

Personalised Pricing

Increasing Transparency
to Improve Trust



Contents

Summary	2
Why did the OFT launch a call for information?	7
What did we find out about personalised pricing?	9
How can prices be 'personalised'?	12
How technology helps to 'personalise' prices	14
Research on whether cookies are used to influence price	17
Consumers' understanding of how their information is used by retailers	21
Consumers' control of the information they provide	24
Is personalised pricing harmful to consumers?	27
Is personalised pricing illegal?	29
When would the OFT be concerned about online personalised pricing?	34
Annexes	40
References	41

Summary

In November 2012, the Office of Fair Trading (OFT) launched a call for information to improve its understanding of how the use of consumers' information is affecting online markets. We looked at the practice of **personalised pricing**, which **is a form of price discrimination** (when a firm charges a different price to different people for the same good or service, for reasons not associated with costs). Price discrimination is a well established business practice, which consumers generally may find unsurprising. It occurs for example where OAPs or students receive discounts for products, or where people pay different prices for a transport ticket depending on when they book. A fuller description of price discrimination is in [annexe 1](#).

In this report we use the term **personalised pricing** to refer to the practice where businesses may use information that is observed, volunteered, inferred, or collected about individuals' conduct or characteristics, to set different prices to different consumers (whether on an individual or group basis), based on what the business thinks they are willing to pay. If personalised pricing is used, it may result in some consumers receiving discounts, while others pay more than they would if all consumers were offered the same price. It is technologically possible, and consumers are concerned about businesses setting higher prices to individuals based on information which companies collect on them – for example, information about their browsing or purchasing history or the device they use.

However, our evidence indicates that businesses are not using information about individuals to set higher prices to them. Rather, businesses are offering personalised discounts, and increasingly using information collected about consumers in order to refine their pricing strategies. For example a business may use information collected about consumers to identify consumers who have not made a purchase for a number of weeks and offer a discount on future purchases.

Because personalised pricing is possible, appears to be in use to some extent and because it has the potential to benefit both consumers and businesses, we have also set down a number of recommendations to businesses as to how they could act both to avoid legal infringements and also to build consumer trust in this area.

What is going on?

We had limited responses from business but the research we looked at indicates that some businesses are using the information they collect from consumers to give them discounts and other offers based on consumers' conduct or characteristics. However, the businesses we spoke to had no desire to identify individual consumers in order to offer them **higher** prices than they would otherwise have charged them, and were very aware of the potential adverse consumer reaction to actual or perceived invasions of their customers' privacy. We did find some evidence of online search results being determined by consumers' conduct or characteristics. We did not look closely at sectors (such as financial services) where the **product** may be personalised, and the price vary accordingly.

Prices online do vary, going up and down (sometimes rapidly). Consumers don't always understand why and may think this is because they are being offered a price based on information collected about them personally and that they might be paying higher prices.

Prices vary depending on factors such as:

- the time of purchase, as prices vary according to the demand for them and availability
- the location of the consumer, for example, pricing in the EU appears to be based on which country you are in, rather than precise IP location, and the price may be the same for all consumers who are in that state
- the route in to the website, so that consumers who arrived at a website via an associated website are offered a price and this price may differ from that shown to consumers who arrive at the website directly. Again, all consumers who arrive onto the website in this way will be offered this price

We found that pricing decisions are influenced by analysis of aggregated information collected about consumers.

Consumers should not however assume they are being offered the best deal – even when dealing with a company they have engaged with before, and should continue to shop around and compare online and offline prices. Discount schemes may also be available.

Does greater personalisation bring benefits?

Generally the ability to segment consumers into groups to present innovative discounts based on personal information has the potential to benefit consumers, where the process is transparent. Well-informed and confident consumers are essential in driving competition between suppliers offering these services. However, we were disappointed with the level of transparency by businesses about what information businesses were collecting and how it is used. This lack of transparency harms consumers' trust in traders and business practices. We found that businesses could do a lot more to make their practices more transparent about what information they are collecting, how it is being used and **give consumers real choice about this**. This is an area that we want to keep under review.

Online and mobile retailers are in a powerful position, with access to a lot of information, and the ability to use sophisticated technology. We do not want to see businesses exploiting this position unfairly because this would create suspicion and could lead to consumers using online and mobile services less. We think that consumer trust is essential for the digital economy to develop optimally.

If personalised pricing is used, so that some consumers pay more, and others less, this **may** have an overall effect that is positive for consumers (where the benefit to consumers who pay less ('the winners') outweighs the harm to those charged more ('the losers')). However even if this is so, we may still have concerns if consumers reduced their online purchases because of fears (whether genuine or misplaced) about the practice of online personalised pricing, or if those who end up paying more are vulnerable, as described in our [Annual Plan](#). We would also be concerned if in fact the harm to those that are made worse off as a result of price discrimination, outweighed the benefits to those that are made better off.

We may have concerns when:

- consumers cannot easily avoid personalisation if they wish to - for example because the trader requires the consumer to sign in, where personalisation is conducted by a search engine or where personalisation is based on IP address, browser type, or the device used by the consumer)
- consumers do not know it is occurring, or
- consumers cannot easily see prices paid by other customers – such as where prices are dynamic, or most consumers receive some form of discount.

Concerns are particularly likely to arise when these conditions arise in markets in which competition is not effective (for example, where there is a lack of switching leading to companies' prices and services not being effectively disciplined by competition).

Any personalisation should be transparent

Where personalisation takes place, it is less likely to be harmful where consumers know it is happening, understand how it works and can exercise effective choice, for example where consumers receive personalised discounts as a result of membership of a loyalty scheme. We think there is potential for harm if consumers receive a personalised price without knowing this is so.

We would also have particular concerns where consumers are misled, or not given important information. For example:

- where there are misleading statements, for example:
 - stating 'best price', when in fact the consumer is paying more than other consumers
 - 'discount' sites which in fact lead the consumer to pay a higher price than going to a retailer directly
 - Recommended Retail Prices or other reference prices where in fact some form of discount is generally available
- where there are misleading omissions, for example:
 - where information used to personalise a price is requested for other stated reasons, such as in order to process an application or order quickly, and it is not clearly stated that this information will have an impact on the price presented information that is collected covertly, for example by undisclosed cookies
 - where it is not made clear that all prices are personalised
 - if there is a base price, not making clear where the price is personalised, and how consumers can opt out of personalisation.

Next Steps

We have written to businesses to advise them to be more transparent about their practices both to avoid legal infringements and also to build consumer trust in this area. We have advised that **we will consider enforcement action if we find evidence of misleading or unfair practices.**

We will work with the Information Commissioner's Office (ICO) to explore and further understand the consumer protection and data protection issues related to the collection and use of information about consumers, particularly in the context of personalised pricing.

