



**Consumer
Focus**
Campaigning for a fair deal

Consumer Focus response to ICO consultation on a Code of Practice for personal information online

March 2009

Contents

Introduction	3
Impact of the code	4
What information does the code apply to?	5
Data protection online	7
Marketing your goods and services online	8
Privacy choices	9
Operating internationally	10
Individuals' rights online	11
General consultation questions	12

About Consumer Focus

Consumer Focus is the statutory consumer champion for England, Wales, Scotland and (for postal consumers) Northern Ireland. We operate across the whole of the economy, persuading businesses, public services and policy makers to put consumers at the heart of what they do.

Consumer Focus tackles the issues that matter to consumers, and aims to give people a stronger voice.

We don't just draw attention to problems – we work with consumers and with a range of organisations to champion creative solutions that make a difference to consumers' lives.

Introduction

The area of personal information online is dense and confusing. Technological development now means our lives, choices and habits are conducted in a very public space. Given the pace of change it is necessary to constantly review whether the consumer protection framework is fit for purpose. We therefore welcome this Information Commissioner's Office (ICO) consultation on a code of practice for personal information online.

The value of the underlying right to privacy in relation to personal information online should not be underestimated¹, but people often find it hard to articulate the harm if it is taken away. However it is clear there is no consent to waiving our right to privacy when we do not have control over our privacy, when usage of personal information is not transparent, or when it is used to build a picture which then stereotypes or discriminates.

On the other hand there is real value in our personal information, from public interest benefits to do with medical research and where to build new schools and hospitals, to the 'black gold' of the online marketers who sell our information, to the hackers and fraudsters who can use it for illegal gain.

Consumers want to be asked, not just have things done to them. They expect fairness in dealings. They want to consent and control but they expect protection as well because they do not have the time or expertise to protect themselves². A code under s.51 has the potential to outline guidance to provide this protection and to be flexible enough to be reviewed on a regular basis to keep up with developments.

Our recommendations for fulfilling the principles under the Act, and therefore the guidance that is issued pursuant to the Act would include the following:

- Compulsory Privacy Impact Assessments
- Privacy by default and (real, active) informed consent
- Privacy by design and minimum storage and processing security standards
- Compulsory notification for all breaches
- Clear liability of data controllers for further processing and use
- Easy access to information records and ability to correct and remove
- Stricter control of 3rd party transactions
- Regular reviews of the code

¹ ICO, *The Privacy Dividend, the business case for investing in proactive privacy protection*, March 2010.

² *Americans Reject Tailored Advertising*, Turrow et al, September 2009 and also *FYI: A people's inquiry into personal information*, DEMOS, upcoming March 2010.

Impact of the code

The process of developing the code was deemed necessary because of public concern about online privacy issues. In particular this means technological developments such as targeted advertising, which use personal information as currency often without the knowledge of the person to whom it relates. The current legal framework does not meet these challenges. The Digital Britain Report acknowledged that our frameworks for online protection have not kept pace with 200 years' development of consumer protection law and enforcement in the offline world³.

There has also been significant criticism of the poor implementation of the Data Protection Directive in the Data Protection Act 1998 ('the DPA'). The Information Commissioner's Office is under-resourced both in powers and resources to enforce the Act and appears to have fewer abilities to investigate and enforce the law than their counterparts in other EU countries⁴.

In the absence of adequate legislation a code provides an opportunity and the necessary flexibility to provide guidance that both sets best practice, is future proof and ensures compliance with the highest standards internationally. It is disappointing therefore that the proposed code goes no further than a statement of some very general common sense principles that are neither challenging nor future proof.

The code should be emphasising the important messages and concerns that the public have about personal information online. Trust needs to be built in this area⁵. It is a significant issue in our day to day dealings with an online world as a record of our online activity will not only reveal our most personal interests but it can expose us to ID fraud or unwanted approaches, can stigmatise and discriminate. Lack of trust can confound commercial and Government business models alike.

