Report of the Nuisance Calls and Texts Task Force on Consent and Lead Generation

Contents

Summary of actions recommended by the Task Force

The Nuisance Calls and Texts Task Force on Consent and Lead Generation was convened by Which? at the request of the Department of Culture, Media and Sport (DCMS), following the publication of the DCMS Nuisance Calls Action Plan in March 2014. The work of the Task Force is not intended on its own to solve the problem of nuisance calls; our proposals are designed to be complementary to, and should be read in conjunction with, the other initiatives underway as a result of the DCMS Action Plan.

The Task Force has focused its attention on how organisations use consumer consent to carry out direct marketing activity and to buy and sell potential customer leads. We strongly believe that consumers should not be confused or misled by requests for their consent, and businesses should make sure that they only purchase personal data which has been legitimately obtained.

Our recommendations are designed to help reduce the incidence of unwanted calls and texts received by consumers by improving the ways in which marketing organisations, regulators and government treat consumer consent to receive direct marketing by telephone and text.

We want more organisations to raise their standards of practice in these areas. This will require businesses, and the individuals who lead them, to demonstrate a commitment to putting consumers back in control of their personal data and protecting them from nuisance calls and texts. It also requires regulators to work together, to enforce the rules and to provide more practical guidance, and for the Government to provide leadership.

Action for businesses: Improving direct marketing practices

Recommendation 1: Businesses should treat compliance with the law on consumer consent to direct marketing as a board-level issue in the context of corporate risk and consumer trust, and should consider actively joining and promoting accreditation schemes aimed at preventing nuisance calls and texts.

Recommendation 2: Organisations that engage in marketing activities should, as a minimum, commit to implementing the Information Commissioner's Office (ICO) guidance in relation to collecting and buying in data. They should specifically make the following clear in their policies and procedures:

a. ICO guidance about informing other companies in the data chain when a consumer wants to opt out of all marketing calls or texts must be followed. This should include providing a way for consumers to easily revoke their consent.

b. Businesses carrying out marketing activity should view the ICO guidance on a six-month time limit for third party consent as a minimum standard and take further steps to ensure its implementation. Businesses that rely on third party consent should satisfy themselves that the consent was not obtained from the consumer more than six months before it is first used by doing the appropriate due diligence checks.

c. Third party consent will not be sufficient to override Telephone Preference Service (TPS) registration, and businesses that purchase leads must screen all telephone numbers obtained from third parties against the TPS unless the company making the calls has been specifically named.

d. Businesses should record standard information as proof of consent (as recommended by the ICO) in a format that can be used by future recipients of the data.

Action for industry bodies

Recommendation 3: Codes of conduct produced by industry bodies should require members to follow good practice guidance on obtaining, recording and sharing consent for marketing, with reference to ICO guidance where appropriate. Member organisations that breach these requirements should be held to account.

Actions for regulators

Recommendation 4: The Competition and Markets Authority (CMA) should take account of the findings of the Task Force and our recommended actions in any work it undertakes on the commercial use of personal data. This should include identifying systemic consumer harm or protection issues. We recommend that the CMA should work closely with the ICO and other regulators where appropriate to understand the issues and to identify action that could remedy problems.

Recommendation 5: The ICO should build on its existing direct marketing guidance to offer further good practice solutions to the causes of nuisance calls, including:

a. A model approach, tested on consumers, to privacy notices and consumer communications which exemplifies best practice for providing information to consumers. This should include wording for opt-in, opt-out, third party consent, and information on controlling and revoking consent in the future. The aim should be that this becomes the industry standard for compliance with the law, and easily recognised by consumers.

b. Clear guidance that consent for marketing practices should always be separate from consent for other business practices. If consent for marketing is a precondition for a consumer offer, for example when entering a competition, it must be made clear how this transaction can be completed without providing consent for marketing.

c. A practical guide, produced in conjunction with representative groups such as the Federation of Small Businesses, the British Chambers of Commerce and the National Council for Voluntary Organisations, to enable organisations of all sizes to comply with the law but with a particular focus on helping SMEs and small charities, including a checklist of requirements for marketing organisations to help them purchase 'safe' leads.

d. Further work with industry bodies to develop an interoperable standard format for recording consent.

Recommendation 6: The ICO should work with industry bodies to develop technical solutions to enable and standardise the process of consumers revoking their consent.

Recommendation 7: The ICO should undertake regular reviews of marketing organisations' practices, including by undertaking mystery shopping, and conduct further analysis of complaints data to ensure compliance with their rules and guidance. Analysis and intelligence should continue to be shared with other relevant bodies to prioritise enforcement action.

Recommendation 8: Ofcom should assess the current level of consumer awareness and understanding of the TPS, for both fixed and mobile phone users. In light of this evidence it should consider whether more should be done to increase consumer awareness by, for example, renaming the TPS, launching a consumer awareness campaign, or finding other channels to further promote the service, such as how to engage consumers with TPS when they sign a new mobile phone contract.

Recommendation 9: Sector regulators and the ICO should work closely together to ensure that their conduct rules and requirements take full account of ICO guidance on direct marketing, and should hold to account businesses that do not comply.

Actions for government

Recommendation 10: The Department of Culture, Media and Sport, and the Ministry of Justice, should review the ability of the ICO to hold to account board-level executives who fail to comply with rules and guidance on the use of consumers' personal data for marketing purposes, and amend legislation to give the ICO further powers as necessary.

Recommendation 11: A cross-sector business awareness campaign should be led by DCMS and BIS, bringing together businesses demonstrating best practice in this area, regulators such as ICO and Ofcom, and consumer groups.

Recommendation 12: DCMS should undertake a review of the Nuisance Calls Action Plan in Spring 2016, including an assessment of the impact of these recommendations, and consider whether further steps are necessary.

Recommendation 13: In conjunction with evidence and recommendations from the CMA and other regulators, the Government should consider how future legislation, particularly at a European level, might be used to tackle nuisance marketing.

Recommendation 14: The Government should consider the potential impact on consumers of nuisance calls and texts by undertaking privacy impact assessments during the development of policy.

Recommendation 15: Public authorities should support the take-up of accreditation schemes such as TPS Assured by taking them into account during the procurement process for call centres.

Introduction

Unsolicited calls and texts cause significant nuisance, annoyance, and in some cases distress for consumers.

There has been increasing activity to tackle this issue in recent years as the volume of consumer complaints has grown, including an inquiry by the Culture, Media and Sport Select Committee and the All Party Parliamentary Group (APPG) on Nuisance Calls, along with investigations and enforcement proceedings by the relevant regulators. Yet the evidence shows that the problem remains unresolved.

The Department of Culture, Media and Sport (DCMS) published a Nuisance Calls Action Plan in March 2014. This included a request for Which? to convene a Task Force to review consumer consent and lead generation issues, as they relate to nuisance calls and texts. Confusion about consumer consent to receive direct marketing calls and texts, and the activities of businesses that generate 'leads' for direct marketing, were identified as key issues in the DCMS Action Plan.

Which? invited representatives of industry, regulatory and consumer bodies to form the task force in order to bring together a diverse range of perspectives and expertise. Meetings included a session in Parliament with the APPG on Nuisance Calls. The Task Force also issued a call for evidence and proactively invited responses from organisations and individuals.

The Task Force was given a specific remit to identify practical measures to reduce nuisance calls and texts within the scope of existing legislation, with a focus on voluntary action but an awareness of when changes to legislation might be necessary.[1] This is due to the fact that new Data Protection regulation is currently being discussed by the European institutions.

1. The Task Force terms of reference can be found in Appendix 2

Consumer consent and lead generation in the context of nuisance calls and texts

Recent statistics show that there are still high numbers of calls and texts being sent in breach of the existing legislation. At our session with the in Parliament, MPs told us that this issue is an ongoing concern for their constituents.

The Information Commissioner's Office (ICO) continues to report high volumes of complaints about marketing calls and texts but, given only a small proportion of consumers make a formal complaint to the regulator, it is likely this only represents the tip of the iceberg in terms of consumer detriment.

Which? research in April 2013 found that over eight in ten (85%) people received an unsolicited call every month, and Ofcom research at the start of 2014 found similar levels of nuisance calls.[2] As the report of the APPG on Nuisance Calls states ***'however it is calculated, the number of unwanted calls is almost certainly over one billion per year'***. While the number of consumers that do complain is significant – for instance, since its launch in July 2013 almost 50,000 complaints have been logged via the Which? online complaints tool with approximately half going on to complain to a regulator – this is a fraction of the number of unwanted calls and texts received.

The ICO, as the regulator of the Privacy and Electronic Communications Regulations 2003 (PECR), has received large numbers of complaints about nuisance calls and texts. In the 2013/14 financial year, 126,206 complaints were received. Nearly half of these were about automated marketing calls and a third related to live sales calls.[3] These levels of complaints have continued through 2014, with 97,757 complaints about calls and texts in the first half of the financial year. Automated calls are still the main cause of concern, with numbers increasing every month until a peak in July 2014. Marketing texts make up a smaller but significant proportion of electronic marketing complaints, with 12,712 complaints received so far in 2014.[4]

There is a lack of hard evidence about the types of business behaviour driving consumer complaints, such as the extent to which it is businesses openly and deliberately flouting the law, or companies unsure of their obligations or not following best practice. Some of the activity generating these complaints is clearly in breach of PECR, for example making automated calls for the purposes of direct marketing without specific consent. ICO data shows it is this activity that drives the most complaints. The Task Force believes companies making these calls may often be lead generators who will go on to sell any information obtained.