We will continue monitoring the development of pricing practices online, particularly in light of other policy initiatives such as changes at EU level to [data protection legislation](#), consumer empowerment initiatives such as the [Government's midata project](#), industry and self-regulatory initiatives, and [action taken by the Federal Trade Commission in the USA](#) in order to inform the work of the Competition Markets Authority, the new body which will replace the OFT and Competition Commission from April 2014.

Why did the OFT launch a call for information?

The internet is an integral part of daily life and is commonly used to shop for goods, services and digital products. The value of online shopping is increasing every year, and there has been a large growth in the use of mobile devices to connect to the internet. In parallel with these trends, companies trading online are devising increasingly sophisticated systems to collect and use information about visitors to their sites.

Historically, a business's ability to collect all the information necessary to help predict how much a consumer would be willing to pay for a product (a good or a service) has been too costly for businesses to implement. However, the internet has dramatically reduced these costs and businesses have increasingly large amounts of information about their current and potential customers. They can use this information when deciding what prices to offer to segments of consumers or, potentially, individual consumers – bringing the prospect of a business's ability to predict how much the consumer would be willing to pay for a product ever nearer. This raises potential consumer protection, privacy and fairness concerns. It also gives rise to worries on the part of consumers, which may lead them to avoid or reduce the use of online and mobile shopping channels, due to fear or caution about the economic consequences of their conduct.

The collection of consumer information however offers potential benefits to both businesses and consumers:

- retailers that know about their customers can customise offers and encourage loyalty
- consumers may obtain a more personalised, efficient and relevant shopping experience through targeted marketing and discounts for products they use
- information collected about people's behaviour online has economic value, and the trade in this information by retailers can lead to lower prices (or even free offers).

Key facts

- 77 per cent of UK households have internet access, and
- There are 17.6 million mobile phone internet users according to the [Office of National Statistics](#)
- The value of online shopping has increased by 93 per cent between 2007 -2011 from £35bn to £68bn according to [Ofcom research](#)
- The OFT's [Online Targeting of Advertising and Prices Market Study](#) (2010) (OTAP) found that the technology exists to personalise prices.

The market for information has facilitated a further range of businesses that provide services to optimise and trade this information and provide services back to retailers and to other businesses. There is also a lot of scope for further development of the digital economy, based on consumers making more use of data collected about them, and intermediaries being able to add value to this data by analysing it for consumers. However, during 2012, media reports alleged that businesses were personalising prices offered to consumers, without clear disclosure, based on their browsing history, demographics, marketing segment or other observable or inferable information they had collected about them. The reports were questioning whether this practice was overstepping the boundaries of fairness, and highlighting privacy concerns. We recognised that if true there may have been issues for us to address, and whether or not true further speculation could cause consumers to lose trust in online markets, and harm the development of new business models based on data analysis for example.

In order to gain a better understanding of what was happening we launched a call for information in November 2012 ([please see annex 2](#)) and asked businesses and other interested parties to provide us with information to:

- understand whether personalised pricing is likely to be harmful or beneficial, or whether this will depend on specific circumstances
- identify how available technology may support personalised pricing
- understand more about the market for personal data and how this is linked with personalised pricing
- research if consumers understand how businesses capture data about them and how that data may be used
- identify the legal framework and policy initiatives that exist in this area, and whether further interventions may be necessary, and
- see whether there was a need for any enforcement action.

What did we find out about personalised pricing?

Businesses set prices according to different factors such as product costs, stock levels, strength of competition and an assessment of how much generally consumers are willing to pay. This means that two products that appear the same to consumers may be offered at different prices. For example, the same mobile application may have a different price depending on which mobile device it will be used on because of the different costs of development. Similarly, demand for products changes over time, so that a product that is expensive when new may become cheaper once it no longer has novelty value and demand for the product falls, or competing products have entered the market. However it is also true that different consumers would often be willing to pay different prices for the same product – for instance different consumers may buy the same product on the same day in different shops, but pay different amounts. Therefore where a product is offered on a website at a fixed price, there may be some consumers who feel that it is a great bargain, while there are others who feel they are not able to afford it at all. There is a benefit to businesses in identifying those consumers who might be willing to pay a bit more for a product, and increasing the price to them, while at the same time reducing the price to those consumers who would not otherwise be tempted to buy at all.

Media reports and consumer complaints expressed fear that businesses were using cookies and other internet technology to identify consumers who might be persuaded to pay more for products, and increasing the price to them. We asked businesses about this, and they told us that they had no desire to identify individual consumers, and were aware of the potential adverse consumer reaction to actual or perceived invasions of their customers' privacy. They are however seeking more information about their customer base in order to help them to make pricing decisions. They do this by using information that they analyse to achieve greater, granular segmentation of their customer base.

The ability to segment consumers into refined groups is enhanced by the collection of large amounts of information about consumers. It enables businesses more accurately to target behavioural advertising and to practise:

- **search discrimination**, where consumers are presented with the products that it is considered they will find most relevant
- **targeted discounting**, where vouchers and discounts are provided depending on previous shopping habits, and
- **dynamic pricing**, where prices fluctuate due to the availability of and demand for a product.

The media reports we reviewed and the consumer complaints we received, which alleged instances of pricing specific to an individual, showed that consumers and media commentators find it difficult to distinguish between personalised pricing and other forms of price discrimination. Prices online go up and down (sometimes rapidly) and it appears that consumers do not always understand why and may think they are being offered a price based on information collected about them personally. However, we think retailers may change prices in response to competition, current demand and stock levels, for example. They may also offer products for different prices on different websites (for instance where these sites are targeted at markets in different EU countries where different prices reflect different costs to the business).

We do not think that businesses in the UK are currently using cookies or other internet technology (see [annexe 3](#)) to offer higher prices to some consumers, as a consequence of the web browsing or purchasing habits of those individuals. However this is an area that we want to keep under review, as we had limited responses from businesses, we know that the technology exists to do this, and it is not always easy to detect when personalised pricing is actually occurring.

Examples of pricing practices online, that have been described as ‘personalised’ pricing in various media reports

Price discrimination: In the USA, some retailers may require the consumer to provide their Zip Code before continuing to shop. The Wall Street Journal research reported that geographic location affects price in US based stationery stores and DIY companies – specifically when there is a proximity to a competitors’ store ([Websites Vary Prices, Deals Based on Users' Information – Wall Street Journal](#)).

Researchers in Spain (Universitat Politecnica de Catalunya, Telefonica Research) found price differences for e-books. In the research, they queried the prices of books listed on an online retailer's 'top 100' list from six locations. In a majority of the cases, the price difference was at least 21% and was seen to be as high as 166 per cent. ([Detecting price and search discrimination on the Internet - Universitat Politecnica de Catalunya](#)).

Search discrimination: Newspaper articles from the US suggested that the type of electronic device used by consumers may affect search options (with the use of more expensive devices potentially leading to more expensive options being highlighted or displayed at the top of the search list) ([On Orbitz, Mac Users steered to pricier hotels - Wall Street Journal](#))

Researchers in Spain (Universitat Politecnica de Catalunya, Telefonica Research) reported that another way to discriminate among customers with different willingness to pay is to provide more expensive products when they search within a particular product category. ([Detecting price and search discrimination on the Internet - Universitat Politecnica de Catalunya](#)).

