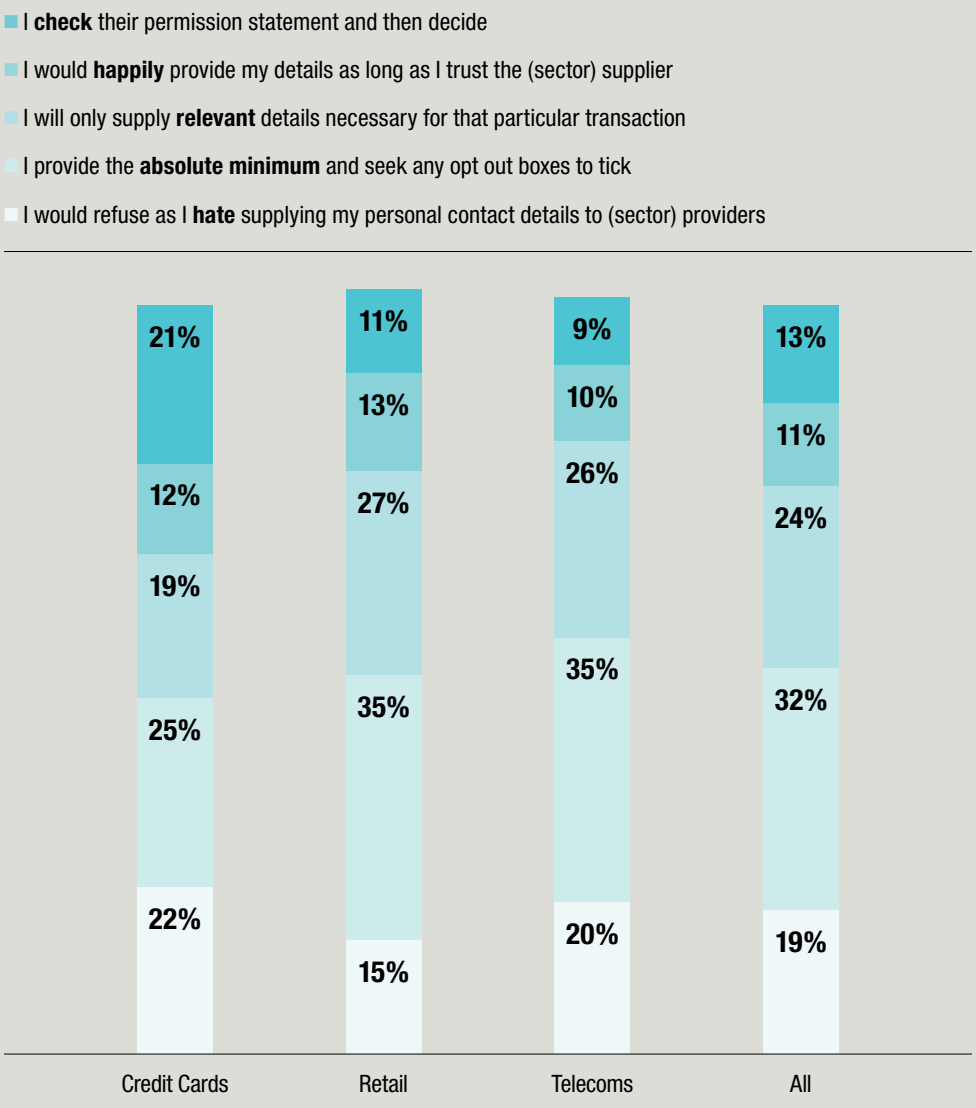
Base: 6,923 All Permissions respondents, Insurance 1,000 customers, Retail Banks 1,000 current account customers.

We also saw sector differences in a question that we revised part way through the survey.

In three sectors – Credit Cards, Retail, and Telecoms – we asked respondents how they would feel about supplying their personal contact details to any organisation in the sector, as follows.

Q: If an organisation were to ask you to supply your personal contact details so they can send you information about new products, sales and special offers, which of the following statements best describes how it might make you feel?

(Credit Cards, Retail and Telecoms)



Base: All 2,876, Credit Cards 876, Retail 1,000, Telecoms 1,000. Numbers don't add up to 100% due to weighting.

Clearly, then, the sector in which an organisation is seen to operate will help determine the 'lie of the land' for data permissions challenges.

RELATIONSHIP BASED FACTORS

It's logical to assume that in an open, competitive market, people are more likely to trust their current suppliers with their personal information than others, and our results confirmed this. But there are many variables to consider.

In our research, we covered markets where respondents may have had only one provider relationship (e.g. an energy supplier, or a credit card supplier) or many provider relationships (e.g. retailers or charities). The lengths of these relationships may have varied by decades, depending on the sector. Some people may even have experienced a rebranding of their provider – such as when Midland Bank became HSBC or Mercury Telecommunications became Virgin.

Because of these complexities, we discriminated between sectors when asking the importance of relationships. In the Telecommunications, Energy, Retail Banks and Credit Cards surveys, we asked respondents how happy they were to receive marketing material from 'My current supplier'.

Q: Which of the following types of (sector specific) providers/suppliers would you be happy to send you information about new products and special offers?

Base: Total 3,920, Telecommunications 1,000, Energy 1,044, Retail Banks 1,000, Credit Cards 876.

When asking the same question in the surveys for the other sectors (Retail, Insurance and Charities) we asked the same question but replaced 'My current supplier' with 'Suppliers I have used before' which was open enough to include both current and previous relationships.