Because making automated calls without specific consent is so clearly in breach of PECR, we believe that some organisations making these calls are unlikely to be receptive to voluntary best practice steps, as they are already likely to be knowingly breaching legislation.

Sending marketing text messages without consent is also in breach of PECR. As with automated calls, it is likely that the organisations sending large numbers of unsolicited texts are knowingly breaking the law.

However, it is also likely that many nuisance calls and texts are generated by businesses that, rather than knowingly breaching legislation, are instead unclear about what compliance and best practice look like. This includes a lack of awareness about how to secure legitimate consent from consumers as well as ensuring that marketing data about potential customers bought from lead generators has been secured from consumers in accordance with the law.

Consent

The Task Force has looked at the nature of consumer consent to receive direct marketing – how it is obtained, recorded and shared – as part of its work. There are a number of key issues in relation to how consumer consent works in practice.

First, there is a lack of consistency in how consent is obtained from consumers. For example, some organisations require consumers to opt in to some marketing processes but opt out of others, during the same transaction. This inconsistent presentation of consent 'tick boxes' can be confusing for consumers. Furthermore, information about how data will be used is not always clearly presented or explained in plain language.

This results in a confusing environment for consumers which makes it difficult for them to give informed consent. The complexity of the information provided in terms and conditions, privacy notices and other tools for obtaining consent means that consumers often do not realise when they have given consent for their information to be passed on, or for third parties to use that information to contact them.

Secondly, consumers can sometimes be required to give consent to marketing – or they may be made to feel that they have to consent – in order to maintain a wider relationship with an organisation or complete a transaction.

2. http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/nuisance_calls_research/
3. http://ico.org.uk/about_us/performance/pecr_concerns
4. http://ico.org.uk/enforcement/action/calls and http://ico.org.uk/enforcement/action/texts

This is particularly worrying when consent to marketing is tied to registration for product safety notices and recalls or when registering product guarantees.

Thirdly, companies buying personal data from other companies or lead generators rely on third-party consent which has been obtained by another business and sold on with the consumer's details. When consent has been given and data has begun to pass between organisations, it is difficult for consumers to track their data and revoke their consent should they wish to do so. Organisations are often unable or unwilling to provide consumers with proof of their consent to carry out marketing, despite ICO guidance recommending that businesses record details of how consent was obtained.

Given that the consent model relies on consumers taking some action to agree to marketing activity, such as completing a transaction or ticking a box, it is often argued that the straightforward solution would be to improve consumer awareness of what they are consenting to. While consumer awareness initiatives are certainly a good thing, insights from behavioural science suggest there will be significant limitations to what they can achieve.

As part of its work, the Task Force reviewed the behavioural literature relevant to privacy and consent.[5] The evidence on consumer decision-making in relation to privacy indicates that consumers are not always aware of the implications of giving consent for marketing practices. Real consumer behaviour does not match the hyper-rational consumer of economic textbooks and the complexity of the issues involved mean that consumers often rely on shortcuts to make decisions about consent, and rarely read the detail of disclosure policies.

This means that consumer choice can be influenced by seemingly small details (such as the wording and design of requests for consent) and also that consumer decision-making in this area is likely to be inconsistent and unpredictable. There is potential for consumers to give their consent unwittingly, or to do so without realising the consequences. Protecting consumers in this context is not straightforward, particularly as there are also many situations in which a consumer may actively want to receive marketing for a period of time from some businesses.

Given that many consumers act unpredictably, effective solutions to the problem of nuisance calls and texts cannot rely entirely on consumers to change their behaviour; there must be a focus on business behaviour too, and this is the area which the task force emphasises in its recommendations.

Lead generation

Organisations planning marketing activity sometimes rely on lead generators to provide contact details and other information about potential customers. Lead generation companies obtain information through a range of platforms, sometimes legitimately and sometimes illegitimately, including through information submitted online, cold calling and spam texts. They sell this data to multiple businesses, some of whom might go on to share or sell the data to further third parties. Organisations also sell information about their own customers. This has led to a market in personal data which consumers may be completely unaware of, or find difficult to follow or understand.

There is a notable lack of transparency or evidence about the lead generation industry. However, lead generation companies appear to account for a substantial proportion of complaints about nuisance calls and texts. There is a legitimate market for lead generation, but responsible companies are in danger of being overshadowed by rogue businesses. For example, the bulk sending of automated calls and texts is a clear breach of the existing legislation. Regulatory enforcement can be an effective tool against the companies responsible, but the Task Force has looked for other ways to influence the behaviour of businesses which purchase leads.

We are concerned that the less reputable elements of the lead generation market continue to exist in part because there are too many companies willing – knowingly or otherwise – to use leads which have been obtained using unlawful or unfair methods. The wider market in personal data is something which would benefit from a more detailed examination to ensure that it is not unfairly impacting on consumers. Businesses should not be purchasing leads without conducting reasonable due diligence checks to ensure that consumers have properly consented to the sale of their data and that the lead was not obtained through unlawful marketing approaches.

There is relatively little practical guidance for businesses on how to conduct due diligence when acquiring leads or other direct marketing services.[6] Smaller businesses in particular might not have the resources available to devise and implement their own solutions. Industry bodies and regulators should therefore take a lead in providing guidance and practical help to organisations, and by doing so improve the overall standards of direct marketing practice.

5. See Appendix 5
6. The ICO's Direct Marketing guidance provides an outline approach for organisations buying marketing lists http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf

Actions recommended by the Task Force

3.1 Action for businesses: improving direct marketing practices

We know that there are numerous businesses conducting their marketing activity in a fair and transparent way. Legitimate marketing should not be restricted because of the actions of businesses that seek to avoid or undermine the existing rules.

While the lead generation companies that make calls or send texts in breach of the law should be subject to rigorous enforcement action, the companies that are offered these unlawfully-obtained leads also have a responsibility to take action to ensure compliance with the law. They should also be aware that using these leads leaves them open to potential enforcement action.

Unlike the lead generators themselves, the buyers of these leads are likely to operate in a regulated industry. Sectors driving the most nuisance calls and texts include accident claims, payday lenders and energy efficiency schemes, all of which are covered by some regulatory authorisation or rules.[7] These businesses need to do more to ensure they are using leads that have been fairly and lawfully obtained. This will be better for consumers, makes good business sense and should lead to a reduction in nuisance marketing by lead generators.

In general, the Task Force believes that more thorough due diligence by organisations buying leads or procuring marketing services will encourage the use of fairly obtained leads and reduce the number of nuisance calls and texts. The necessary behavioural changes must be driven from the top level in organisations. Senior executives and non-executive directors must understand that nuisance marketing is a serious issue for consumers, and that failing to address these issues leaves the door open to reputational damage as well as regulatory action.

Improving the consistency and clarity of how consent is explained to consumers should help them to understand how their information will be used. The Task Force has considered whether it is desirable to introduce standard wording for privacy notices or other privacy information provided to consumers. There was some concern that universal standard wording might have a negative impact on how businesses interact with their customers in particular contexts and relationships.[8] The Task Force accepts that many organisations will want to retain some flexibility.

However, on balance a move towards a common, easily recognised standard will benefit consumers and also assist organisations that are unsure of how to comply with best practice.

However, providing information to consumers at the time when they give consent can only be part of the solution, because of the difficulties that consumers have in understanding the implications of the information provided and the problems caused by data being continually passed between businesses. Consumers find it difficult to follow the trail of their data and to revoke consent from all the organisations which hold it.

Businesses should therefore do more to help consumers by taking reasonable steps to pass on revoked consent to organisations further down the data chain. Alongside improved privacy notices organisations should focus on providing better tools that enable customers to control their personal data. This should be considered when systems are being refreshed, or re-procured, following a 'privacy by design' approach. Whilst they might not have direct legal compliance responsibilities it is important that vendors of marketing IT systems offer better solutions 'out of the box'.

Businesses should also be more careful about the use of consent originally given to another organisation, because of the difficulties in ensuring that the consent is valid. The Task Force considered the application of stricter time limits to using information obtained from third parties. Treating an agreement to receive marketing from third parties as providing indefinite consent is likely to be unfair to consumers. The Task Force accepts that some flexibility is required to allow for different marketing contexts. As a result, we support the current position in the ICO's direct marketing guidance. This establishes a general rule that third party consent will be valid for six months from when it was first obtained from the consumer. This period of time allows organisations to send marketing and establish a customer relationship soon after obtaining consent, when contact is most likely to be expected and relevant to consumers.

Businesses should hold consistent records of the purposes consent has been obtained for, and how and when consent was obtained from each individual. Furthermore, businesses that buy data from lead generators must ensure that they have a record of consent. Where possible this information should be held in a format which allows it to be shared and used by other organisations in the data chain.