Some companies suggest different credit cards to consumers based on information gathered ([On the Web's Cutting Edge, Anonymity in Name Only – Wall Street Journal](#)).

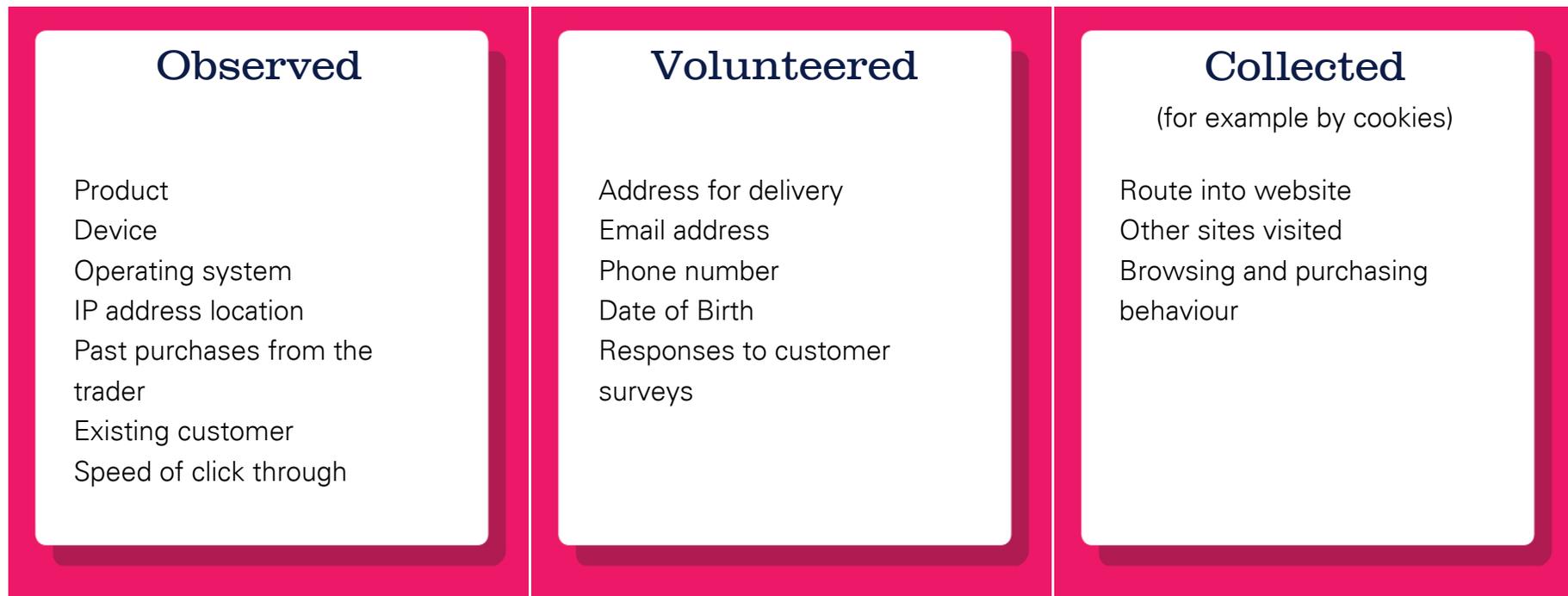
Targeted discounting: Articles in the Wall Street Journal alleged that routing via a price comparison site may affect the price of a product listed on the source site (as such consumers may be seen as bargain hunters/savvy) ([Want a Deal Online? Pose as a Bargain Shopper – Wall Street Journal](#)).

Dynamic pricing: Online retailers use fluctuations in demand to change the prices of their products depending on availability. Products which are likely to be priced dynamically are those which may be perishable, time-sensitive (airline or travel tickets), those with a depreciating value (technology based goods), or if they are scarce (event tickets). Allegations were that browsing history (in particular the information captured by cookies) affected the price offered, by indicating the consumer's desire to purchase. ([Behavioral Pricing: A consumer's worst nightmare, a merchant's dream – The Next Web](#)).

How can prices be ‘personalised’?

Businesses with limited consumer information can only segment consumers into large groups. However, as businesses collect more information to make inferences about how much consumers would be willing to pay, they may be able to place consumers into more refined groups. One way of doing this more accurately is to use information that is observed, volunteered, inferred, or collected about individuals. Such information could include some or all of the categories in the boxes below, for example, whether a consumer has arrived at a website via a price comparison site, a consumer’s postcode, their previous shopping history or what type of device they are using to browse a website.

In general, the more information that a business has about a consumer, the more accurately they are likely to be able to predict willingness to pay.



The research and evidence we have collected indicates that prices online are often dynamic or variable, but do not appear to be set on the basis of personal information. Prices vary depending on factors such as:

- the time of purchase, as prices vary according to the demand for them and availability
- the location of the consumer, for example, pricing on EU websites appears to be based on which country you are in, rather than precise IP location, and the price may be the same for all consumers who are in that state, and
- the route in to the website, so that consumers who arrived at a website via an associated website are offered a price and this price may differ from that shown to consumers who arrive at the website directly.