People want their dealings with an online world to be within their control and choice. The issues of consent and transparency are very much part of the current debate but hardly mentioned in this document. These must be the guiding principles for any Code of Practice in the area and the standards by which fairness must be judged.

We hope that a more reasonable balancing of interests can be achieved post-consultation. The code should set best practice and meet minimum standard criteria such as those developed by the OFT for their approved codes⁶. The code needs to be regularly monitored and reviewed and recommendations for legislative amendments considered in light of compliance with the code, developments in law and practice in other jurisdictions and technological developments.

³ As above, p 189

⁴ *Data Sharing and data protection* – National Consumer Council's response to the Data Sharing Review, February 2008.

⁵ A European Commission study of over 5000 young people (aged 15 – 25) showed that most young people are sceptical of the internet as an environment for the exchange of personal data and have major doubts about personal data protection. They perceived high levels of risk in giving personal data and called for 'hands-on' regulation. *Young People and Emerging Digital Services, An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks*, JRC European Commission, EUR 23765 EN - 2009

⁶ OFT Consumer Codes Approval Scheme, Core Criteria and Guidance, March 2008

What information does the code apply to?

There is a need to expand the definition of what is personal data and the ways an individual may be identified online in order to keep pace with technological development. There is an increasing recognition about how little information is needed to identify individuals through information exchanges online and how much access sites and services have to a range of data that can be used to identify individuals. This code does not appear to have taken account of developments that show that so called anonymised data can be used to identify individuals.⁷ The US Federal Trade Commission (FTC) has acknowledged that restricting protection to personally identifiable information does not recognise developments in profiling technology. The FTC state that both Personally Identifiable Information (PII) and non-PII raise privacy issues and so the distinction is no longer meaningful⁸.

There is a reference to 'practical difficulties in complying with all aspects of the DPA in respect of non-obvious personal identifiers' which seems to be condoning a lack of compliance with the law. If business models are not compliant then they should not be used.

The code needs to clarify that the onus needs to be on those collecting and using data to determine if there is any possibility that an individual may be identified through the use of data. This would include the transfer of a piece of information to another party which on its own may not be used to identify an individual but could do so when combined with the information held by the other party. It would also include the need to take adequate security measures to ensure that anonymised information was secure and not liable to hacking.

It would be preferable to err on the side of caution when giving advice about compliance and assume that, where there is doubt, that personal information is involved, rather than seeking expert legal advice which is costly and not definitive.

Question 1: Does this section explain clearly what information this code applies to?

It is correct to say that there is real confusion about who the data controller is and therefore who has responsibility for data protection. The law is as it is and the data controllers themselves must exercise responsibility and control over any information transferred to or accessed by others, whether contractually or by limiting access and use. The code provides an opportunity to urge responsibility be taken by data processors as well as data controllers. A narrow definition of responsibility does not serve the principles of data protection.

The section proposes a very narrow and limited application of the code which may even belie current interpretations of the EU Directive and subsequent interpretations of the DPA. We suggest that a public liability/risk mitigation stance is far more appropriate because it is not always clear that someone will be impacted, but there should be an obligation to mitigate risk.

⁷ Arvind Narayanan and Dr Vitaly Shmatikov *De-anonymizing Social Networks*, March 2009.

⁸ FTC staff report: *Self-Regulatory Principles For Online Behavioral Advertising*, February 2009.

Question 2: Have we properly understood the technical issues of collecting personal data online?

The code seems to downplay technical capabilities and focus on cookies as a means of collecting information. However there are numerous information collection techniques that circumvent browser settings which delete cookies, such as email address, eg Local Shared Objects (LSO), flash, or Microsoft Silverlight cookies, web bugs, re-spawning practice, web beacons. Cloud computing and mobile applications are further areas where the control or contractual nexus may be broken and personal information is collected and stored without consent or tools to prevent the collection.