7. http://ico.org.uk/enforcement/action/texts and http://ico.org.uk/enforcement/action/calls
8. DMA response to call for evidence

Organisations that collect and use personal data for marketing purposes should ensure they provide specific information to help consumers understand how data will be used and enable them to make an informed decision. This includes clear, prominent statements explaining how consumers will be contacted and the types of organisations the data might be shared with.

The Task Force reviewed the guidance already available to businesses on using consent in a marketing context. The ICO's Direct Marketing guidance provides information on complying with the law and also includes several good practice measures.[9] Although the guidance is the ICO's interpretation of the law and does not necessarily have legal force, the Task Force takes the view that its guidance should be taken as the minimum standard for marketing practices.

Recommendation 1: Businesses should treat compliance with the law on consumer consent to direct marketing as a board-level issue in the context of corporate risk and consumer trust, and should consider actively joining and promoting accreditation schemes aimed at preventing nuisance calls and texts.

Recommendation 2: Organisations that engage in marketing activities should, as a minimum, commit to implementing ICO guidance in relation to collecting and buying in data. They should specifically make the following clear in their policies and procedures:

a. **ICO guidance about informing other companies in the data chain when a consumer wants to opt out of all marketing calls or texts must be followed. This should include providing a way for consumers to easily revoke their consent.**

b. **Businesses carrying out marketing activity should view the ICO guidance on a six-month time limit for third party consent as a minimum standard and take further steps to ensure its implementation. Businesses that rely on third party consent should satisfy themselves that the consent was not obtained from the consumer more than six months before it is first used by doing the appropriate due diligence checks.**

c. **Third party consent will not be sufficient to override TPS registration, and businesses that purchase leads must screen all telephone numbers obtained from third parties against the TPS unless the company making the calls has been specifically named.**

d. **Businesses should record standard information as proof of consent (as recommended by the ICO) in a format that can be used by future recipients of the data.**

3.2 Action for industry bodies

Industry bodies and trade associations have an important role to play in the promotion of best practice. The Task Force heard at its public evidence session that businesses can find the guidance produced by industry bodies to be more relevant and accessible than regulators' guidance.

Guidance from the main regulators is spread across various websites and documents, and is often written to address a broad range of sectors and activities. Industry bodies are able to provide sector-specific knowledge and identify exemplars of good practice for others to learn from. The Direct Marketing Association's code of practice was cited as an example of useful practical guidance.

Consumers should also have confidence that businesses that are part of a trade association are meeting a high standard of marketing behaviour. This means that businesses which fail to meet the required standards should be helped to comply and held to account by their peers for repeated or serious failings.

The Task Force urges industry bodies and trade associations with codes of conduct to ensure that their rules include measures to prevent nuisance calls. The good practice guidelines published by the statutory regulators should act as the minimum standard for voluntary industry body codes of practice.

Recommendation 3: Codes of conduct produced by industry bodies should require members to follow good practice guidance on obtaining, recording and sharing consent for marketing, with reference to ICO guidance where appropriate. Member organisations that breach these requirements should be held to account.

9. http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf

3.3 Actions for regulators

Regulatory bodies have a key role to play in tackling nuisance calls and texts. They need to provide clear guidance to organisations, backed up by enforcement action for non-compliance when appropriate. The Task Force has been encouraged by action taken against rogue marketing companies recently.

The ICO reported that monetary penalties issued for breaches of PECR had a clear deterrent effect and led to a reduction in complaints about other businesses in the related sector. Proposals to strengthen the ICO's power to fine companies are being addressed as part of the DCMS Action Plan. There are further areas where regulators can take more steps to provide guidance to businesses, to help consumers, and to work together.

The Competition and Markets Authority

It became clear to the Task Force during the course of our work that we would only be able to look at a small part of the significant market in personal data. Lead generation as a cause of nuisance marketing is just one aspect of an issue that engages a number of sectoral, regulatory and legislative contexts. It is clear that more evidence is needed on how the use of personal data is benefiting or harming consumers, including uses that comply with the basic requirements of the Data Protection Act.

The ICO is responsible for enforcing the Data Protection Act, with a focus on promoting good practice and investigating specific breaches, but it is not set up to investigate market features or general characteristics across different sectors. The Competition and Markets Authority is the regulator that is best placed to conduct a wider review into the market in personal data.

The CMA should be able to draw on support from the ICO in its investigations. In particular, the ICO should be able to provide some initial analysis of how the trade in personal data operates. This could include an overview of the key sectors and types of businesses involved in the obtaining, sale and reuse of personal data. The ICO should also be able to provide initial evidence of some of the practical aspects of this industry – the methods of data collection and transfer, and the types of security and compliance procedures already in place.

Recommendation 4: The Competition and Markets Authority should take account of the findings of the Task Force and our recommended actions in any work it undertakes on the commercial use of personal data. This should include identifying systemic consumer harm or protection issues. We recommend that the CMA should work closely with the ICO and other regulators where appropriate to understand the issues and to identify action that could remedy problems.

The Information Commissioner's Office

Effective regulation is not just about enforcement action. Regulators can educate organisations on how to comply with that law, and on how to go beyond the legal minimum to achieve standards of best practice. The Task Force believes that many of the companies engaged in marketing activity are doing so with the intention of complying with the law. However, we also heard from businesses that organisations are not always certain of what practical measures are required to meet standards of good practice.

The Task Force endorses the approach to PECR set out in the ICO's current direct marketing guidance.[10] The ICO intends to conduct a review of the guidance in the future, in line with its standard approach to new publications. The Task Force has some recommendations for supplementing the existing guidance with new tools to assist organisations in meeting best practice. Many of these complement the recommendations we make to organisations on good marketing practices.

The Task Force has not called for a compulsory standard wording for privacy notices, and accepts that organisations desire some flexibility. However there is scope for the ICO to produce a suggested wording which can be voluntarily used by organisations. Widespread adoption of such wording would help consumers to identify organisations that work towards the ICO's good practice guidelines. It is important that new approaches are tested on consumers to ensure that they have the desired effect of explaining what consumers are consenting to in a straightforward and understandable way.

The Task Force has identified the purchase of unfairly-obtained leads without due diligence checks as a key area for the ICO guidance to address. There are some sectors which are likely to benefit from some more specific practical guidance on this topic. Smaller businesses and charities are less likely to have experience in addressing this problem, and guidance aimed at those organisations should help them to comply with the law.

10. http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf

The ICO should use its position as the regulator and as a source of authoritative guidance to advocate standard approaches and products to help organisations record consent more effectively and assist consumers in revoking consent where desired. Organisations should be encouraged to record proof on consent in an interoperable format, and to provide simpler ways to revoke consent across the data chain. There is an important role for the ICO to play in helping to develop technical solutions in this area, but any form of industry standard needs input and support from a broad range of stakeholders.

Finally, the Task Force urges the ICO to continue to work proactively in tackling nuisance calls and texts, finding ways to research the market that might highlight emerging consumer detriment, and ensuring close collaboration with other regulators by sharing threat assessments and intelligence.

Recommendation 5: The ICO should build on its existing direct marketing guidance to offer further good practice solutions to the causes of nuisance calls, including:

a. **A model approach, tested on consumers, to privacy notices and consumer communications which exemplifies best practice for providing information to consumers. This should include wording for opt-in, opt-out, third party consent, and information on controlling and revoking consent in the future. The aim should be that this becomes the industry standard for compliance with PECR, and easily recognised by consumers.**

b. **Clear guidance that consent for marketing practices should always be separate from consent for other business practices. If consent for marketing is a precondition for a consumer offer, for example when entering a competition, it must be made clear how this transaction can be completed without providing consent for marketing.**

c. **A practical guide, produced in conjunction with representative groups such as the Federation of Small Businesses, the British Chambers of Commerce and the National Council for Voluntary Organisations, to enable organisations of all sizes to comply with the law but with a particular focus on helping SMEs and small charities, including a checklist of requirements for marketing organisations to help them purchase 'safe' leads.**

d. **Further work with industry bodies to develop an interoperable standard format for recording consent.**

Recommendation 6: The ICO should work with industry bodies to develop technical solutions to enable and standardise the process of consumers revoking their consent.

Recommendation 7: The ICO should undertake regular reviews of marketing organisations' practices, including by undertaking mystery shopping, and conduct further analysis of complaints data to ensure compliance with their rules and guidance. Analysis and intelligence should continue to be shared with other relevant bodies to prioritise enforcement action.

Ofcom

The Telephone Preference Service (TPS) is an important tool for consumers seeking to prevent nuisance calls. Live marketing calls account for a substantial number of complaints to the ICO, but PECR only permits organisations to make live marketing calls to a number if the subscriber has not registered their number with the TPS, or has given express consent to receive such calls.

The ICO and Ofcom have conducted research into the effectiveness of the TPS.[11] They found that TPS registration reduced the volume of live sales calls by around a third and also reduced other types of nuisance calls. There is a clear benefit to TPS registration and it should continue to be promoted to consumers as a beneficial service. Ofcom should continue to ensure that consumers are aware of TPS.

Increasing mobile phone subscriptions to the TPS should be seen as a priority. The Task Force heard that mobile phone numbers make up a small proportion of TPS registrations but make up a growing proportion of marketing calls. Ofcom and the TPS should investigate how to improve mobile number registration. The most obvious time to encourage mobile users to register would be when they sign or receive a welcome pack for a new phone contract.