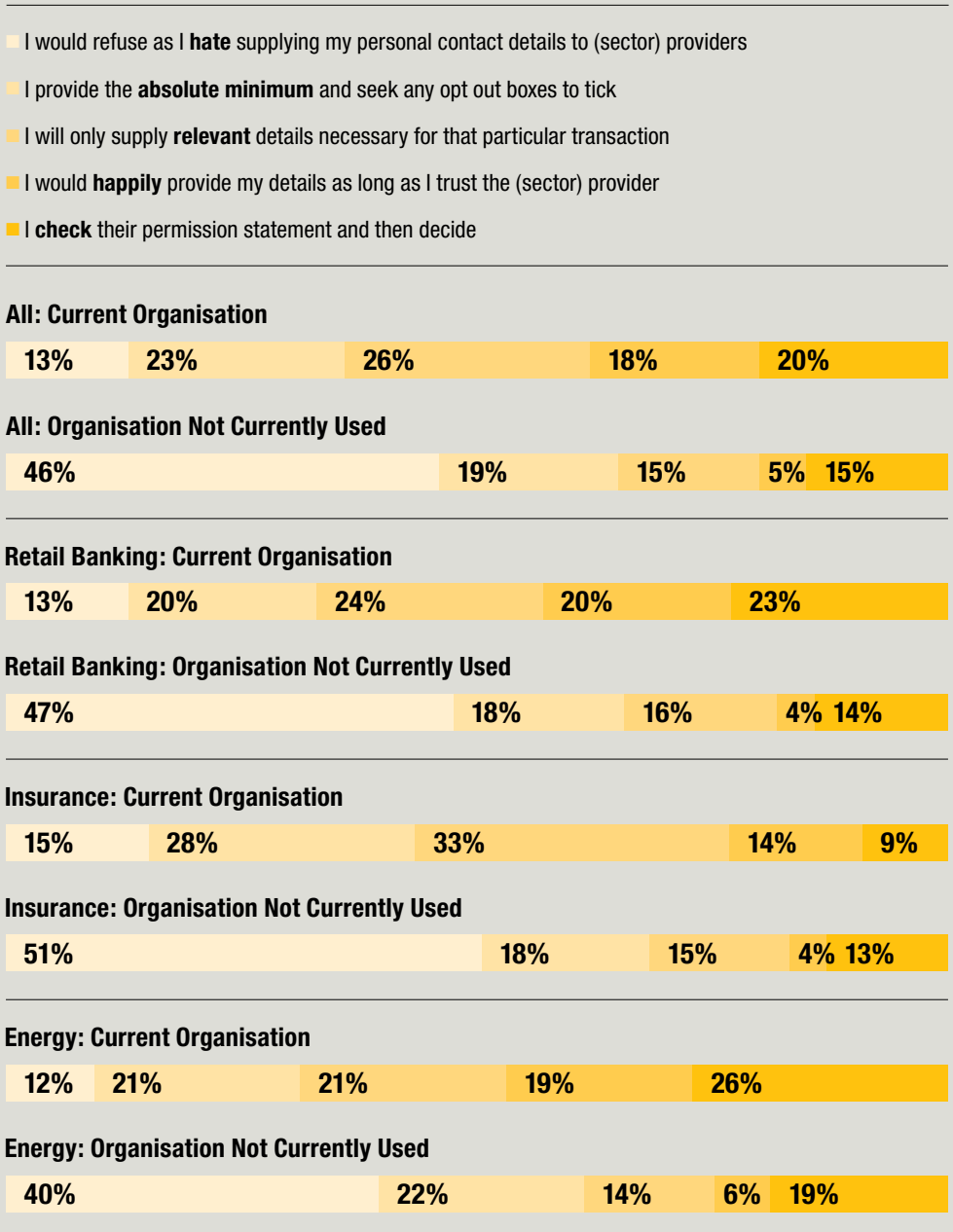
Although slightly less positive, 46% of the respondents in these surveys also indicated that a previous relationship was important in encouraging them to listen. Again, it was respondents in the Insurance survey that had the least positive score: only 40% selected this option.

Quite clearly there is a 'home field' advantage.

Customers were also likely to provide a bit more information to existing suppliers, and to be more open generally. The chart below indicates that without a relationship of some sort, respondents were more selective with giving their contact details.

Q: If an organisation were to ask you to supply your personal contact details so they can send you information about new products, sales and special offers, which of the following statements best describes how it might make you feel?

(Retail Banking, Insurance, and Energy)



Base: All Permissions respondents 3,044 (Retail Banking, Insurance, Energy), current account customers 1,000, Insurance customers 1,000, Energy customers 1,044.

As the results show, existing relationships matter a great deal when asking for personal details, even with minor variances between the sectors we measured. But we believe there may be many more substantial variances based on the strength of individual brands (within the specific context of data privacy and security).

We suggest undertaking more extensive research with robust samples of an individual organisation's customers and those of its key competitors. This may shed more light on the challenge that lies ahead.

GAINING PERMISSION FROM YOUR CUSTOMERS

THE PROBLEM WITH PERMISSION STATEMENTS

Opt in or opt out, online or off, it's natural to see granting permission as a solitary event.

Of course this is not technically correct. Even today, customers can withdraw permission and opt out of communications at any time.

But many people, particularly existing customers, have experienced a series of touchpoints with a brand that builds up a brand perception. These experiences influence their answer when they are asked a data permission question (along with the content of the question itself).