Data protection online

Question 3: Are there any other specific issues relating to online security that you think it would be helpful for us to cover in the code?

The ICO has developed some useful guidance on privacy impact assessments and yet they are not mentioned here as an appropriate measure for organisations to take prior to undertaking any information collection activity. The ICO has also done work on privacy by design and explanation of the measures available, and a strong recommendation to adopt privacy by design should be included.

The staff of data controllers and processors should be trained in data protection and privacy regulation and principles as well as security procedures so that they understand why the security procedures are so important.

Question 4: Do you think the section on vulnerable people is comprehensive enough? Are there any specific issues that you think we should include?

A public liability approach (that is eliminating all foreseeable risks) to protection of privacy and personal information under the Act is the only practical way to ensure that the data collection is not misleading or exploitative and the duties of fairness under the Act are fulfilled. Unless there is a relationship with the user it will be difficult to ascertain vulnerability and capacity, and even where there is a relationship (membership, SNSs, etc) it will often still be hard to verify understanding.

We support the definition contained in this guidance that 'vulnerable people' means individuals who for whatever reason may find it difficult to understand how their information is used. The definition of who is a vulnerable user is not currently consistently applied under the legislation or in the various codes and guidance that apply to online information collection (and this is especially so in relation to children) and so this definition is welcomed and puts the onus back on the controllers and processors.

Informed consent will be required under the amended e-privacy directive, as storing or gaining access to information will only be allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information about the purposes of the processing, and is offered the right to refuse such processing by the data controller⁹. Where there are potential risks if there are no legally compliant verification procedures then data should not be collected at all. The human right to privacy requires consent and there is no consent where there is no capacity.

⁹ Directive 2002/58/EC, Article 5(1)

Marketing your goods and services online

Where a group of organisations work together to deliver content through a single portal and there is doubt about the responsibilities of the organisations, the safe option is to adopt joint and several responsibility, ensure the highest standards and ensure others do too.

Question 5: Have we properly reflected the issues relation to the marketing of goods and services online?

There is a lack of awareness as to how online personal information can be used and abused. It is not a matter of attributing fears to a misunderstanding of technology. Indeed the more people find out about technology and technological capabilities, the more they tend to be concerned about privacy. Our most technological savvy users have the same fears¹⁰.

There should be an emphasis on the underlying right to privacy and the need to ensure business models don't contravene this. The Phorm example shows that when a company crosses the line, even when the law fails to intervene, market forces may be mobilised with a devastating effect on that company's business. Trust needs to be developed in order to develop a business and a brand. Treating people fairly and in accordance with their expectations goes towards building trust and can distinguish the good from the bad. High standards in a code can distinguish those willing to comply and drive choice by a consumer, thus having the effect of dealing with those who don't comply.

Consumer's value their privacy and want to have control over how their personal information is used. Research undertaken by the Information Commissioner's Office indicates that 94 per cent of the population thought that 'protecting people's personal information was a major concern, ranking as the most important social concern along with preventing crime¹¹'. The default setting, the turn off or opt out model, should not be one that undermines an established right and relies on people to take positive steps to make the right meaningful. Real consent is required and users need to be empowered to give that consent through an appropriate understanding of what their information is being used for and why.

The All Party Parliamentary Communications Group recommend that 'the Government review the existing legislation applying to behavioural advertising, and bring forward the new rules as needed, to ensure that these systems are only operated on an explicit, informed, opt-in basis.' They further recommend that 'the UK Council for Child Internet Safety (UKCCIS) consider how behavioural advertising that is aimed at children and young people should be regulated¹².' This code needs to go further in outlining the fundamentals of consent.

¹⁰ See *Americans Reject Tailored Advertising*, Tarrow et al, September 2009 and *Young People and Emerging Digital Services, An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks*, JRC European Commission, EUR 23765 EN – 2009.

¹¹ Report on the Finding of the Information Commissioner's office, *Annual Track 2008*, 4.1.