Recommendation 8: Ofcom should assess the current level of consumer awareness and understanding of the TPS, for both fixed and mobile phone users. In light of this evidence it should consider whether more should be done to increase consumer awareness by, for example, renaming the TPS, launching a consumer awareness campaign, or finding other channels to further promote the service, such as how to engage consumers with TPS when they sign a new mobile phone contract.

11. http://media.ofcom.org.uk/news/2014/effectiveness-telephone-preference-service/

Other sectoral regulators

The Task Force has identified sectoral regulation as an additional way to promote good practice and take enforcement action against companies that break the law.

Complaints data from the ICO indicates that nuisance marketing activity has a tendency to concentrate around particular sectors. Marketing texts have focused on accident claims, payday loans and debt management. Automated calls have shown a recent surge in complaints about companies related to the Green Deal offering new boilers and other home improvements.

The companies doing this marketing are not necessarily businesses directly involved in the activities being promoted. Instead they can be lead generators attempting to obtain information which can be sold on to multiple businesses as potential customers. This is one of the ways in which personal information enters the market in data.

Lead generation companies operate in a relatively unregulated market which is difficult to research or penetrate. The ICO is able to take some enforcement action when it can identify serious offenders, but the problem will remain while the market in unlawfully obtained leads remains. The companies buying these leads are often more visible and operating in a more closely regulated sector. These companies must also change their behaviour and do more to ensure that they only buy leads which have been lawfully obtained and have a clear record of consent to receive further marketing.

Sectoral regulators have an important contribution to make to this line of work. These bodies are more likely to have a detailed knowledge of how their area works, compared with the ICO and Ofcom as more general regulators of nuisance calls legislation. Sectoral regulators should consider producing specific guidance on marketing topics for the organisations they oversee, and can use this to promote good practice. They should also consider using their enforceable codes of conduct to make compliance with good practice a requirement of doing business.

The Claims Management Regulator (CMR), a unit in the Ministry of Justice, has shown how sectoral regulators can tackle nuisance marketing. The CMR's Conduct of Authorised Persons Rules makes compliance with the Committee of Advertising Practice code and Direct Marketing Association's code of practice a requirement for their regulated businesses. This has the effect of creating more effective enforcement avenues for those codes. Analysis of complaints suggests that this step has led to improvements in the marketing practices of the CMR's sector.

The CMR's approach may not be appropriate for every sector, but the Task Force encourages sectoral regulators to promote the good practice guidance produced by the ICO and DMA. Where possible, sectoral codes should make this compliance an enforceable requirement and regulators should take action against businesses that continue to use unlawfully obtained leads.

Sectoral regulators will not necessarily have a detailed knowledge of PECR and data protection issues. The ICO is the authoritative regulator of these areas and we encourage them to work with sectoral bodies to improve their understanding of these topics and ensure that they are equipped to support the ICO's aims.

Recommendation 9: Sector regulators and the ICO should work closely together to ensure that their conduct rules and requirements take full account of ICO guidance on direct marketing, and should hold to account businesses that do not comply.

3.4 Actions for government

The DCMS Action Plan is a welcome step by the Government to address nuisance calls and texts, and the measures identified in the Action Plan must be implemented in full. This is a complex sector covered by several layers of legislation, regulators, businesses and activities, and it is essential that the Government continues to look at standards in the direct marketing industry as a whole.

The Task Force has focused on finding solutions that can work within the existing legislative framework.

However, one area which might require further legislation is the Task Force's recommendation that more is done to hold board-level executives to account. The Data Protection Act contains provisions which allow directors to be prosecuted for criminal offences committed by a company with their consent or because of neglect. This does not extend to the civil breaches of the DPA or PECR which cover unlawful marketing.

The nature of bulk marketing technology also means that it is relatively easy for an individual to close and re-establish a business. This poses particular challenges when trying to enforce the existing legislation.

The Task Force believes it is vital that board-level executives take greater responsibility for their companies' marketing methods. Making enforcement easier in this area should assist the ICO in putting a stop to nuisance calls caused by executive negligence.

Recommendation 10: The Department of Culture, Media and Sport, and the Ministry of Justice, should review the ability of the ICO to hold to account board-level executives who fail to comply with rules and guidance on the use of consumers' personal data for marketing purposes, and amend legislation to give the ICO further powers as necessary.

The Task Force has already highlighted the need for clear guidance on good practice and the importance of organisations meeting those standards. It should not be an excuse for organisations to claim ignorance of what is expected from them. We have suggested ways for the ICO to ensure that practical tools for improving compliance are available to businesses. The DCMS Action Plan will lead to other changes in regulatory and business activity. There should be further efforts made to ensure that all businesses are aware that conduct leading to nuisance calls is harmful to consumers and bad for the reputation of direct marketing.

A business awareness campaign should be launched to raise awareness of existing guidance, provide practical assistance to organisations, and establish a platform for developing technical standards and solutions. This should involve general publicity about guidance but could also include practical workshops or other events aimed at businesses. The Task Force believes that this campaign will be most effective if it is led by the Government. This reflects the fact that nuisance marketing crosses sectoral and regulatory boundaries, and will demonstrate the Government's support of the regulators' approach. The regulators should continue to have an important role in the campaign, and consumer groups should also be involved to represent the voice of consumers.

Recommendation 11: A cross-sector business awareness campaign should be led by DCMS and BIS, bringing together businesses demonstrating best practice in this area, regulators such as ICO and Ofcom, and consumer groups.

The DCMS Action Plan provided a range of potential solutions to nuisance calls. The remit of this Task Force means our recommendations can only address one element of the problem. The Action Plan contains a broader range of measures, all of which are necessary to reduce nuisance calls and texts. The Task Force has focused on the gathering of consent and the trade in personal data, but implementing other areas of the Action Plan will increase the protection of consumers from nuisance marketing.

It is therefore important that DCMS commits to a thorough review of this Task Force's recommendations and the wider Action Plan, to examine the impact of the current proposals and consider the need for further steps if nuisance calls continue to be a significant problem for consumers. Organisations engaged in marketing will need some time to implement the recommendations before a review is carried out.

The Task Force has not proposed significant changes to legislation because we believe that the existing laws can provide adequate consumer protection and allow legitimate marketing, provided organisations are committed to following good practice guidance. The voluntary measures we have proposed should be given a chance to work. However, the Government should be alive to the possibility of introducing new legislation if improvements in marketing practices cannot be demonstrated.

We are also conscious of the ongoing negotiations at a European level on a draft Data Protection Regulation. The new law may lead to changes in how organisations conduct marketing, and particularly on how they are able to use consent. The Government needs to consider how any new legislation can be used to protect consumers from nuisance marketing, and should ensure that the expertise of regulators is used to inform their position. This may require a more detailed understanding of how the market in personal data currently operates, which is why we recommend that a review by the CMA is done to provide further evidence for any future legislation.

The ICO has promoted privacy impact assessments (PIAs) as a process which can help organisations to understand how policies and projects will affect privacy.[12] PIAs are already in use across government as a tool to assist new projects. PIAs help government to understand the impact on consumers as well as on businesses of proposals for new marketing practices and regulation, and we encourage more government departments to use the process.

Recommendation 12: DCMS should undertake a review of the Nuisance Calls Action Plan in Spring 2016, including an assessment of the impact of these recommendations, and consider whether further steps are necessary.

12. https://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

Recommendation 13: In conjunction with evidence and recommendations from the CMA and other regulators, the Government should consider how future legislation, particularly at a European level, might be used to tackle nuisance marketing.

Recommendation 14: The Government should consider the potential impact on consumers of nuisance calls and texts by undertaking privacy impact assessments during the development of policy.

Finally, we believe that accreditation schemes for call centres, such as the TPS Assured, should be promoted as a way for organisations to demonstrate their commitment to best practice in managing consumer consent for direct marketing. Voluntary and self-regulatory systems encourage member organisations to adopt policies which can protect consumers. We think that the Government can do more to encourage organisations working with call centre providers to choose partners that are part of an accreditation scheme. As a starting point, we would like to see the Government commit all public bodies to taking membership of accreditation schemes into account when marketing services are being procured.

Recommendation 15: Public authorities should support the take-up of accreditation schemes such as TPS Assured by taking them into account during the procurement process for call centres.

Conclusions

The Task Force approached the issue of nuisance calls and texts from the point of view that current guidance and legislation could be used to better protect consumers. The recommendations presented here therefore set out a number of solutions that work mainly within current legislation and focus on how businesses, regulators and consumers can work together to make a real difference to the extent and impact of nuisance calls and texts.

Regulatory enforcement will always be necessary to tackle the behaviour of the worst offenders and create a deterrent to those who would deliberately break the law, but our solutions have been focused on organisations willing to do more to comply with best practice. Accreditation schemes, technical standards and practical guidance can all be used to establish better standards.

Throughout our work we have been encouraged by indications that the marketing industry is willing to be proactive in preventing nuisance calls and texts. But if voluntary measures and self-regulation do not work then more stringent legislation may be needed.