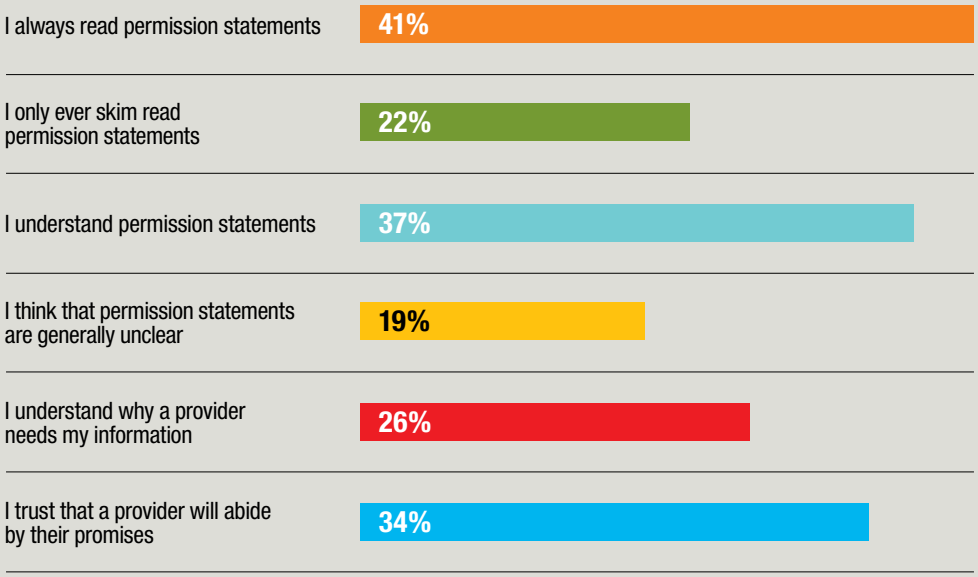
Moreover, the decision to 'opt in' or 'opt out' may not be overly influenced by the permission statement itself; because not all are read, understood or considered.

As an example: when installing a new application on a computer or phone, we're often confronted with a link to a Terms and Conditions page and forced to tick a box saying we have read and agree to them. But do we always read all of these documents carefully and with consideration before we click yes? Taking the time to study Ts & Cs is not particularly rewarding. And even if we try, they can often seem incomprehensible.

The same is true of data permission statements.

We asked respondents about their attitudes and behaviours when faced with permission statements today:

Q: Please can you read the following statements and tick the ones that apply to you.



Base: 6,923 All Permissions respondents. Multiple answers allowed.

One obvious conclusion should be that thought needs to be given to the creative execution of the actual permission information and response mechanism, to better engage consumers.

Julia Porter, DMA Chair and The Guardian's Director of Consumer Revenues, speaking at the DMA's Data Protection Day 2015, described the challenging internal process undertaken there to deliver a simple, unambiguous permission statement.

Delivered as a short video, the communication required a great deal of cross departmental work and cooperation – not simply from marketing, data, CRM and revenues teams – but also from a legal, risk and editorial perspective. But the result was a communication with creative cut through and which worked within the framework of both the financial model and corporate values of The Guardian and its owners, the Scott Trust Limited.[9]

9. Julia Porter, Director of Consumer Revenues, The Guardian and Chair of the DMA. Thoughts taken from her speech entitled: 'Having it both ways – trusted brands and big data', presented at the DMA Data Protection Day 2015.

But while asking effectively is undoubtedly important, it is only part of the solution. Impactful creative execution, multi-channel response opportunities and journey timing may substantially improve the relevant figures in the previous chart. But no matter how well you ask, relying solely on messages surrounding the request for permission cannot fully address the problem: many people will fail to read them, understand them, or trust the organisation to live up to them.

The implication is that in order to succeed, existing communication programmes need to begin to build the case for permission long before they ask for it. Continual and consistent messages over time – whether overt or discreet – will build a foundation so that when the question is formally made, there is a greater likelihood of success.

These messages will need to address data related trust issues effectively, and make a clear argument as to the benefits of continuing to receive communications from the organisations by demonstrating relevance and value.

The question then becomes one of content; what information should be communicated to most effectively create the right foundation?

WHAT KIND OF CONTENT – PULL OR PUSH?

In years gone by, salesmen were often taught about the role of push or pull sales tactics. Pull referred to increasing the customers desire for a product. Push messages were about addressing the barriers to purchase.

For example, a car salesman might be taught to emphasise the unique selling points – top speed, luxury and social status of a vehicle – to pull a customer in. However, to close the sale he or she might need to push them over their barriers to purchase. The content of his or her sales pitch might turn to high miles per gallon, safety or easy payment terms.

In our research we examined the importance of both pull and push content.

PULL MESSAGES

Across the different surveys we asked respondents in what circumstances they might be willing to give their details. They were offered different kinds of pull offers in exchange for their details – they might get discounts, exclusive offers, the opportunity to join rewards programmes, or receive information that would help them save money. Each questionnaire was tailored to a particular sector, so the results are not directly comparable; but overall, these offers of a value exchange were persuasive to many.

In the Energy survey, for example, 65% of respondents said they would be happy to give their details to an energy provider in exchange for discounts or special offers, and for incentives such as energy efficient light bulbs. In the Retail survey, 58% said they would give their details for money off vouchers, and 50% would do so in exchange for free samples.

These findings suggest that a pull approach – which recognises that customers know their information is valuable and will exchange it for a transparent benefit – will have a role to play; particularly at the time of asking permission.

But there are reasons to be cautious about applying this approach on its own.

Firstly, an incentive might work well to increase a response rate on a direct response campaign from 1% to 2%. But the scale of consent required to maintain an efficient, contactable database is on a different level. The cost of incentives powerful enough to persuade only 50%, 60% or even 70% of an existing database could threaten the financial health of any organisation.

Secondly, providing a value exchange may have little impact on trust. So while it might work for some people in the moment, it doesn't address the fundamental issue of trust and so may not be a solid foundation for an on-going relationship.

Therefore, the role that value exchange can effectively play in gaining permission will be significant but limited, if the components of trust are not already in place.

PUSH MESSAGES

Push messages help overcome barriers to action. And as long ago as 1979, Daniel Kahneman and Amos Tversky published a seminal paper entitled 'Prospect Theory: An Analysis of Decision Making Under Risk.'[10] In it, the authors demonstrated through clinical research that people are more motivated by the threat of loss than the possibility of gain. Prospect theory has been reviewed and refined again and again over the intervening years, and its core thought has stood the test of time.

In the context of consumer data, we have shown that many people are worried that allowing organisations to hold and use their personal information may cause them harm. That harm may be imagined as financial loss through some form of identity theft, or as simply the feeling of lost privacy.