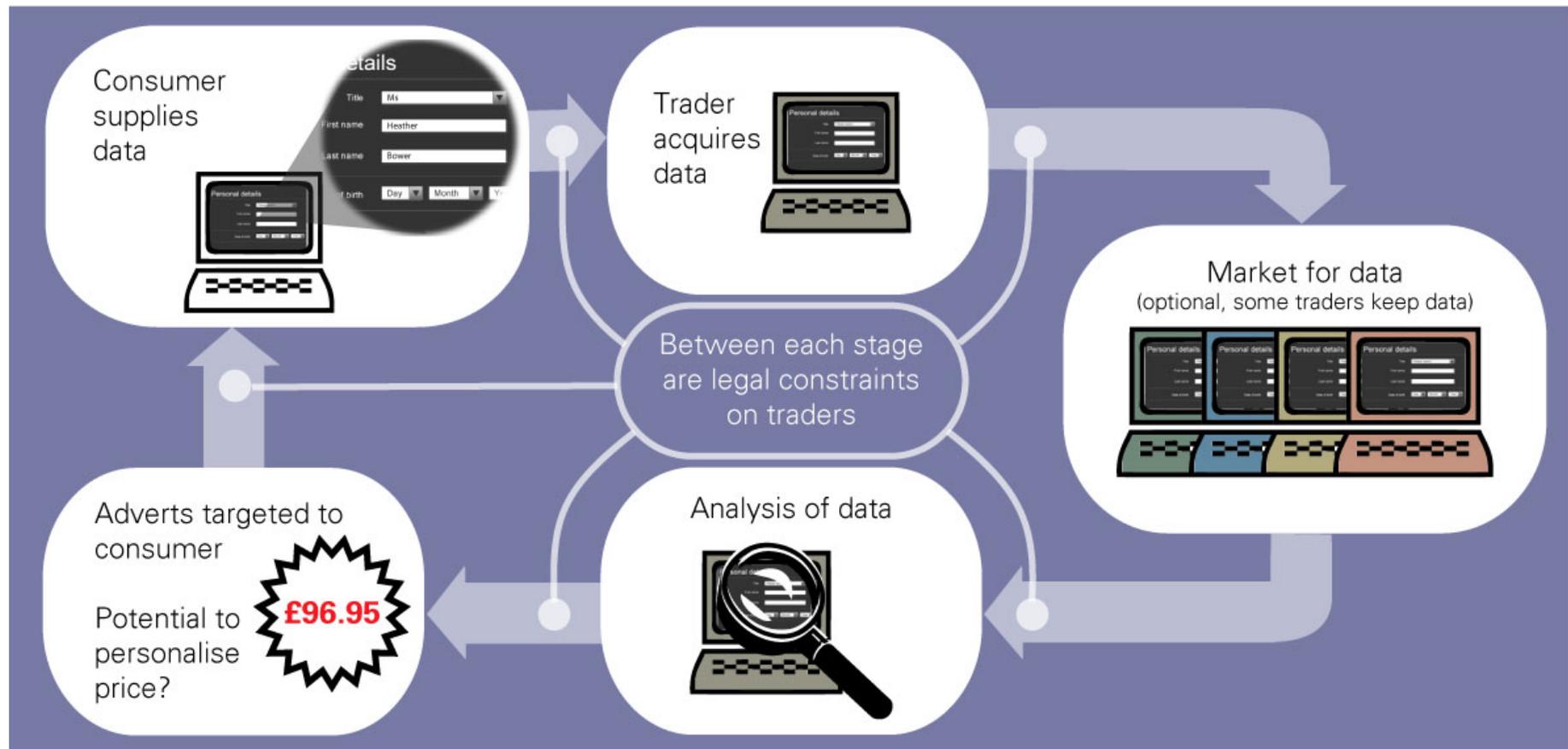
The research and evidence we have collected indicates that businesses are trying to identify different sorts of customer and segment their customer base into fine groups, rather than seeking to identify who individuals are. They are very aware of the potential adverse consumer reaction to actual or perceived invasions of their customers' privacy ([Data transparency builds trust – Brand Republic](#)). However businesses do use more personalised information in order to offer discounts and special offers, and this practice is generally welcomed by consumers.

Case study

Many respondents referred to what happened to Amazon.com in the USA in 2000. At the time a company spokesman described it as 'a very brief test to see how customers respond to various prices'. One man recounted how he ordered a DVD, paying \$24.49. The next week he went back to Amazon and saw that the price had jumped to \$26.24. As an experiment, he stripped his computer of the electronic tags that identified him to Amazon as a regular customer. Then the price fell to \$22.74. It is widely reported that customer criticism led to Amazon offering refunds to DVD buyers who bought at the higher price. In our own research, we found no evidence of prices being set on the basis of individual consumer profiles by Amazon or any other company, as opposed to a broader group, or type, of consumers. However, we have seen that the technology exists to do this (please see [Annexe 3](#)).

How technology helps to ‘personalise’ prices

The responses we received from businesses confirmed that the technology which may enable businesses to personalise prices was likely to be similar to the technology used to personalise advertisements ([Online Performance Marketing, Cookies and You – Internet Advertising Bureau UK](#)). The practice of personalising prices is facilitated by the process of capturing, processing and analysing information captured about consumers (see [annexe 3](#)). Businesses agreed that the process could be illustrated as shown:



Information about a consumer's interaction with a business is often captured by an online retailer when a consumer is searching or shopping online, for example, their interest in a particular company or product. [Annexe 3](#) explains how retailers capture information using different technology tools.

The business now holding this information has a potentially valuable commodity, which it may wish to use for its own analytical research and/or may pass on to other businesses (third parties) which operate in a market for consumer information.

These third parties might offer data-analysis services, or may combine or aggregate the information with other, additional information, or offer data analysis tools. All of these services help to optimise the value of the information and may make the collected information more useful to retailers.

The information might also be used to personalise offers, such as offering a consumer a discount on listed prices based on that consumer's previous shopping history, or might alternatively be used to entice consumers to purchase new products based on inferred interests or preferences.

There appear to be constraints to the practice of personalised pricing, such as losing the good will of consumers. Businesses we spoke to referred to the reports about Amazon.com in the USA in 2000 ([see case study p13](#)) and told us that damage to their brand's reputation was a significant consideration. We may expect that the degree of sophistication around price discrimination will increase over time, as businesses use services and technology to more finely segment consumers. We think that increasing the price depending on an assessment of an individual's willingness to pay is unlikely at present, although we think it is more likely where the product in

Case study

We spoke to a company considered to be one of the market leaders in providing technology that allows e-commerce websites to track consumer behaviour and supply personalised advertising, promotional offers and product recommendations to its clients. The company claims to help retailers increase sales and effectively monetise website traffic by taking consumers' data, including what items they have clicked on, and their search, purchase and shopping cart history, and then provides the most relevant products, content and offers to shoppers.

question is highly personalised (such as is often the case with financial services), and the price is therefore naturally likely to vary from person to person.

Pricing online is becoming increasingly dynamic, and there are often discount vouchers available. We would encourage consumers to be more aware of this when shopping online. When searching for the best deal they should compare with offline prices and not assume they are being offered the best price possible, even when dealing with a company they may have engaged with before.

Research on whether cookies are used to influence price

A common allegation that we considered was whether cookies are used to influence price. Cookies can be used to track people's use of the internet – see [annexe 3](#) for more information.

We received complaints that prices increased because of repeated searching when using travel aggregator, hotel/accommodation and transport websites. We also looked at allegations that prices changed if different devices were used, if a consumer took a different route to a website and that different prices were offered on a dating website dependent on the consumer's age. Whilst we acknowledge that we could not exactly recreate the same conditions which would have been experienced by the consumer in these cases, we looked at the websites which were brought to our attention, to see if they raised concerns that warranted further investigation. We did not find any evidence that would warrant further investigation in these limited and specific tests.

However, research carried out by Universitat Politecnica de Catalunya in 2012 examined 600 different products from 35 product categories and 200 vendors; selecting low/med/high price products from each vendor ([Detecting price and search discrimination on the Internet - Universitat Politecnica de Catalunya](#)).

The tests compared:

- technological/system differences (different browsers running on different operating systems)
- geographic location (US, Spain, Germany, Korea and Brazil), and
- personal information (by creating an affluent and budget conscious consumer)

The research found:

- There was no price/search discrimination based on the use of operating system or browsers.