Regulators and government need to ensure that the right tools and guidance are available for the organisations that need them. The existing guidance provides the right approach to marketing activity, and the challenge is now to ensure that more organisations are meeting best practice instead of operating in the grey areas of the law.

Appendix 1: Task Force members and meeting dates

Task Force Members

Richard Lloyd, Executive Director, Which? (Chair)

Lynn Parker. Director of Consumer Protection, Ofcom

Steve Wood, Head of Policy Delivery, Information Commissioner's Office

John Mitchison, Head of Preference Services, Legal and Compliance, Direct Marketing Association

Jan Smith, External Affairs Director, CallCredit

Michael Bristow, Marketing Operations Manager, Barclaycard

Anne Marie Forsyth, Chief Executive, CCA Global Ltd

Kevin Rousell, Head of Claims Management Regulation, Ministry of Justice

Fiona Lennox, Executive Director, The Communications Consumer Panel

Mark McLaren, Parliamentary and Legal Affairs Manager also represented Which? at each meeting.

The secretariat for the Task Force was provided by Which? adviser Thomas Oppé.

Substitute Attendees

Jaya Chakrabarti, Member, Communications Consumer Panel (for Fiona Lennox on 9 July)

Rob Pike, Chair of Standards Council, CCA (for Anne Marie Forsyth on 9 July & 18 September)

Iain Bourne, Group Manager, Policy Delivery, Information Commissioner's Office (for Steve Wood on 5 August)

Task Force Meeting Dates 2014

Tuesday 27 May
Wednesday 9 July
Tuesday 5 August
Thursday 18 September
Tuesday 14 October
Monday 3 November

A note of every meeting was published shortly afterwards on the Which? website.

Appendix 2: Task Force terms of reference

As part of the Department for Culture, Media and Sport's (DCMS) Action Plan on nuisance calls, Which? has been asked to set up a Task Force to review how consumers give consent to being contacted by direct marketing firms. The Task Force aims to identify what is causing the most significant concern or detriment to consumers. It will make recommendations for practical and effective solutions.

These terms of reference set out the issues which the Task Force expects to address.

Consent and lead generation

The Task Force will consider issues in relation to consumers' consent to receive direct marketing by telephone calls, text messages, and email.

Specifically, the Task Force will consider:

- What improvements can be made to the language used when asking for consent.
- Whether a more consistent approach to obtaining consent across communications channels would be beneficial, and how this would be implemented.
- The separation of consent for marketing from consent for other business purposes (e.g. customer information notices, product recalls).
- Stricter controls on the use of third party consent, especially when overriding previous choices.
- Barriers to consumers tracking and revoking their consent.
- Information that might be recorded alongside contact details to improve clarity on the nature of consent.
- Ways for lead generation and companies engaging in direct marketing to improve governance of marketing activity, and to monitor and improve their practice.

The main focus of the recommendations are expected to be for the direct marketing industry and businesses conducting marketing activity to improve how they obtain and use consent, and how they use purchased leads.

The wider range of solutions which the Task Force may consider include:

- Recommendations to the marketing industry on how to promote and monitor good practice.
- Identifying the most suitable regulatory approaches and responses to complaints about consent and lead generation issues, and ensuring that regulators are able to work together to enforce the legislation.
- Highlighting the limits of voluntary actions, and where other action including possible new legislation may need to be considered to provide clarity for businesses and consumers.

Appendix 3: Task Force call for evidence

As part of the Department for Culture, Media and Sport's (DCMS) Action Plan on nuisance calls, Which? has been asked to set up a Task Force to review how consumers give consent to being contacted by companies.

The Task Force membership includes organisations representing businesses, the marketing industry, consumers, and regulators. The Task Force is also issuing this call for evidence so that other organisations and individuals are able to share their expertise in certain areas. The aims of the call for evidence are to understand the impact on consumers of issues surrounding consent to direct marketing and lead generation and the extent to which consistent and practical solutions can be applied.

We welcome evidence from any interested stakeholder focused on the questions below. We will also be identifying individuals at key organisations to feed into the consultation. A more general call for evidence will also be placed on the taskforce pages on the Which? website.

General questions for businesses

- What are the main reputational considerations in relation to direct marketing?
- Does the current legislation covering consent and lead generation provide enough clarity on how personal data can be used?
- How useful is the existing guidance produced by regulators or trade bodies, and is further guidance necessary?
- What is causing consumer complaints on this issue, and how can consumers be better informed about marketing choices?
- Is the approach to enforcement taken by regulators effective and proportionate?

Questions for businesses doing marketing (and their representative bodies)

- How significant is the role of buying leads in your marketing activity?
- When purchasing leads, what checks do you have in place to ensure compliance with the Data Protection Act and Privacy and Electronic Communication Regulations?
- How do you record proof of consent, dates of consent, or the source of information?
- If standards of consent were made consistent across communications channels, what would be the impact on your marketing activity?
- Do you use third-party consent (i.e. consent obtained by another organisation and passed on to you) as a basis for marketing?
- How do you approach potential conflicts between third-party consent and information held on the TPS or similar suppression list?
- To what extent might an industry-led code of practice on using lead generation bring clarity to this area and improve consistency between companies?
- What steps do you take to separate consent for customer data to be used for marketing purposes from information which can be used for other internal business practices?

Questions for lead generation companies (and their representative bodies)

- What internal compliance or governance processes do you use to ensure compliance with the data protection act and PECR?
- Is the law and existing guidance clear enough on how personal information can be used in the context of lead generation?
- Do you keep a record of how you have obtained and sold information, and could this be made available to consumers?
- How do you provide information to consumers about the use of their information?

Questions for consumers

- What makes you more or less likely to share your information with an organisation, or to agree to receiving marketing?
- Have you asked companies for more information about how they have bought and sold your personal information, and what was the result?

Responses were received from a wide range of interested organisations, MPs, and individuals.

Appendix 4: Nuisance Calls and Texts Task Force Background paper

Drivers of complaints about marketing calls and texts

Prepared by Which?

This paper reviews existing evidence and identifies the areas where the Task Force should focus its recommendations.

There is no single cause of complaints about nuisance calls and texts. Consumers might be contacted by companies they have an existing relationship with, or by an organisation they have never heard of. Personal data is collected for marketing purposes in various ways – some is entirely legitimate, some might be shared accidentally, and some might be obtained in a clear breach of legislation. This information can then be sold on to a variety of organisations which vary in size, sector, and willingness to comply with best practice. The type of communication and the content of a message (such as aggressive sales techniques) are also likely to affect the perceived level of detriment or nuisance.

What types of marketing are causing complaints?

Consumer complaints data

Graphs showing the types of marketing and the business sectors generating complaints to the ICO can be found in the appendix below. The ICO continues to report high volumes of complaints about marketing calls and texts. Complaints about sales calls, including live and automated calls, increased over the first three months of the financial year from 11,276 in April 2014, 13,500 in May to 15,890 in June. In this period there were 22,072 complaints about automated calls and 18,594 about live sales calls. Complaints reported about calls are at their highest levels since April 2013. [13]

The number of complaints received relating to text messages fell during the same period, with 2,601 reported in April 2014, 2,369 in May and 1,829 in June. This amounts to a total of 6,799 complaints. The proportion of complaints received about text messages has decreased, with 10% of all complaints about unsolicited marketing relating to text messages in June 2014, compared with 19% in April 2014. [14]

Automated calls made without specific consent are a breach of PECR. Companies making these calls are typically lead generators who will go on to sell any information obtained. This activity drives the most complaints but the organisations making automated calls are unlikely to be receptive to voluntary best practice steps, as they are already knowingly breaching legislation.

Marketing text messages sent without consent are also likely to breach PECR. As with automated calls, it is likely that the organisations sending large numbers of unsolicited texts are lead generators knowingly breaking the law.

Live sales calls can be made without consent but will breach PECR if the number called is registered with the TPS. Recent research showed that although TPS registration can significantly reduce the number of calls received, it does not eliminate them entirely. [15] This suggests that improving consumer awareness of the TPS would be likely to reduce the number of nuisance calls, but that there is also work to be done in ensuring that companies are properly screening against the list.

Consumer preferences

The legislation on direct marketing sets out the restrictions on its use and the circumstances in which it is allowed. However, this does not necessarily take account of how consumers might actually prefer to be contacted. Individuals are perhaps more likely to make a formal complaint if they are contacted in a way they find particularly annoying or intrusive.

The DMA's customer acquisition barometer suggests that consumers have a strong preference (77%) for being contacted by email.[16] Calls to landlines, mobiles, and texts were far less popular with consumers. The barometer also recorded the reasons for unsolicited calls being unwelcome. The most common reasons for a frustrating marketing call were that it was from an overseas call centre (32%), that the calls were too frequent (22%) and that the calls were not about relevant products (19%).