We asked respondents what messages would give them confidence that an organisation would handle their contact details responsibly. Given prospect theory and the scale of concern people have, it was not surprising that both the percentage of people and the intensity of feeling (the proportion saying very important rather than fairly important) of the responses were high.

10. '**Prospect Theory: An Analysis of Decision Making Under Risk**', Daniel Kahneman and Amos Tversky, Econometrica, March 1979.

Q: How important are each of the following in giving you confidence that an organisation will handle your personal contact details responsibly?

Base: 6,923 All Permissions respondents.

Indicating that something is 'very important to give me confidence' is not the same as saying 'if I am confident, I will provide permission'. But the scale and intensity of these responses means it is fair to assume that addressing these concerns will be a crucial part of building and maintaining the trust that will help generate positive responses when customers are asked.

And what is perhaps most important is that these factors can be communicated today. Actions include showing good security measures on a website, making contact details clear, explaining that your organisation adheres to the Data Protection Act, saying you have put in place both powerful data protection policies and practices, and – perhaps most importantly – if you do not share customers personal data then say so. These are all things that can be put in place now. And they can be repeated again and again well before any new legislation is agreed, much less put in place, laying the foundations for a successful permission request.

All of this does not negate the potential usefulness of offering a value exchange of some sort at the time of asking for permission. Ultimately, both pull and push content will have a role to play – but push messages can and should begin today.

IF YOU HAD TO ASK FOR PERMISSION TODAY

In this research we explored four content territories using draft permission statements. The exact statements evolved throughout the study both to match the particular sector we were studying and as a result of insight gained from survey to survey.

The territories were as follows:

1. Security/Privacy

In these statements, we highlighted aspects such as a declaration that their personal information would not be shared with a third party, that it would be well-protected in a secure system and/or that it would be held safely according to the Data Protection Act.

2. Communication Control

Highlighted in this territory was the opportunity for the individual to opt out of communications at any time, and in some cases the chance for the individual to state how they would prefer to hear from the organisation.

3. Value Exchange

These statements said that the customer was valued by the company, and highlighted the benefits the individual would receive if they provided their personal information. These included exclusive offers, discounts, money-saving advice and tips and tools. In some, it was mentioned that the more the company knew about the individual's preferences and needs, the more valuable and relevant the communications would be.

4. Basic

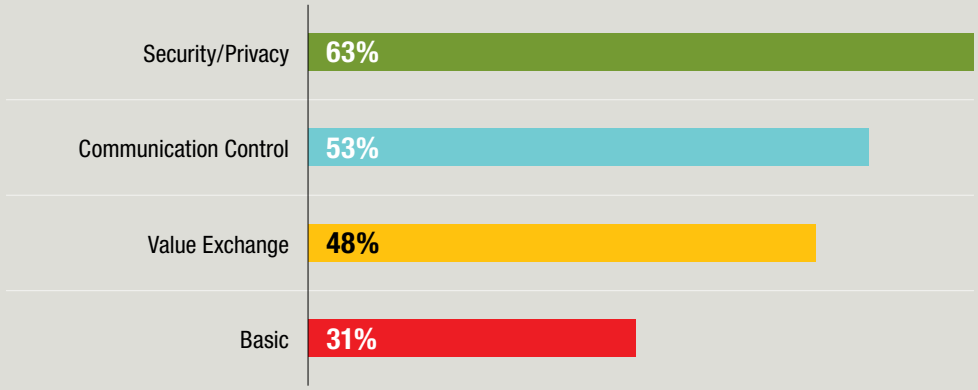
This statement was designed to offer a straight, administrative approach. It communicated nothing more than saying 'We'd like to hold your personal details in order to send you information about our services and offers.'

Given that the statements were not identical from survey to survey, combining the response is not statistically appropriate, and the responses shown opposite must be interpreted with caution. But given the relative consistency across the individual surveys, we believe the results are fair and indicative.

In each survey, respondents were shown the statements one at a time (rotated in presentation) and asked 'If you were asked for your permission like this by a (sector specific) supplier, would you tick the box?' The results were as follows:

Q: If asked for your permission by a (sector) supplier like this, would you tick the box?

A: Those that said yes to each statement

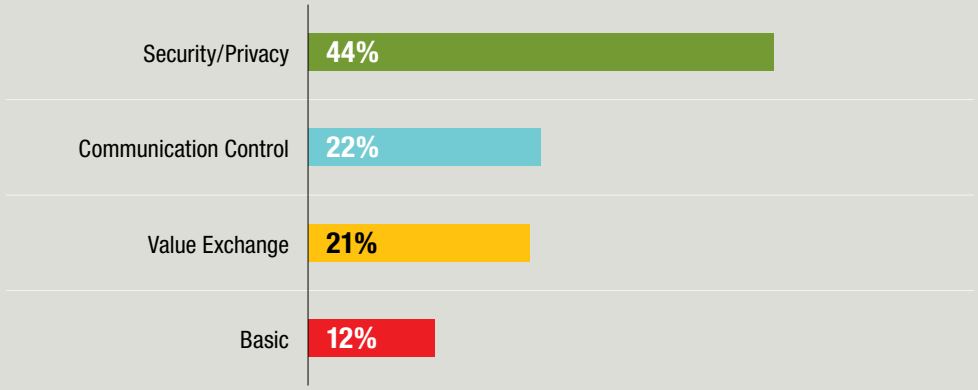


Base: 6,923 All Permissions respondents.

After all four statements had been considered, respondents were then asked to rank the statements in order of likelihood to agree.

Q: Please rate the permission statements in priority order based upon how likely you are to agree to each?