- There were price differences based on geographic location, for example digital products- ebooks and video games- are priced differently in different countries. There were price differences for a USA stationery retailer when the queries originate from different locations within the same US state.
- When (fake) personas based on affluent or budget conscious consumers were used, there was evidence of search discrimination; products up to 4 times more expensive were shown to affluent personas rather than the budget conscious persona, in search engine 'sponsored' results (although 'natural' search results were unaffected).
- The research also found signs that for some product categories, visiting a vendor site via a discount aggregator site gave prices 23% lower than when visiting the vendor site directly.

What did consumer complaints reveal about personalised pricing?

The consumer complaints we reviewed indicated that consumers appear to be more concerned in some situations than others.

Consumers are likely to be more concerned when:

The fact that price discrimination is occurring is not transparent to consumers

Price discrimination is not expected by consumers with respect to the products they are purchasing

Pricing is ever-more personalised (approaching being specific to an individual).

This may bring two different concerns. First, consumers may be generally concerned about their privacy as information is being collected about their behaviour online. Second, they may have additional, or alternative, concerns about this information being used to influence the prices that they face when searching and shopping online.

Where consumers do not understand online pricing practices or they suspect that they are being presented with higher prices than other people, there may be a reduction in trust in online markets. We are likely to be concerned if consumers reduced their online purchases because of fears (whether genuine or misplaced) about the practise of online personalised pricing, or if they made less use of useful functions on their mobile devices, or were afraid to engage with new business models that could otherwise deilver value to consumers and the wider economy.

Transparency, the ability to **opt out** of the collection of information and **understanding** are crucial to developing and maintaining trust in online markets. There is a risk that businesses will not be able to capitalise on the benefits of internet and mobile commerce if consumers' trust is undermined. Businesses can help by providing greater transparency to help consumers gain an improved understanding of their online business practices and how information provided by consumers is used for their online business.

Consumers' understanding of how their information is used by retailers

midata

The Government's midata work is recognising the value of personal information. This project aims to release information back to consumers to enable them to make more informed decisions.

The Enterprise and Regulatory Reform Bill included provisions to give ministers power to regulate to require companies to release their data back to customers and has now received Royal Assent. Before using the power the programme will review progress across the key elements of: data release, building confidence and fostering development of new insightful services. The review process is due to start in 2013. For more information on the Act see the [midata factsheet](#).

Businesses operating online often collect and analyse data about consumers. Comprehensive information gathering is prevalent online and our [Online Targeting and Advertising of Prices study](#) explained that the collection, analysis and exchange of consumer information underpinned behavioural advertising. It also underpins personalised discounting, selling personalised products and 'personalised pricing'. Consumers' information has a value to companies and is stated by businesses and advertisers to underpin much of the 'free' content on the internet.

Businesses told us about the categories of information they collect to fulfil orders (such as demographic, payment and transaction information) and how they use such data for other purposes (for example, in order to improve their website, for future marketing or to make websites easier to navigate). This could include analysis of which parts of the website people actually look at, when people are browsing, and in what circumstances people go on to buy products. However there so far appears to be very little development of business models which analyse the historic shopping habits of specific individuals, in order to offer added value to those consumers. This may change as take up of the **midata** programme broadens.

Businesses say they are using their ability to aggregate and analyse vast amounts of consumer information to innovate and grow. Most of the businesses that did respond told us they provide information to consumers about data collection. There were both positive and negative responses about whether consumers could opt out from having their information collected in the first place. However, we had few responses from businesses engaged in this part of the data market. This may be because many of these businesses are based in the US, and at least one internet based legal commentator publicly advised data brokers not to respond to the OFT's call for information. Given the low response rate, we do not know, for example, if consumers' information is kept for many months or years. Indeed, businesses collecting the data may not know themselves how or whether it will ultimately be used, and at which level of detail (for example, highly aggregated or disaggregated).

We did not initiate any new research about consumers during the call for information as we found a great deal of recent research about consumers' understanding, awareness and attitudes, which we set out [at annexe 5](#), regarding the collection and use of their data online.

Federal Trade Commission

In the USA, the **Federal Trade Commission** recently announced action to regulate data brokers' activities so that they provide consumers with greater transparency as to what data brokers do with personal information, and detail the access rights and other choices for consumers for the data they maintain. As many brokers are based in the USA, these measures are likely to have an impact internationally and not only in the USA.

See '[FTC to Study Data Broker Industry's Collection and Use of Consumer Data](#)'

This research showed that consumers:

- have a low understanding of what companies and websites do with information gathered about them
- have high levels of concern about businesses that collect and sell on information, including volunteered personal data (such as mobile phone number, date of birth and responses to customer surveys) to other third parties, which then target consumers with products and adverts
- are concerned about their privacy, and
- want to protect their personal information

However, in practice it is very difficult for consumers to know the full extent of the information collected about them as it is aggregated and transferred to other third parties. Also, we found that consumers are not made particularly aware of how this data market operates, so the question of whether they fully understand the value of their information to businesses in this market remains unanswered.

Consumers' control of the information they provide

Although the law is not prescriptive about the method of communication, usually cookie notices and privacy policies, which are available to view on a firm's website, set out how consumers can control the collection and use of their information – both that which the company collects on them and that which the company allows others to gather from their website. However, research showed that only 50 per cent regularly read privacy policies ([Communications Consumer Panel research report](#)) and suggests that consumers may remain largely unaware of the amount of information collected or that the information collected about them whilst online may be released to third parties without the consumer taking some action, such as clicking through to give their preferred permission or to prevent this if they wish to. Generally we were disappointed with the level of transparency by businesses about what information businesses were collecting and how it is used. This lack of transparency harms consumers' trust in traders and business practices.

Online and mobile retailers are in a powerful position, with access to a lot of information, and the ability to use sophisticated technology. We do not want to see businesses exploiting this position unfairly, because this creates suspicion and could lead to consumers using online and mobile services less, or seeking to use avoidance strategies that inhibit the development of useful new business models. For example if consumers are concerned about businesses identifying their geographical location through their mobile phone, and disable this functionality in consequence, this will hinder them from taking up useful app based products which could offer benefits when shopping. Similarly, suspicion about 'leaky' apps is likely to reduce consumption of these generally.

We think that low engagement from consumers may also undermine the efficacy of the mechanisms which are in place to protect them. Consumers have a significant role to play in how their information is released to businesses online in the first place, and businesses should do more to help them to be more engaged with this process ([Online and computing – Information Commissioners' Office](#)). It remains to be seen whether recent regulations on disclosure of use of cookies on websites increases consumer engagement with the way their information is collected and used.

During the call for information, we reviewed the privacy policies of the top 20 UK retail websites and found that all of these collected consumer information and permitted collection by third parties too. If a consumer wanted to look at information about a cookie placed by a third party, it was sometimes necessary to look at that third party's own cookie policy or notice. We found that many lacked detail on those issues which were likely to be important to consumers.