¹² *Can we keep our hands off the net?* Report of an Inquiry by the All Party Parliamentary Communications Group, October 2009, p21.

Privacy choices

This section is rather misleading in that it implies that a user currently has and exercises choices to enable options to protect privacy and make better use of the internet. In fact not many browsers or sites provide you with this degree of control. The reality usually involves deleting all cookies, whether functionally useful or intrusive. The lack of control over functionality may be a deterrent to using privacy settings, where users know about them. Our recent research on cookies indicates that almost half the people surveyed did not know what cookies were and that these numbers increased among older people and lower socio-economic classes. Of those who are aware of cookies only just over half of these deleted them regularly¹³.

Question 6: Should we try to develop specific recommendations relating to default settings? If so, do you have any suggestions on how these defaults could be set? What areas of activity do you think we should cover?

Consumers will generally accept the default setting and so it can not be said that any choice or consent is being exercised in the current environment. This is not due to a laziness on the part of the consumer but due to time constraints, lack of expertise and the complexity of the information and the system being presented. Underlying the Data Protection Act are principles of control, security and privacy, principles that should drive the default position. The default position should be no data collection.

Any data collection should require positive, active consent. The e-privacy Directive proposes a formulation which requires consent after being provided with clear and comprehensive information¹⁴. This position should not pose any problems for trusted brands with good business models but will pose problems for those brands big and small that don't put their customers first.

We agree with the proposal that it is good practice to reflect the likely wishes and expectations of the individuals you deal with and that the evidence from numerous studies show that individuals want their privacy protected. Privacy should be the default. At the very least there should be no default third party data collection as this is collection by stealth and fundamentally impacts the user experience.

¹³ Consumer Focus, upcoming research report.

¹⁴ Directive 2002/58/EC, Article 5(1).

Operating internationally

While we agree that the data protection principles should be the foundation for compliance, the interpretation and application of these seems to have fallen behind other jurisdictions. We would expect this section to advocate principles based on the highest common denominator to ensure companies that complied had some confidence that their compliance had universal application.

Contractual arrangements about processing of data should require compliance with the data protection principles and ensure joint liability, breach notification and adequate remedies where there are problems. Contracts should specify minimum security and privacy protection and storage requirements. We support the recommendation to encrypt data prior to it being transferred to an online services company.

Question 7: Are there any other international issues you would like to see covered?

There is increasing focus on data protection and personal information online internationally, with some strong statements being made by the law makers in Europe and America that trading of personal information without consent can not continue and that they are ready to intervene¹⁵. Better implementation of Directives (and the DPA has been widely criticised for poor implementation of the European Directive) and relevant legislation might also help achieve greater consistency in compliance and less burdens for businesses in dealing with the differences.

¹⁵<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/63&format=HTML&aged=0&language=EN&guiLanguage=en>, <http://www.ftc.gov/speeches/09speech.shtm>

Individuals' rights online

This is a rather deceptive heading as it seems to limit the discussion of rights to subject access. We would like to see a full discussion of the right to privacy here and how this translates online and guides decision making.

Question 8: Does this chapter clearly explain how individuals' rights apply in an online context?

No. It is limited to a right to subject access and even then needs to better explain individual entitlements to have records corrected or removed and to recommend how this could be facilitated.

It does not mention consent or the additional rights individuals have through consumer protection law such as in relation to misleading statements, unfair contracts, impact of privacy notices, the right to be informed of data breaches, and rights of action and liability (particularly where third parties are involved). Nor does it mention the fundamental right to privacy and what this means and its precedence or otherwise in relation to data protection principles.

General Consultation Questions

Question 9: Overall, do you think the draft code of practice is useful? If not, what would improve the final code?

The code is not particularly useful because it does not go beyond a rather narrow interpretation of current legislation. We believe such a code should set clear standards for best practice and be future facing and that the current proposal does neither of these things.