A: Most likely to agree with

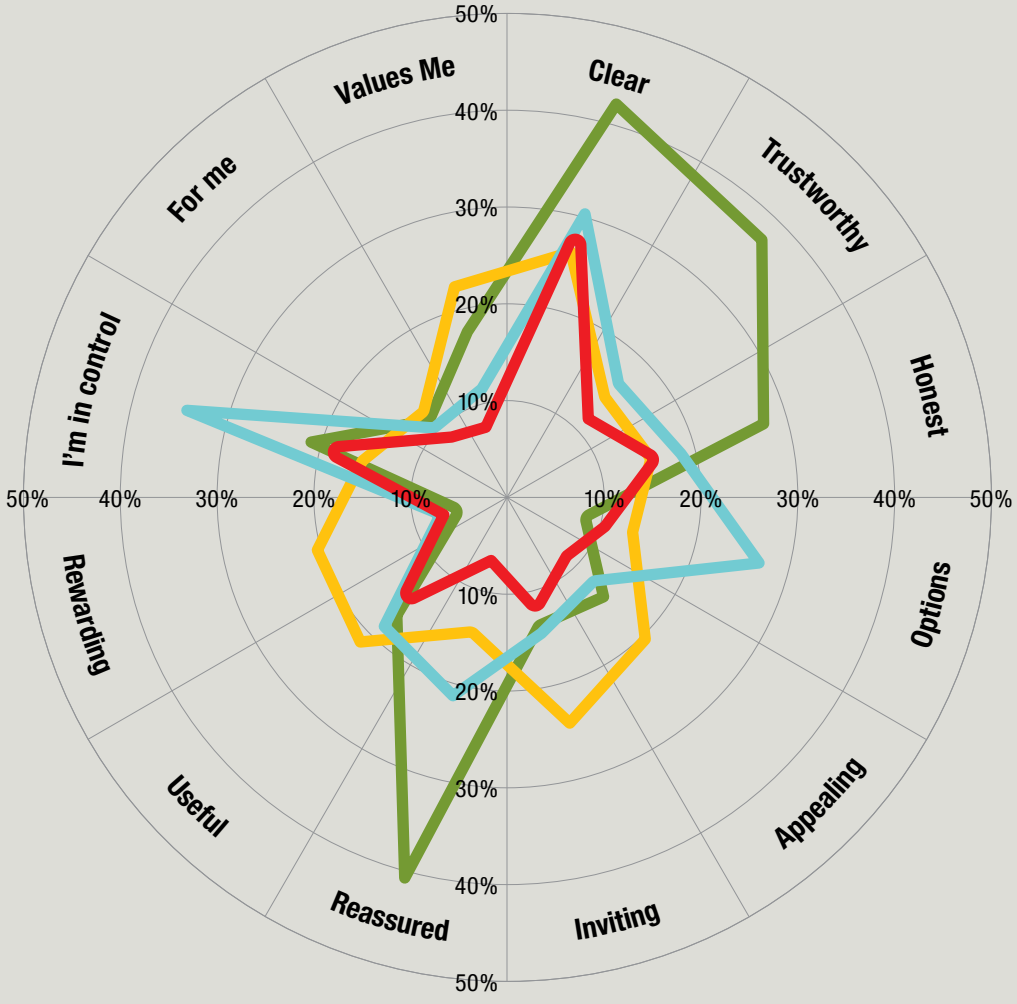


Base: 6,923 All Permissions respondents. Numbers don't add up to 100% due to weighting.

Finally, the respondents were asked to identify words which they would associate with the statement that they had ranked as the one they were most likely to agree with.

Q: Which of the following words do you associate with this statement?

A: Those who ranked the statement most likely to agree with



Base: Security 3,041, Value Exchange 1,485, Communication Control 1,541, Basic 853.

The Communication Control statements gave their supportors a strong sense of 'control' (38% of those who preferred this statement associated it with 'I'm in control'). The Value Exchange statements were most 'inviting' (25%), 'useful' (22%) and best communicated the feeling that the organisation 'values me' (23%). Clearly these routes are worth testing.

But the Security/Privacy statements scored significantly higher in key trust dimensions by both implying it (clear, trustworthy and honest) and creating the corresponding emotional response (reassured).

Combining the results from the different Security/Privacy, Value Exchange and Communication Control statements means these findings are open to challenge. But given the consistency across sectors – and with the rest of the findings in this report – we believe they are well worth reporting.

Taking them into consideration, we feel confident in suggesting that addressing both the intent and competence components of trust is the most effective approach to gaining permission, whether today or tomorrow, but that offering both control of communications and some form of value exchange should be tested as well. It may be that a multi-message communication campaign staged over time may result in the most effective approach of all.

THE ROLE OF MAIL IN GAINING PERMISSION

"What digital media hasn't changed is people. We are still physical creatures that thrive on human contact and stimulation. Giving, receiving and handling tangible objects remain deep and intuitive parts of the human experience. In the never-ending stream of two-way virtual communication, sending a direct sensory experience of your brand can mark a pivotal moment in the customer journey."[11]

Over the past 18 months Royal Mail MarketReach has carried out extensive research which demonstrates the powerful role that mail has within a multi-channel communications programme.