Some businesses failed to:

- provide specific details on how information would be used
- make it clear to consumers which information was being collected because it was essential to a transaction, and which was being collected for other purposes
- provide specific details about the other organisations they would transfer information to, particularly the names of other businesses in a connected 'group' or their 'trusted partners'
- make it clear how to opt-out of certain types of data collection or use, or provide any opt-out at all

We think that it is not practical for consumers to be required to click through to several third party privacy policies in relation to each web page visited in order to understand how their information will be used. Therefore, consumers cannot efficiently and effectively engage with privacy policies and cookie notices which are meant to enable them to exert more control over the collection and use of their information. It

Cookies

For most of the websites we looked at during the call for information, the numbers and nature of third party cookies present on websites were observed using a cookie detection application, and this was then compared with the information provided in the Cookie notice and/or Privacy Policy of the websites in question. This demonstrated that in most cases there were a varying though substantial number of third party cookies on these websites and that the policies often did not inform the consumer of the nature of them, and even when they were listed, this list did not always tally with those found by the cookie detection application.

We think that this demonstrates how confusing it can be for a consumer to attempt to find which specific cookies were on the websites they were visiting and what information was being collected about them.

should also be noted that by the time the consumer has visited the third party policy, the cookie may already have been set and information on the consumer collected.

We have referred our research on privacy policies to the ICO in line with our [memorandum of understanding](#) The ICO and OFT will continue to seek to share information and intelligence, under this MOU, and we are alert to complaints or cases of common interest in this area.

Is personalised pricing harmful to consumers?

Much of the commentary about personalised pricing tends to assume that personalised pricing is something to be feared or at least treated with suspicion. A major part of our work was to consider the impact on consumers of personalised pricing, in order to try to understand in which circumstances this might be harmful to them. Our research looked at highly refined, direct, price discrimination online, where prices are targeted at specific groups of consumers.

Our economic research indicates that personalised pricing can have both harmful and beneficial effects depending on the particular circumstances in which it takes place. It may have a positive impact on consumers overall if a significant number of additional consumers were able to buy a product at a cheaper price due to higher prices paid by others. This is more likely when there is effective competition in the market. For example, if a producer of a new electronic device is able to identify a sufficient number of consumers with a high willingness to pay for the product, this may enable them profitably to also offer the same product at a lower price to consumers with a low willingness to pay who otherwise might not buy the device at all. The benefit to the latter may outweigh the harm to the former.

In essence price discrimination often entails winners and losers. We would be concerned if the harm to those that are made worse off as a result of price discrimination, the 'losers', outweighed the benefits to those that are made better off, the 'winners'. For example, we may be concerned if online retailers used information to identify and target a group of more price sensitive consumers (such as those with an intention to switch). The ability to offer discounts to a relatively small group of price sensitive consumers may mean that the business is able to increase prices to a larger group of consumers who are less price sensitive, meaning that consumers overall pay more. This could be particularly problematic in markets where there is a general lack of switching, or where there are only a few powerful firms. We may have additional concerns if price discrimination were to be used in an exclusionary way. For example, if discounts were offered to dissuade consumers switching to a new entrant, or to cause a rival business to exit the market, the consequence may be that the remaining firm is able to increase prices to consumers overall.

Furthermore, even if the overall benefit to consumers of price discrimination were positive, we may still be concerned if the group who were disadvantaged by price discrimination were considered vulnerable (vulnerability may relate to the capacity of the consumer – for example, poor literacy or numeracy skills or low income (individual vulnerability), and may also relate to the nature of the product or service, and/or the way it is sold, such as high pressure selling (situational or transactional vulnerability)).

However, our most significant concern currently is the potential for personalised pricing to harm consumers by leading to a reduction of trust in online markets. Where there is a reduction in trust, it is likely that consumers will reduce their consumption, or refrain from consuming new products, which may have a negative impact on the growth of internet shopping. This is more likely where personalisation is carried out in ways that are not transparent and it is hard to understand what is taking place.

For more details about our economic analysis see [annexe 4](#).

We have set out an economic literature review of online personalised pricing in a separate report '[The economics of online personalised pricing](#)'. The literature review provides a detailed assessment of how different characteristics (for example, the type and intensity of competition between online retailers) affect how imperfect, direct, price discrimination would impact consumers compared to circumstances where there was only uniform pricing.

Is personalised pricing illegal?

There are laws and rules that apply to businesses at three stages in the process of personalising prices –at the time that information is collected from consumers, during the processing and analysis of that information, and when a price or product is presented or advertised to the consumer. Please see [annexe 6](#). The laws that apply include:

- regulations governing the **terms of contracts**, which may include privacy policies or other website terms of use
- privacy rules governing the use of **technology** to gather information about website users
- data protection law restricting how **personal information** can be collected and used
- equality laws which prohibit **discrimination** in relation to specific characteristics
- legal and industry rules on **advertising** and price statements

Key facts

The terms of use of a website, and any privacy policy applying to users of a website, may be contracts for the purposes of the **Unfair Terms in Consumer Contracts Regulations 1999** ('UTCCRs'). Terms that provide for how data will be collected and used are likely to be subject to the test of fairness under the UTCCRs.

UTCCRs at a glance

The UTCCRs require standard contract terms to be in plain and intelligible language, meaning the consumer must be able to understand what rights and obligations the term actually creates.

Important contract terms, particularly those which may disadvantage consumers, must be clear, prominent and actively brought to consumers' attention. It may not be sufficient only to include terms in a privacy policy, especially where that document is lengthy or otherwise hard to find or navigate.

Businesses must not take advantage of a consumer's weaker bargaining position or lack of experience in deciding what their rights and obligations shall be, and the terms should be drawn up in a way that respect a consumer's legitimate interests. This is particularly relevant in relation to the online collection and use of data, as consumers may be unfamiliar with the technological aspects of these practices, or be unable to exercise effective choice.

Privacy Regulations at a glance

Web publishers must provide clear and comprehensive information about any first and third party cookies on their site

Web publishers must obtain consent to store such cookies on a user's device

If the website includes third party cookies, third party advertisers which set cookies share these responsibilities

Those setting cookies should ensure that they provide information about how consent can be withdrawn, and cookies that have already been set removed (for example, in a privacy policy).

The Privacy Regulations ([The Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#)) govern the use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment such as their computer or mobile. They require parties which set cookies on a user's device to obtain informed consent to their use unless the cookies are essential for the supply of a service requested by the user, for example to add goods to a shopping basket. The Regulations apply whether or not the cookies collect personal data.

In addition, the **Data Protection Act 1998** ('DPA') governs the processing of personal data ([Definition of 'personal data' in the DPA](#)) including sensitive personal data (for example as to a person's race, religion, or sexual life). It requires businesses to process personal data lawfully and fairly which, in this context, includes telling individuals what they intend to do with information they collect and whom it will be shared with, and obtaining consent for certain uses. For example, it is likely to be impermissible to process data in order to identify a person's state of health, including whether they are pregnant, or sexual interests etc, unless the person has specifically consented to this processing.