Question 11: Do you think the advice given in this code meets the realities of current business practice?

Technology and innovation in business practice have developed way ahead of consumer rights in the area and so a better question would be how it meets the needs of consumers and the public interest.

Question 12: Are there any key areas that we have not covered?

As indicated it is limited and could have been a best practice guide with a rights and fairness approach not a standard practice guide that presents no challenges.

Question 14: We will be providing examples of good and bad practice in the final code. Are there any good or bad practice examples that you would like us to include?

Good examples

- Google Dashboard (although needs to apply beyond email account holders and needs to be opening screen)
- Microsoft Browser choice screen (an example of how you would provide choices on an opt in basis as a front screen), six month limit on retention of data and in private browsing (although this also needs to be opening screen)
- Godzilla and Firefox also have in private browsing options (but need to be opening screen)
- Encryption and PETS in Financial and Health Services

Bad examples

- The Facebook unilateral change to terms and conditions and their control of personal data even when you leave the service
- The Rural Payments Agency data leak and the failure to admit to this and to try and implement damage limitation for six months
- myguide.gov.uk, the Government information site which provides an introduction to the internet for new or non-users, requiring pages of personal information before you register and an acceptance of terms and conditions before you actually get to read them

Question 16: Is there any other relevant guidance that we should refer to? We would welcome suggestions of useful links to other websites that could be included in the code.

- Federal Trade Commission guidance, Rules of the Road, the FTC Staff Report on Self-Regulatory Principles for Online Behavioural Advertising of February 2009, David Vladeck's speech on the Role of FTC in Consumer Privacy Protection, <http://www.ftc.gov>
- Canadian Privacy Commissioner's Web site, http://www.priv.gc.ca/information/guide/index_e.cfm
- Recommendations from the All Party Parliamentary Communications Group 'Can we keep our hands off the net?', October 2009
- Canadian Internet Policy and Public Interest Clinic submission to the Federal Trade Commission, March 2008
www.ftc.gov/os/comments/behavioraladprinciples/080411cippic.pdf
- Article 29 Working Group opinions:
 - 5/2009 on online social networking
 - 1/2008 on data protection issues related to search engine
 - 4/2007 on the concept of personal data
- National Consumer Council, *The Glass Consumer, Life in a Surveillance Society*, 2005
- Scottish Consumer Council, *Protecting Personal Privacy, guidelines for collecting and using people's personal data*, 2001

Question 17: Are there any further comments you wish to make?

There is no mention of data breaches and guidance on what to do (both for individuals and organisations). Given the new obligations being introduced in the e-privacy directive it is important these issues are covered.

The code specifically states that it is a toothless tiger, ie 'the Information Commissioner's Office cannot take action over a failure to adopt good practice or to act on the recommendations set out in this code' and herein lies the problem. As it currently stands it just restates the law and its current interpretation. We are aware that enforcement actions are rare and powers are not sufficient but without an indication that there is a possibility of action for breaches and that the code may be used in mitigation it is hard to see the value of the code in its current form.

The code needs to really stretch the current industry friendly boundaries and to propose best practice and high standards.

Consumer Focus response to ICO consultation on a Code of Practice for personal information online

If you have any questions or would like further information about our response please contact Linda Weatherhead, Principal Policy Advocate, by telephone on 020 7799 7986 or via email: linda.weatherhead@consumerfocus.org.uk

www.consumerfocus.org.uk

Copyright: Consumer Focus

Published: March 2010

If you require this publication in Braille, large print or on audio CD please contact us.

For the deaf, hard of hearing or speech impaired, contact Consumer Focus via Text Relay:

From a textphone, call 18001 020 7799 7900

From a telephone, call 18002 020 7799 7900

Consumer Focus

4th Floor
Artillery House
Artillery Row
London
SW1P 1RT

Tel: 020 7799 7900

Fax: 020 7799 7901

Media Team: 020 7799 8004 / 8005 / 8006