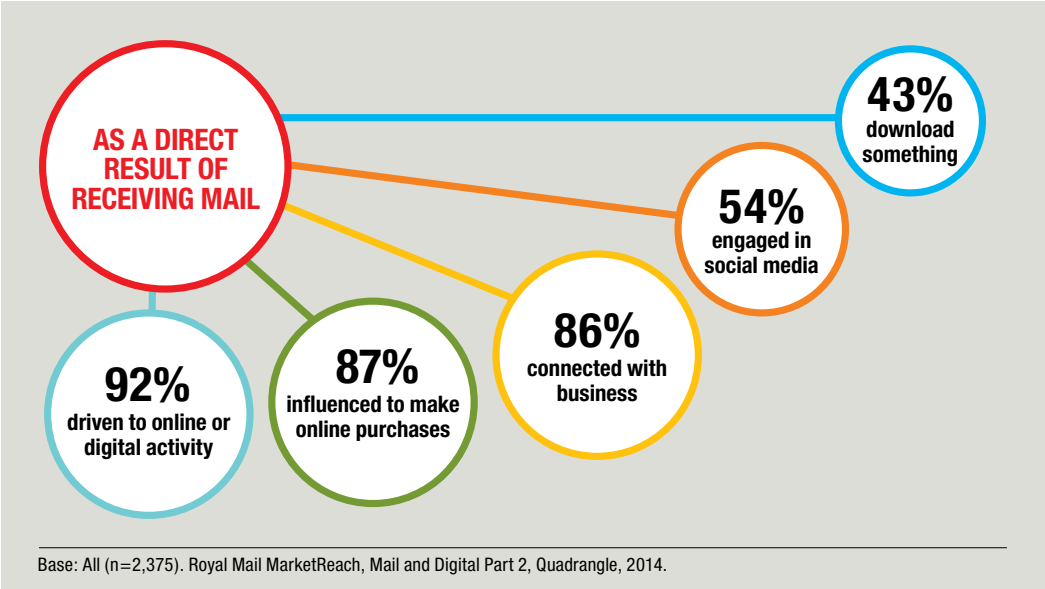
As behaviour between on and offline worlds is increasingly integrated, research showed that if people were given a choice to be contacted by post or email or a combination of the two, 51% of respondents preferred a combination of email and mail. Add to this the 17% who indicated that they wanted to be contacted by mail alone, and we have 68% of consumers looking for communications by mail.[12]

11. Royal Mail MarketReach, Private Life of Mail, 2015.
12. Royal Mail MarketReach, Mail and Digital Part 1, Quadrangle, 2013.

MAIL DRIVES ACTION

What's interesting is that mail drives considerable action to online activity, with an overwhelming 92% of consumers going online as a result of receiving mail. It drives purchasing and connection with businesses.

And mobile is making it easier than ever for people to do this.



Base: All (n=2,375). Royal Mail MarketReach, Mail and Digital Part 2, Quadrangle, 2014.

In fact, mail and email make a very compelling partnership.

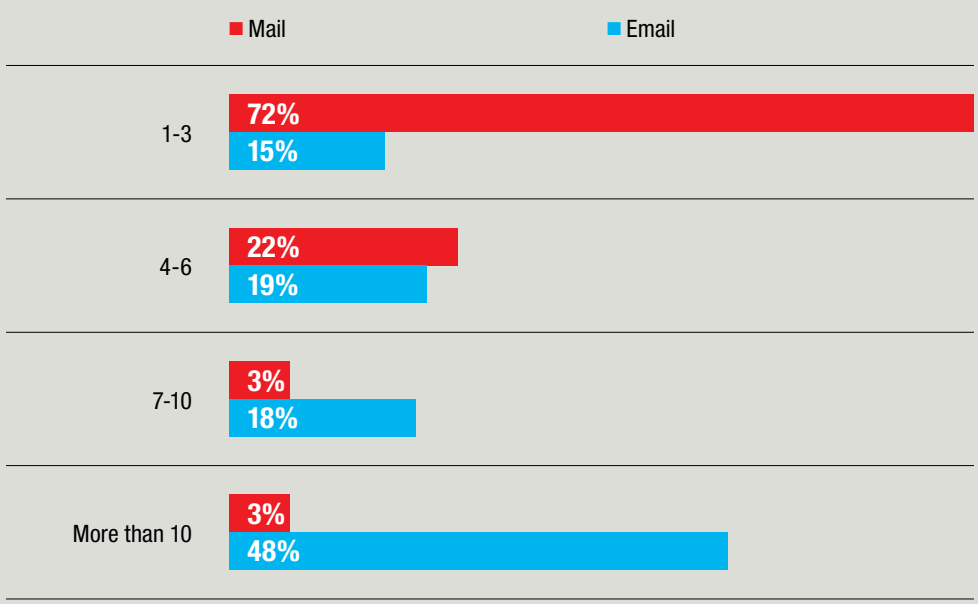
Our extensive research also identified other qualities that mail provides for the delivery of important messages: cut through and impact.

MAIL DRIVES CUT THROUGH

Getting someone's attention continues to be one of the biggest issues marketers have. As you can see from the following chart, mail is received at fairly modest volumes on a daily basis, with 72% of individuals receiving 1-3 mailings on a typical day. However 48% of people are getting more than 10 emails a day (compared to only 3% receiving this much mail).

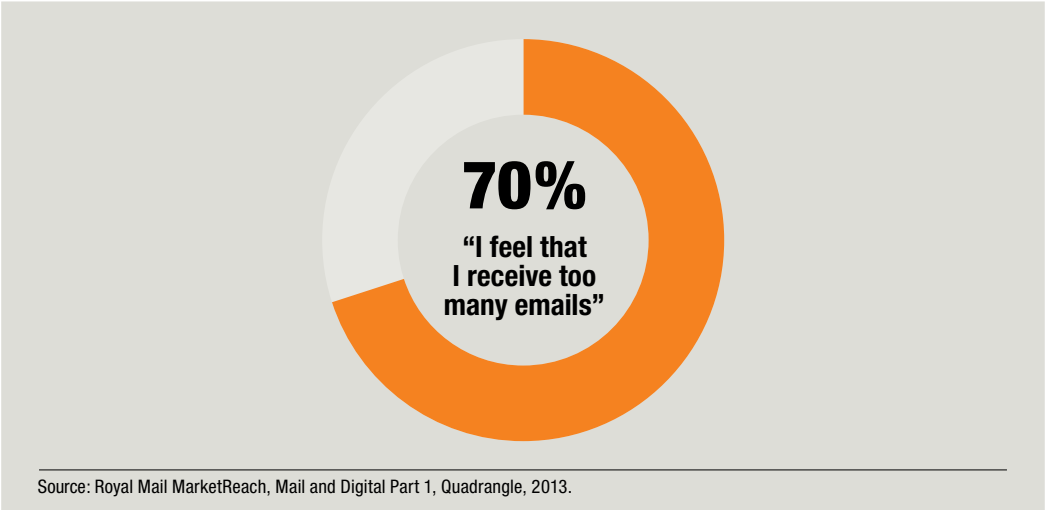
This suggests on a number of levels that mail is much more likely to achieve cut through and get noticed.