The ICO carries out [annual surveys](#) to track public awareness of issues relating to data protection. They found that people have very high levels of concern generally about the ways in which organisations handle their personal information. These concerns included organisations passing or selling on personal details to others, requesting too much or irrelevant information and holding information for longer than is required.

The **Equality Act 2010** prohibits, with a few exceptions, discrimination on the basis of protected characteristics such as age, disability, pregnancy, gender or sex related issues, marital status, race or religion. The [Equality and Human Rights Commission](#) ('EHRC') has the statutory remit to enforce the Equality Act. The EHRC has powers of investigation and enforcement.

The Provision of Services Regulations 2009 (PSRs) restrict discrimination between customers in the EU on the basis of their place of residence. For example the PSRs prevent online retailers from offering different terms for providing the same service to consumers on the basis that they live in different locations (either within the same country or in different countries), unless this can be justified objectively (such as on the bases of additional costs due to distance travelled or technical characteristics of the services).

If information such as the collection, use and transfer of their information, or information about prices is omitted or is false or misleading then this may also affect a decision that a consumer

Data Protection Act at a glance

If a web publisher collects information through which an individual may be identified, for example to build a consumer profile, it must comply with the data protection principles, in particular to process personal information fairly and lawfully. It must:

- make sure individuals are aware of the identity of anyone who collects personal information through the site and what they will process their information for
- tell individuals if it will disclose such information to third parties
- tell people what information is being collected and for what purpose
- process personal data securely using appropriate technical and security measures and keep it securely, and
- keep it for no longer than necessary.

CPRs at a glance

The CPRs prohibit traders from engaging in unfair commercial practices which have or are likely to have an effect on the economic behaviour of the average consumer.

They prohibit such practices where they fall below an acceptable objective standard of market practice; where they are misleading actions (such as the provision of false or misleading information), misleading omissions (such as the omission of certain material information), or aggressive (practices which significantly impair or are likely to significantly impair the average consumer's freedom to make free or informed choices in relation to a product).

Breach of the CPRs may be a criminal offence and may also be enforced by way of civil enforcement.

Certain practices are considered unfair in all circumstances and are specifically prohibited, for example falsely claiming to be a member of a code of conduct or authorisation scheme, or being a member and failing to comply with the requirements of the code or scheme.

may make in relation to a product (a 'transactional decision') and, as such, breach the **Consumer Protection from Unfair Trading Regulations 2008** (CPRs). The CPRs prohibit unfair commercial practices which distort consumers' transactional decisions, as well as a number of practices that are prohibited outright.

A business may breach the CPRs by, for example, failing to tell consumers that information is being collected about them, and used commercially, where a privacy policy does not accurately represent the information actually being collected, or where information is being used covertly to personalise a price. The failure to provide this information could be a misleading omission. It may also breach the CPRs by falling below an acceptable standard of market practice.

Statements about prices, such as special offers, discounts and similar, could be misleading if the use of personalised pricing makes them untrue. For example, if an internet retailer were to make a claim that a price is discounted, when in fact it is higher than that paid by other consumers. This too could be a misleading action under the CPRs.

The Advertising Standards Authority ('ASA') has introduced [new rules on Online Behavioural Advertising](#) ('OBA') OBA is a form of targeted advertising, where customised advertisements are displayed on the sites visited by web users. Third party advertising businesses – such as networks – work with web publishers to analyse a web user's browsing activity to decide what advertisements they might be interested in, and then store cookies in their web browser which determine what advertisements are displayed. This process does not identify a consumer.

The rules – integral and complementary to a pan-European industry initiative – (see [Your Online Choices](#)) require these third parties to provide notice in or around the advertisements themselves which inform web users that OBA is being carried out. The notice could be an icon, symbol or text, with a link to the opt out mechanism. The third parties must also provide a similar notice and way of opting out on their own website.

Third parties that collect information about all or most of the sites a web user visits, for example via Internet Service Providers, must get explicit consent to collect and use that information for OBA. Third parties must not target OBA at children aged 12 or under.

The rules apply to the third parties who collect, analyse and use information for OBA, rather than the advertisers themselves, but advertisers will be expected to co-operate with the ASA to identify the relevant third party.

Businesses that fail to comply with industry rules such as these may also infringe the CPRs, if their conduct is likely to

Future Developments

At the European Commission, there are negotiations to implement a revised Data Protection Regulation. For more information see the Proposed new EU General Data Protection Regulation analysis paper. Current discussion on the revised Data Protection Regulation can be found on the Information Commissioner's Office website.

We are providing a summary of the legal requirements at [annexe 6](#) and will be working with the Information Commissioner's Office to develop joint guidance on privacy notices covering the consumer protection regulations and the Data Protection Act.

have an impact on consumers' economic behaviour. Other self-regulatory organisations across Europe, like the ASA, will be implementing similar rules to complement the EU scheme.

When would the OFT be concerned about online personalised pricing?

Online businesses are in a powerful position because they are able to accumulate lots of information about consumers which can inform their pricing strategies and practices. Lack of clarity by traders, and lack of understanding by consumers, about what data is collected and how it is used, has an impact on trust in online markets. There is also a real risk of consumers perceiving this sophisticated form of price discrimination as unfair. This could cause a reduction in online retail or cause consumers to take expensive or time consuming avoidance steps.

The [economic analysis](#) has shown that in general, personalised pricing, relative to uniform pricing, is more likely to be harmful under the following set of circumstances:

- Consumers make repeat purchases and how they behave on the retailer's website today affects the price they will be charged tomorrow, but consumers do not recognise this.
- It is not transparent to the consumer that price discrimination is occurring.
- It is very costly to the firm to price discriminate and this has an upward pressure on price.
- Concerns about online personalised pricing trigger a reduction in demand for products bought online due to a loss of consumers' trust in online markets. Consumers typically do not like the prospect of online price discrimination because it gives rise to uncertainty about how they will be affected individually, and due to concerns about fairness and privacy.

Generally the ability to segment consumers into groups to present innovative discounts and offers has benefits for consumers, especially where this increases competition. However we may have concerns with specific instances of online personalised pricing, even if it is shown that the overall effect is likely to be positive for consumers. We may be concerned if a significant number of consumers reduced their online purchases because of fears (whether genuine or misplaced) about personalised pricing or if those consumers disadvantaged by personalised pricing were vulnerable.

Where personalisation takes place, it is less likely to be harmful where consumers know it is happening, and understand how it works, for example where consumers receive personalised discounts as a result of membership of a loyalty scheme. However we may be concerned if it is practically difficult for consumers to avoid personalisation, even if they know it is happening, for example where it is conducted by a search engine, or it is based on user credentials the consumer is obliged to enter, or the equipment that the consumer is using to browse the internet – such as their device, browser type or operating system.