13. http://ico.org.uk/enforcement/action/calls
14. http://ico.org.uk/enforcement/action/calls
15. http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/tps/tps-effectiveness.pdf
16. http://www.dma.org.uk/research/customer-acquisition-barometer-2014-report

The report on TPS effectiveness found that consumers are much more likely to describe unwanted marketing calls as 'annoying' rather than 'distressing'.[17] The ICO is able to take enforcement action against a breach of PECR, but can only issue a monetary penalty where it can show that the breach was of a kind likely to cause substantial harm or distress. Qualitative feedback on distress is difficult to measure but the ICO's penalty notices do provide some examples of more serious cases, for example calls made to vulnerable people. The ICO has also issued monetary penalties on the basis that a large number of nuisance calls is cumulatively of a distressing nature.[18]

However, this interpretation has subsequently been rejected by the upper tribunal on appeal. Regardless of whether nuisance calls amount to a legal definition of 'distress' it is clear from the number of complaints that they continue to be an annoyance to thousands of individuals making complaints.

Which business sectors are causing complaints?

A small number of sectors are responsible for the majority of nuisance calls and texts reported to the ICO. In the most recent reporting period, accident claims, payday loans and debt management were the most complained about topics of text messages, with the numbers of concerns raised about PPI-claim messages falling from 581 in March 2014 to only 189 in June 2014 (compared with 395 in June 2013).[19]

For live calls, accident claims, lifestyle surveys and computer scams are the most complained about topics. Surveys which are genuine market research are not covered by PECR, but the Market Research Society highlighted in its evidence to the Task Force that surveys are sometimes misleadingly used to obtain information for lead generation. Scams are an area which is outside the remit of the Task Force.

The most notable trend for automated calls is the sudden rise in messages related to the Green Deal. Boilers, solar panels and insulation are the most complained about topics of automated calls. The ICO reports that there were 9,000 complaints related to unwanted automated sales calls about boilers between April 2014 and June 2014. Before 2014 these sectors caused a relatively low number of complaints.

Types of business to be addressed by Task Force recommendations address

The previous issues paper proposed a typology of business behaviour:

- Best practice – companies that are exemplary in the way in which they seek consent for direct marketing or use lead generation, going above and beyond minimum legal requirements.
- Compliance – companies that are complying with the spirit and letter of the law and guidance.
- Unintended non-compliance – companies that are unaware they are not complying with the law and guidance, for example because they are unsure of how to comply or because they have misunderstood the spirit or intended application of the law and guidance.
- Deliberate breaking of the law – companies that are not following the existing law on direct marketing.

The existing evidence does not indicate the spread of businesses across these categories or directly show which are causing complaints. However, it is possible to suggest how different types of behaviour from various organisations have led to large numbers of complaints.

Organisations that fall into the best practice or compliance categories are unlikely to generate many complaints about their marketing activities. Their approaches to compliance would be useful to use as case studies to demonstrate good practice to other businesses.

The Task Force can also take these types of organisation into account when considering the impact of any recommendations on businesses making use of legitimate direct marketing.

Unintended compliance and deliberate compliance groups are responsible for the majority of complaints about nuisance calls and texts. Deliberate non-compliance is likely to be the main driver. This can be shown through the high proportion of complaints which are about automated calls – this type of call is generally always going to be an intentional breach because it requires specific consent. Nuisance texts are also likely to be deliberate breaches, and the ICO's monetary penalty notices indicate large scale deliberate sending of unlawful texts.

A challenge for the Task Force is that companies deliberately breaching the law are unlikely to respond to voluntary good practice schemes. These companies should be subject to enforcement action under existing provisions. Although it might be difficult to change the behaviour of these companies, the Task Force could identify ways to assist regulators in taking action against businesses in this category.

17. http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/tps/tps-effectiveness.pdf
18. http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/first-financial- monetary-penalty-notice.pdf and http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/reactiv-media-monetar-penalty-notice.pdf
19. http://ico.org.uk/enforcement/action/texts

The 'unintended non-compliance' group are the companies where the Task Force could have the most positive impact. The existing evidence does not easily identify these companies but it might be possible to identify types of behaviour associated with this category. Companies calling numbers on the TPS might be following bad practice without deliberately seeking to breach PECR. Companies who buy leads which were improperly obtained might not do so knowingly. These organisations would be more receptive to advice on good practice and other voluntary measures, especially if they can see compliance as a positive business practice.

Lead generators and their clients

There is a distinction between marketing messages sent by a company directly to a customer (or prospective customer) and a message sent by a lead generator with the aim of passing on the consumer contact to a client. The DMA stated in its response to the call for evidence that businesses who have an ongoing relationship with a customer will not want to damage that relationship by making nuisance calls. This behavioural restriction does not apply to lead generators whose main aim is to obtain as many leads as possible.

It seems likely that the majority of complaints about nuisance marketing relate to lead generation companies. This is not directly evident from published statistics but those companies are more likely to use methods such as automated calls, and have a strong presence in the sectors which cause most complaints.

The ICO has highlighted that 'big name' companies are also responsible for generating a significant number of complaints. [20] The cause of complaints about these companies was reported as being poor practice in using sales lists, or from confusing privacy statements leading to unexpected calls. High profile companies seem to have been receptive to less formal enforcement action, and changed their behaviour after being contacted by the ICO. This suggests that different regulatory approaches are needed depending on the nature of the business.

Privacy solutions for companies

Rules on marketing apply equally to all organisations, but smaller businesses may lack the resources to implement best practice measures. Regulators can help by producing guidance aimed at SMEs, such as the checklist produced by the ICO for marketing guidance.[21] SMEs could benefit from more products designed to help them achieve best practice, for example in their privacy notices or customer contact systems. There does not appear to be significant evidence of these products existing, but this might be an area for the Task Force to recommend further work.

Conclusions

Although there is an increasing amount of complaints data available, this only presents one aspect of the nuisance marketing problem. The evidence does seem to indicate that the calls which cause most irritation to consumers are from rogue lead generators working in a small number of sectors. These businesses are the subject of enforcement action from the ICO but are unlikely to engage with voluntary measures. But there is also a market for legitimate lead generation, and the Task Force could encourage businesses to ensure they engage with the compliant end of the market.

Sectoral regulators have a significant role to play by overseeing the companies who purchase leads. There is some variation in how regulators are approaching the problem of nuisance calls. The Task Force should be able to identify the features of effective regulation and make recommendations for these to become the standard across all sectors.

20. https://iconewsblog.wordpress.com/2014/05/19/nuisance-calls-and-texts-big-name-brands-can-be-to- blame/
21. http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-checklist.pdf

Appendix 5: Nuisance Calls and Texts Task Force background paper

How do consumers make decisions about privacy?

Prepared by the Behavioural Insights Team, Which?

Introduction

The literature on information privacy is both extensive and disparate. It has grown enormously in the last thirty years – as has the importance of privacy to consumers and policy-makers due to the growth of the internet and the increasingly connected nature of society – and is spread across many academic fields including law, economics, psychology, management, marketing and information systems.[22] As a result, the literature reveals a number of insights about consumer attitudes and behaviour.

The nature of the studies means that very few address the issue of nuisance calls or texts directly. Nevertheless, the findings of this body of research can provide some useful insights for the Task Force, particularly in terms of how consumers view privacy as a concept and in the fact that attitudes and behaviours often do not correlate. This finding – the existence of a 'privacy paradox' – reflects much of the specific research into nuisance calls which shows a gap between consumer attitudes and behaviours and could go some way to explaining the different understanding of consumers and marketers regarding granting of consent.

This review, carried out by the Which? Consumer Insight Team at the request of the Task Force, begins with an examination of consumer attitudes to privacy and the concept of the privacy calculus – a cost/benefit analysis that many researchers have claimed that consumers undertake in order to make decisions regarding their personal information.

The review goes onto examine challenges to this interpretation, which arose from the gap between what consumers say they feel about privacy and the way they act in reality. In particular the review looks at what behavioural research has to say about the way consumers make decisions about privacy issues.
The key questions that the review looks at are therefore as follows:

- How do consumers make decisions about privacy?
- What insights can behavioural research add to our understanding of consumer decision-making about privacy?

How do consumers make decisions about privacy?

Many researchers have investigated consumer attitudes to privacy and their willingness to disclose personal information based on the view of privacy as a commodity to do with individual decisions about control. For over twenty-five years (late 1970s–2004) the Westin-Harris privacy indexes measured the privacy concerns of thousands of US consumers. This type of research continues to be widespread, for example, the Direct Marketing Association regularly poll consumers on their attitudes and expectations around providing personal details to companies.

The studies looking at drivers of privacy concern are disparate. Brought together, they paint a picture of privacy concern as a complex concept that has a number of drivers. For example some have found previous negative experiences of privacy abuses as a key driver of concern for privacy in the future.[23] Similarly, trust in a company leads to lower levels of concern about privacy. This is an important finding and is confirmed by a number of studies,[24] one of which finds that businesses may find it easier to build trust around the way they use data, rather than reduce consumer concern.[25]

Demographic differences have also been found to make a difference to people's attitude to privacy, with women,[26] young people, less educated and less wealthy people likely to me more concerned about privacy.[27] Personality differences have also been found to be important: introverts are more likely to be concerned than extroverts,[28] as are those with higher social awareness.[29] Each of these conclusions should be taken with a pinch of salt as they are often US studies conducted on small sample sizes.[30] It is questionable how universally the findings can be applied.