Q: How many items do you receive in a typical day?



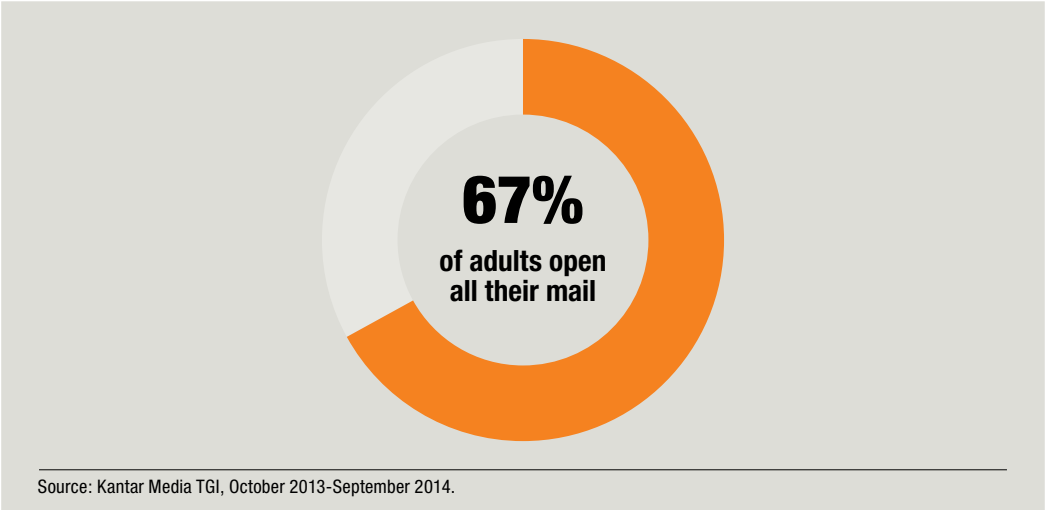
Source: Royal Mail MarketReach, Mail and Digital Part 1, Quadrangle, 2013.
Email is to personal inbox and excludes letters/emails from friends and family.

Our research also indicates that the volume of emails is a concern, with 70% of consumers saying they get too many.



Source: Royal Mail MarketReach, Mail and Digital Part 1, Quadrangle, 2013.

On the other hand, TGI informs us that 67% of all adults open all their mail. Add to this the number who open most of their mail and it rises to 84%.[13]



Source: Kantar Media TGI, October 2013-September 2014.

13. Kantar Media TGI, October 2013-September 2014.

Turning to another industry source, IPA Touchpoints, mail commands a great deal of attention, with adults spending on average 22 minutes a day reading their mail. By comparison, magazines are read on average 14 minutes a day.[14]

But that's only part of the story.

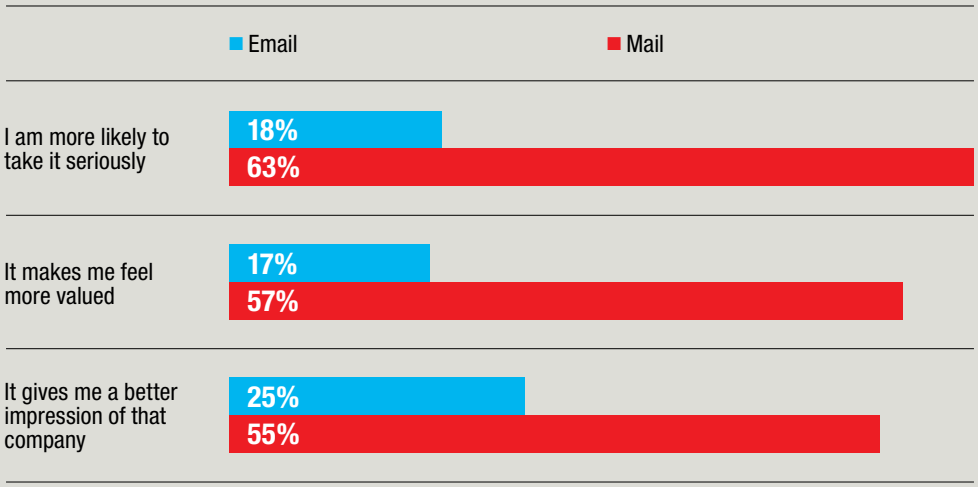
MAIL DRIVES IMPACT

Our research also suggests that cut through is not the only property that means mail really gets through to consumers. We also wanted to understand what consumers felt about mail and the messages that they received through the post versus those they get by email. Email has different properties than mail because it is associated with being spontaneous, quick and informal versus mail as considered, believable and personal.[15]

In comparison to email, mail commands gravitas, with 63% of consumers saying they are more likely to take it seriously. Coupled with the fact that 57% of people say it makes them feel more valued by the organisations sending mail to them – you can see that mail has the potential to play an important part in a communications strategy.

Finally, as mail also creates a better impression of a company (55% of respondents), mail is a clear front runner when you need to have an important conversation with your customers.

Q: Thinking just about the messages you get from businesses, please tell me whether you think [statement] is most true of mail, or of email in your opinion?



Base: UK consumers 1,000. Source: Royal Mail MarketReach, Mail and Digital Part 1, Quadrangle, 2013.

14. IPA Touchpoints 5, 2014. Data based on Monday-Saturday reading.
15. Royal Mail MarketReach, Mail and Digital Part 2, Quadrangle, 2014.

These findings show that mail creates a different profile from email: in terms of how people felt about the *communication*, how they felt about the *relationship* between themselves and the company, and how they saw the *company* itself. These qualities are important in a relationship building strategy that encourages customers to give consent to hold and use a consumer's personal information.

READ MORE ABOUT THE EFFECTIVENESS OF MAIL

Our recently published report 'The Private Life of Mail' is the result of 18 months of extensive research, including ethnography, neuroscience, and advertiser case meta-analysis. It's an unprecedented look at what happens after mail enters the home. To read more about everything from positive advertiser metrics to specific details of the neuroscience results, download the 'The Private Life of Mail' report from **www.mailmen.co.uk**

SUMMARY AND CONCLUSIONS

1. Lack of trust in organisations is a well-researched concern these days. The issue of trust plays a major role in consumers attitudes and behaviours regarding the use of their personal information by the establishments they interact with. Our findings confirm previous research into this problem. But it also brings into focus the component parts of trust:

   Trust in the competence of an organisation in this context refers to its ability to hold personal information safely and securely. In this arena, consumers are concerned about data security; that their information could be stolen, hacked, or lost and used to steal their identity and or money. Overall, 71% of our sample said they were concerned (47% very concerned, 24% fairly concerned) – that a supplier could lose their contact details. It is an issue of data security.

   Trust in the intent of an organisation relates to how an organisation will use the information and how this will affect the individual. Here, the issue is data privacy. Consumers are worried that an organisation will sell or swap their information to other companies that will either send unwanted material or fail to protect their information. 90% of our sample said they were concerned – 64% very concerned – that an organisation would pass on their details to another organisation. They are also concerned that the company holding their information will not use it to send better, more relevant and appropriate communications, but will just use it to send more.

   Addressing these trust issues is the key challenge to gaining permission to hold and use personal information.

2. This research identified three factors that influenced trust and customer readiness to give consent.

   Socio demographic factors

   We found that certain socio-demographic factors were associated with general attitudes towards giving or withholding personal information. Typically, older people were more likely to be resistant than younger people; women were more likely to be hesitant than men; and people with lower household incomes were more unwilling than those on higher incomes.

Sector factors

Our findings indicated that the customers of different sectors had different attitudes about giving information to suppliers in that particular sector. So the benchmarking of consent potential should be done at sector level.

An exceptionally important point arose from this comparison however; we began to understand that trusting a brand generally may not be directly related to trusting a brand to hold and use personal information. Thus overall brand trust measures may not reflect the opportunities or problems regarding consent.

Relationship factors

Unsurprisingly, people are more likely to give permission to organisations they currently have a relationship with than to those that they do not. But this is not uniform. This may be a factor of the sectors themselves, or the nature of individual/provider relationships. In some areas, an individual may have only one relationship; in others he or she may have many. Some relationships may last many years; others may change annually or more often.

Companies should consider conducting research on the specific issue of data trustworthiness across their key customer segments.

3. Our research established that organisations can and should begin to communicate messages that will increase the propensity of individuals to provide permission well before they are formally asked. Building data-relevant reassurances to create trust should be part of normal communications.

   This is particularly important because many people admit they do not read, understand, and consider the information in the specific permission requests. Improving the creative impact of these requests will help, but laying the groundwork first is an important task to begin today.

4. Many people seem to understand that their information has value and were willing to be ‘pulled’ into giving permission by a value exchange message. Others found that an overt offer of control over the communication programme was most likely to persuade them to give consent to their information being held and used.

   But our research concludes that many more have security and privacy barriers and will need reassurance that their information will be held securely and not shared.

Across all of the surveys we conducted, Security/Privacy based statements were chosen as the most compelling permission statement of the four we tested. Twice as many ranked this route as the one most likely to gain their permission (44%) than any other. Communication Control was ranked first by 22%, and Value Exchange by 21%.

Given this, we suggest that a permission programme should be based on testing these three territories – in isolation, combination, or over time – to find the most effective way of gaining permission. But we believe that enhancing trust will be key to success.

5. In a world where it is increasingly difficult to get someone's attention, mail provides cut through and impact. Comparing mail with email, receiving mail means the majority of customers feel more valued, have a better impression of the company and are more likely to take the communication seriously.

   These qualities are important for building a customer relationship and gaining consent for using and holding their personal information. With its ability to drive action, especially digitally, mail is a key channel for generating an effective permissions strategy.

ABOUT MARKETREACH: HOW WE CAN HELP

Royal Mail plc has emerged from one of the largest ever transformations of a UK business as a profitable, £9 billion revenue, FTSE 100 company. With that has come new capabilities and focus driven by our core beliefs.

The first is in the power of 1 to 1 communications. Mail and digital make a powerful combination. Digital has changed behaviour and inspired marketers to focus on 1 to 1. This has given mail a new role: helping organisations combine the instant gratification of digital with the reassuring authority of print.

Mail earns more 1 to 1 time with consumers, sticks more deeply in the memory and persists more strongly in the home. So when you use it as part of an integrated campaign or in targeted programmes, mail increases ROI.

Our second belief is that we only win when mail users and recipients also win; that's why we focus relentlessly on developing products and services that are right for modern direct marketers.

And thirdly, we believe in the power of partnership. We enjoy working alongside other marketers and their agencies towards a common goal – we'd like you to think of us as the direct mail experts within your wider marketing team. With our team of media specialists, planning and data experts who have a deep understanding of both direct mail and of your industry sector, we are well-placed to apply our tools and our insights to your business and your particular brief.

Call us on **0800 032 4880** to discuss how we can help or go to **www.marketreach.co.uk** to learn more about us.

NOTES

We have a team of media experts and data planners ready to apply these learnings to your organisation.

To discuss how we can help you, call us on **0800 032 4880** or visit **www.mailmen.co.uk**

Royal Mail
MarketReach