22. P Pavlou (2011) 'State of the Information Privacy Literature: Where are we now and where should we go?' MIS Quarterly, 35(4): 977-988
23. H Smith, J Milberg & J Burke (1996) 'Information Privacy: Measuring Individuals' Concerns about Organizational Practices' MIS Quarterly, 20(2): 167-196
24. See H Smith, T Dinev & H Xu (2011) 'Information Privacy Research: An Interdisciplinary Review' MIS Quarterly, 35(4): 989-1015
25. G Milne & M Boza (1999) 'Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices' Journal of Interactive Marketing, 13(1): 5-24
26. K Sheehan (1999) 'An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors' Journal of Interactive Marketing, 13(4): 24-38
27. M Culnan (1995) 'Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing' Journal of Interactive Marketing, 9:10-19
28. Y Lu, B Tan & K Hui (2004) 'Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits', in R Agarwal, L Kirsch, and J DeGross (eds.), Proceedings of 25th International Conference on Information Systems, Washington, DC, December 9-12, pp.272-281
29. T Dinev & P Hart (2006) 'An Extended Privacy Calculus Model for E-Commerce Transactions' Information Systems Research 17(1): 61-80
30. P Pavlou (2011) 'State of the Information Privacy Literature: Where are we now and where should we go?' MIS Quarterly, 35(4): 977-988

Indeed, some studies have shown that in Italy, for example, consumers have a very different conception of privacy which leads to different types of concerns about information disclosure. [31]

Another key problem with this body of research is that attitudinal data does not look at how privacy concerns relate to decision-making about information disclosure (i.e. what people actually do). Research conducted in the 1990s and early 2000s looked at consumer decisions about disclosure. With the advent of the internet this research stresses that such decisions are made in situations of uncertain risk and are increasingly complex and frequent. This led to the conception of a 'privacy calculus.'

The privacy calculus simply states that generally, consumers undertake a cost (risk)-benefit analysis before making decisions about data disclosure. They analyse the risks of disclosing their data and compare this to the benefits achieved from the disclosure. Research in the last decade based on the privacy calculus has identified the following costs and benefits associated with such decision-making: [32]

Costs/risks	Benefits
Perception of the firm's data collection policies	Personalisation
Perception of the firm's data protection and storage policies	Loyalty rewards (including convenience)
Perception of accuracy of the firm's data policies	Financial rewards

The privacy paradox

However, numerous studies have found inconsistencies in consumers' approach to privacy decisions. The main inconsistency relates to the fact that despite high levels of concern about privacy risks, consumers often give up their privacy (both in experimental and actual situations) for relatively low-level rewards. In other words, the consumer calculus is biased towards low benefits instead of high risks. [33] This gap between consumer attitudes and consumer behaviour is known as the 'privacy paradox.' In terms of nuisance calls and texts, this paradox is reflected in the fact that consumers and businesses have been found to have different interpretations and understandings of the consent process. This is not to say that consumers are making incorrect decisions, but reflects the fact that consumer decisions are inconsistent and therefore difficult to predict.

Some researchers have argued that the paradox can be at least partly explained by the fact that individuals' stated disclosure intentions do not reflect their actual disclosure behaviours.[34] Yet there is consensus in much of the literature that the privacy paradox reflects more fundamental findings about the decisions involved in such situations. In particular there are two key points:

- The factors involved in privacy decisions are extremely complex and specific to each individual.
- Individual decision making is subject to conditions of bounded rationality and a number of behavioural biases.

The privacy calculus itself is based on the rational choice model of consumer behaviour in which consumers have stable preferences and are able to find (and comprehend) all the necessary information needed to make informed decisions. Behavioural economics has challenged these assumptions and has implications for the privacy paradox, in particular in terms of the systematic 'biases' that affect consumer decision-making and the heuristics (rules of thumb) that consumers use to simplify complex decisions. However, before looking at these, it is important to look at how information asymmetries cause extra complexity for consumers when making decisions over information disclosure:

Individual decisions about information disclosure are complex because many subjective perceptions and preferences influence our decisions to protect or share personal information. Perceptions of risks and potential damages, psychological needs, and actual personal economic returns all play a role in the privacy calculus. [35]

31. T Dinev, M Bellotto, P Hart, V Russo, I Serra & C Colautti (2006a) 'Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences between Italy and the United States' Journal of Global Information Management,14(4): 57-93; T Dinev, M Bellotto, P Hart, V Russo, I Serra & C Colautti (2006b) 'Privacy Calculus Model in E-Commerce – A Study of Italy and the United States' European Journal of Information Systems, 15(4): 389-402
32. see H Smith, T Dinev & H Xu (2011) 'Information Privacy Research: An Interdisciplinary Review' MIS Quarterly, 35(4): 989-1015
33. L Montiwalla, X Li & X Liu (2014) 'Privacy Paradox: Does stated privacy concerns translate into the valuation of personal information' Pacific Asia Conference on Information Systems, Paper 281
34. M Keith, S Thompson, J Hale, P Lowry & C Greer (2013) 'Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior' International Journal of Human-Computer Studies, 71(12): 1163-1173.
35. A Acquisti & J Grossklags (2008) 'What Can Behavioural Economics Teach Us about Privacy?', in A Acquisti, S Gritzalis, C Lambrinoudakis and S De Capitani di Vimercati (eds.), Digital Privacy: Theory Technologies and Practices, Boca Raton, Florida: Auerbach Publications

Privacy choices are made much more complex as they are affected by incomplete and asymmetric information

Compared to the companies that they interact with, consumers have very little information about the way that their data will be used and it is not often clear to the consumer how much control they can exercise over their own data. Information asymmetries, for example, can prevent consumers from knowing when a firm has purchased their data from another. They may also be unaware of the consequences of this second firm gaining access to their data. The difficulties this presents for consumers trying to accurately judge the risks of information disclosure are far reaching and have been amplified by the "highly networked, digitized, and interconnected information societies" we now live in.[36]

For example, when evaluating the risks of disclosure, consumers have to consider multiple layers of outcomes and possibilities. This "complexity of the privacy decision environment leads individuals to arrive at highly imprecise estimates of the likelihood and consequences of adverse events, and altogether ignore privacy threats and modes of protection."[37]

Due to this lack of information, consumers face numerous 'layers of uncertainty'

The complex 'life cycle' of data results in a set of consequences that consumers need to take into account in order to make an accurate decision about risks/benefits. However, due to incomplete information available to consumers, these consequences cannot be viewed as risks because they cannot be ascribed probabilities. As far as consumers are concerned, these outcomes are uncertain and unpredictable. The complexity of the context within which consumers make decisions mean that these uncertainties are layered, making consistent and accurate decision-making ever more difficult for consumers:[38]

This means that:

- Consumers are only vaguely or limitedly aware of the possible actions they can take to protect themselves.
- Consumers are only vaguely or limitedly aware of the possible/actual actions of marketers.
- Consumers have little or no idea how data will be used, or what certain actions will result in (eg. registering your number on TPS).
- Technological change is shifting the boundaries all the time (eg. technology may soon allow private data retrieval).
- Certain 'common sense' actions may not be available/possible (eg. informing all companies holding your data that you don't want to be contacted by them).
- The more a consumer attempts to understand the issues, the more uncertainty they are exposed to and the greater likelihood that some action will be miscalculated.
- Privacy issues are often 'bundled' with products and therefore any action involves weighing up a trade-off between some 'good' (eg. the convenience of buying online, or access to discounts (eg. ClubCard) and a bundled giving up of certain privacy.

Consumers will often be overwhelmed by these layers of uncertainty and the information asymmetries related to privacy threats and information disclosure. Yet even if consumers had access to complete information, the sheer scale of the interconnected issues and consequences involved means that consumers would still find it difficult to process them and act optimally on the large amounts of data. Behavioural economists have introduced the idea of bounded rationality to explain this: that people often use simplified shortcuts to make decisions about privacy risks.[39]

While this may lead policy-makers to conclude that simplified and clearly-worded messages are effective ways to help consumers make more consistent privacy decisions, recent evidence has shown that consumers will still act unpredictably.[40] Research from psychology into the way that people process information has shown that this is because people do not consciously decide what information to pay attention to: "certain items capture attention while others disappear into the background, even if they are exceedingly important, and even if it would be rational to focus on them."[41]

36. A Acquisti & J Grossklags (2008) 'What Can Behavioural Economics Teach Us about Privacy?', in A Acquisti, S Gritzalis, C Lambrinoudakis and S De Capitani di Vimercati (eds.), Digital Privacy: Theory Technologies and Practices, Boca Raton, Florida: Auerbach Publications
37. A Acquisti & J Grossklags (2008) 'What Can Behavioural Economics Teach Us about Privacy?', in A Acquisti, S Gritzalis, C Lambrinoudakis and S De Capitani di Vimercati (eds.), Digital Privacy: Theory Technologies and Practices, Boca Raton, Florida: Auerbach Publications
38. See A Acquisti & J Grossklags (2008) 'What Can Behavioural Economics Teach Us about Privacy?', in A Acquisti, S Gritzalis, C Lambrinoudakis and S De Capitani di Vimercati (eds) Digital Privacy: Theory Technologies and Practices, Boca Raton, Florida: Auerbach Publications
39. See A Acquisti & J Grossklags (2005) 'Privacy and rationality in decision making' IEEE Security & Privacy, 24-30
40. See S Spiekermann, J Grossklags & B Berendt (2001) 'E-Privacy in 2nd Generation E-Commerce: Privacy preferences versus actual behaviour' EC'01, October 14-17, Tampa, Florida, USA
41. See G Loewenstein, C Sunstein, and R Golman (2013) 'Disclosure: Psychology Changes Everything' Regulatory Policy Program Working Paper RPP-2013-20, Cambridge, MA: Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, Harvard University

Findings from behavioural economists and psychologists have a great deal to say about the way that consumers make decisions:

Consumers use heuristics to make complex decisions

Operating under bounded rationality, due to limited attention, people use heuristics (or, rules of thumb) to help simplify complex decisions:[42] These include:

- Simulation heuristic – Events that are difficult to imagine are discounted as improbable. This may have an influence on how consumers conceptions of the risks of identity theft, for example.[43]
- Representative heuristic – This is where we use shortcuts to see certain things as representative of other, not necessarily clearly associated things. For example, a privacy policy that has a clean or neat design may be associated with trustworthiness, regardless of its actual content.[44]
- Affect heuristic – This effectively means that the mood that the decision-maker is in can have an impact on how consumers process information.[45] This is known to particularly be the case for issues surrounding judgement of risks.[46]
- Bounded attention – This is where consumers ignore certain pieces of information. This is particularly true for ubiquitous pieces of information such as privacy disclosure policies. Indeed, research suggests that very few people read privacy policies when asked to disclose information and consumers think that the mere presence of a privacy policy implies protection.[47]

Consumer decision-making is subject to systematic biases

Decision-making is also influenced by a number of systematic 'biases' which lead people to behave in different ways to those predicted by simple cost-benefit analyses:

- Hyperbolic discounting – This is the tendency to value the present higher than the future and is a key feature of consumer decision making in the privacy field. It has been cited as one of the key explanations for the privacy paradox in that consumers discount large long-term risks for smaller short-term gains.[48]
- Endowment effect – This is the tendency for people to value something they already own more than they would if they did not own it. Empirical research suggests that this is the case in terms of privacy research: people offered money to give up details (i.e. something they already had) valued their privacy greater than those who were offered the chance to purchase more privacy (i.e. something they did not yet have).[49] This indicates that the way that privacy is presented can have an impact on how seriously consumers view threats to it.
- Overconfidence – There is a general trend in decision-making for people to be overconfident in their own ability/ knowledge in the particular area. This can be seen in privacy through an experiment which found that past disclosure behaviour is a better guide to future behaviour than stated intentions.[50] Other research on social media sites has found that consumers tend to be more willing to disclose information if they feel in control of it.[51]
- Probability judgements – Behavioural research in a number of areas has shown that consumers do not calculate probabilities (especially small probabilities) accurately.[52] Research has also shown that people do not only make random errors, but are subject to systematic biases in the way that they process probabilities. It is likely that consumers therefore do not calculate the risks of information disclosure in a way that economists would predict. This has implications for the design of privacy policies. An accurate presentation of the risks could therefore – provided consumers do pay attention to it – either scare consumers, or perhaps reassure them more than it should.[53]

42. See R Thaler & C Sunstein (2008) Nudge: Improving Decisions about Health, Wealth, and Happiness, London: Yale University Press
43. D Kahneman & A Tversky (1982) 'The simulation heuristic', in D Kahneman, P Slovic, & A Tversky (eds.), Judgment under uncertainty: Heuristics and biases, Cambridge: Cambridge University Press, 201–210
44. A Acquisti & J Grossklags (2008) 'What Can Behavioural Economics Teach Us about Privacy?', in A Acquisti, S Gritzalis, C Lambrinoudakis and S De Capitani di Vimercati (eds) Digital Privacy: Theory Technologies and Practices, Boca Raton, Florida: Auerbach Publications
45. See F Kehr, P Mayer & D Wentzel (2013) 'Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect – research in progress' Thirty Fourth International Conference on Information Systems, Milan
46. See E Nyshadham & G van Loon (2014) 'An Affect Primary Framework for Privacy Decision Making' SAIS 2014 Proceedings, Paper 27
47. G Loewenstein, C Sunstein & R Golman (2013) 'Disclosure: Psychology Changes Everything' Regulatory Policy Program Working Paper, RPP-2013-20. Cambridge, MA: Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, Harvard University
48. A Acquisti (2004) 'Privacy in electronic commerce and the economics of immediate gratification', Proceedings of the ACM Conference on Electronic Commerce (EC '04), 21–29
49. A Acquisti, L K John & G Loewenstein (2013) 'What is Privacy Worth?' The Journal of Legal Studies, 42(2): 249-274 50. D Wilson & J Valacich (2012). Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus International Conference on Information Systems.
51. A Acquisti & R Gross (2006) Imagined Communities: Awareness, information sharing, and privacy on the facebook, Carnegie Mellon University.
52. See R Thaler & C Sunstein (2008) Nudge, London: Yale University Press
53. See G Loewenstein, C Sunstein & R Golman (2013) 'Disclosure: Psychology Changes Everything' Regulatory Policy Program Working Paper, RPP-2013-20. Cambridge, MA: Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, Harvard University

- Status quo bias – It is a well-known finding from behavioural science that people tend to be more comfortable not making a decision when there are elements of complexity involved; hence the popularity of defaults as policy solutions.[54] In terms of privacy, research has found that on social networks users rarely change the default privacy settings.[55]
- Framing – It is a well-established in behavioural economics that people's decisions are influenced by the way that their choices are framed. This is no less the case in privacy decisions than elsewhere. Experimental evidence confirms this by finding that when privacy choices are framed with ambiguous outcomes, people tend to be more willing to accept giving away their data.[56]
- Reciprocity and fairness – the behavioural evidence shows that people often have an innate desire to act fairly in transactions, but also to retaliate or reward others behaviour when appropriate.[57]

This could have implications for how marketers request and use consumer data.

Conclusions

A review of the literature has found that while much research has been done on explaining and predicting consumer behaviour, there are gaps in terms of a focus on design of implementable tools to help consumers effectively make informed choices about information.[58] Consumer behaviour is very complex and, as this review has shown, can often vary dramatically from what one would expect. Solutions to the problems identified by the Task Force must take care to keep the real consumer in mind, rather than the hyper-rational consumer of economic textbooks.

Therefore potential remedies to the issues of nuisance calls and texts should work with the grain of consumer behaviour, rather than against it. Information should be designed in a careful way that actually helps consumers navigate this complex area while at the same time not bombarding consumers with information that they are likely to ignore or avoid. Consumer-facing recommendations proposed by the Task Force should be properly tested to ensure that they have the desired effect and avoid unexpected results. Behavioural experiments, using randomised controlled trials, in situations as close to reality as possible are the best way to ensure that solutions achieve their desired effect and do not have unintended consequences.

Nevertheless as the review has revealed, there are limits to the results that can be expected from improving the design and clarity of information provided to consumers. This review has shown that decision-making regarding information privacy is a hugely complex area with layers of uncertainty and numerous heuristics and biases at play. Changing consumer behaviour is therefore a significant challenge and even the most well-designed interventions may only have a limited effect. Other solutions, such as ensuring that businesses treat their customers fairly, and do not exploit the biases inherent in consumer decision-making, should also be central to the Task Force's recommendations.[59]

54. See R Thaler & C Sunstein (2008) Nudge: Improving Decisions about Health, Wealth, and Happiness, London: Yale University Press
55. A Acquisti & R Gross (2006) Imagined Communities: Awareness, information sharing, and privacy on the facebook, Carnegie Mellon University.
56. A Acquisti & J Grossklags (2005) 'Uncertainty, Ambiguity and Privacy' Workshop on Economics and Information Society (WEIS '05), Boston, MA
57. A Acquisti & J Grossklags (2008) 'What Can Behavioural Economics Teach Us about Privacy?', in A Acquisti, S Gritzalis, C Lambrinoudakis and S De Capitani di Vimercati (eds) Digital Privacy: Theory Technologies and Practices, Boca Raton, Florida: Auerbach Publications
58. P Pavlou (2011) 'State of the Information Privacy Literature: Where are we now and where should we go?' MIS Quarterly, 35(4): 977-988
59. A final point is that there is a key behavioural point that relates to provider rather than consumer behaviour: the spotlight effect. This shows that firms sometimes overrate consumers' attention to information and therefore improve their behaviour without consumer pressure. This means that efforts to promote better behaviour among providers could succeed even without stimulating any change in consumer behaviour. Examples of this the fact that putting 'scores-on-the-door' hygiene ratings of restaurants in Los Angeles inspired improved hygiene without any evidence of consumer pressure. The placing of energy efficiency ratings on appliances in the EU has been seen to have had a similar effect on provider behaviour. see G Loewenstein, C Sunstein & R Golman (2013) 'Disclosure: Psychology Changes Everything' Regulatory Policy Program Working Paper, RPP-2013-20. Cambridge, MA: Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, Harvard University.

December 2014

Which? 2 Marylebone Road, London, NW1 4DF | which.co.uk | 020 7770 7000

Which? is the trading name of Consumers' Association – a registered charity No' 296072