We may also be concerned where consumers are misled or treated aggressively at the point of presentation of the price, for example:

- Where there are misleading statements, for example:
 - stating 'best price', when in fact the consumer is paying more than other consumers
 - 'discount' sites which in fact lead the consumer to pay a higher price than going to a retailer directly
 - Recommended Retail Prices or other reference prices where in fact most consumers receive some form of discount.

- Where there are misleading omissions, for example:
 - where information used to personalise a price is requested for other stated reasons, such as in order to process an application or order quickly, and it is not clearly stated that this information will have an impact on the price presented
 - information that is collected covertly, for example by cookies
 - where it is not made clear that prices are personalised
 - if there is a base price, not making clear where the price is personalised, and how consumers can opt out of personalisation.

We would be concerned about price discrimination which is illegal, for example where there is a contravention of the Equality Act or the Provision of Services Regulations, or if sensitive personal data is being processed unlawfully, since this is not likely to be in line with acceptable market practice. Similarly, we think that personalisation should not take place where the use of data for online behavioural

advertising would not otherwise be permitted by a self regulatory code (such as the pan-European self-regulatory initiative as well as ASA rules in the UK) for example personalising prices for children under 12.

We think that consumers may make different transactional decisions if, for example, they know that their personal information may be passed on to third parties without their consent having been freely given. Consumers may also value their privacy to varying degrees and, if they do not want to share information, they may take different transactional decisions in these circumstances too.

While online businesses may wish to require access to consumers' data in order to permit access to a website or app they are offering, we consider that in this situation there should be full, upfront disclosure on the face of the website or before the app is downloaded, of what information is being collected and what use it is going to be put to. If the collection of data about consumers is not necessary for the provision of an online or mobile service, we believe that there should be no collection of data without the appropriate consents, and an ability to opt out of future collection. We consider that consumer trust would be improved if there is also a way of being able to request that data held about them for marketing purposes could be deleted.

We would need to consider the facts on a case by case basis but, but a non-exhaustive indication of issues we may consider relevant depending on the facts of the case may include:

When firms are collecting information, issues we may consider:

- if there is an impact on current or future transactions
- if the collection leads to higher prices or worse product offerings

When firms are using information, we may consider:

- if the use of the information collected breaches legal requirements, for example the analysis of information to identify sensitive personal data such as health, religion, sexual activity, etc
- if there had been a change in the context of the use which would be a surprise to the consumer, such as use of information gathered in order to make a delivery to target prices

- use of information that has been unlawfully obtained, or where the user is not able to demonstrate the provenance of the information (eg lead generation)
- if there was evidence of non adherence to the privacy policy and if there were issues about the provenance of information
- further transfer of information to a third party without agreeing the use the information will be put to.

If firms are using collected information to influence the final price stated, we may consider:

- transparency (how and at what point this was made clear to the consumer)
- whether a misleading action had led the consumer to think a certain price was available but in fact it wasn't.

We consider that transparency is key to enable consumers to know more about how information about them is collected and passed to other businesses. Consumers should be able to exercise choice about how their information is used easily and selectively.

Consumers' information has economic value, and the market for this information is likely to work better if consumers were able to engage with it more proactively. The market for this information is likely to develop further, and it is important that, in analysing business models that use comprehensive data collection, consideration is given by regulators and policymakers to market issues (the OFT's focus) as well as data protection and privacy issues (the Information Commissioner's Office's focus).

Greater transparency

Businesses should be more transparent about what information they are collecting about consumers, and how this is used, in accordance with data protection, privacy and consumer protection laws. Compliance with the Data Protection Act and EU self-regulatory initiative, should minimise the concerns we have. We support the EU self-regulatory initiative principles of notice, choice and education and think that if businesses provided **Notice**, **Choice** and **Education** to consumers about any personalisation, this would improve consumer trust significantly.

We would like consumers to be more aware that pricing online is increasingly dynamic and that prices fluctuate due to many factors ([Coming Soon: Toilet Paper Priced](#))

EU Self Regulatory Initiative principles

1. **Notice:** Transparency about data collection and use practices associated with behavioural advertising, providing consumers with clear, prominent and contextual notice through multiple mechanisms, including an icon in or around advertisements linked to further information and control mechanisms.
2. **User choice:** Greater consumer control over behavioural advertising.
3. **Data security:** Appropriate data security and retention of data collected and used for behavioural advertising purposes.
4. **Sensitive segmentation:** Limitations on the creation of 'interest segments' to specifically target children and on the collection of sensitive personal data collected and used for behavioural advertising.
5. **Education:** For consumers and businesses about behavioural advertising and the self-regulatory Framework.
6. **Compliance and enforcement:** Mechanisms to ensure the effectiveness of the Framework, including a trading seal to be granted to compliant businesses once independently audited and which demonstrates to other businesses that the holder adheres to the obligations under the Framework.
7. **Review:** Regular review of the Framework to ensure it evolves with developing technology

For further information see [IAB unveils your online choices](#)

[Like Airline Tickets – Wall Street Journal](#))

When searching for the best deal they should compare with offline prices and not assume they are being offered the best price possible, even when dealing with a company they may have engaged with before. Consumers should look at a website's privacy and cookie policies and act to protect their information if they have concerns.

We expect businesses to take the opportunity to review how clearly they present options for consumers to opt out of first and third party information collection and to make privacy policies more transparent. More advice can be found at [annexe 6](#).

We will work with the ICO to explore and further understand the consumer and data protection issues related to the collection and use of information about consumers, particularly in the context of personalised pricing. We will also input into consultative process the ICO intends to run to review its Privacy Notices Codes of Practice and Personal Information Online Code of Practice, to see whether further data protection guidance can be provided on this issue and explore how any guidance can complement or work with guidance on consumer protection law.

Annexes

Annexe 1 - [What is online personalised pricing?](#)

Annexe 2 - [What information did we ask businesses for?](#)

Annexe 3 - [How technologies collect information from consumers](#)

Annexe 4 - [Economic analysis of where personalised pricing is harmful to consumers](#)

Annexe 5 - [Research on consumer attitudes and understanding about how their information is collected](#)

Annexe 6 – [Legal requirements and privacy notices](#)

References

A list of weblinks by page –

- Pg 4 OFT's Annual Plan
www.offt.gov.uk/shared_offt/about_offt/annual-plan13-14/OFT1462.pdf
- Pg 6 EU data protection legislation
http://europa.eu/rapid/press-release_IP-12-46_en.htm
- Government's midata project
<http://blogs.bis.gov.uk/midata>
- Action taken by the Federal Trade Commission in the USA
www.ftc.gov/opa/2012/12/databrokers.shtm
- Pg 8 Office of National Statistics – statistical bulletin
www.ons.gov.uk/ons/rel/rdit2/internet-access--households-and-individuals/2011/stb-internet-access-2011.html
- Ofcom research
<http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr12/post/uk-6.13>
- OFT's Online Targeting of Advertising and Prices Market Study
www.offt.gov.uk/shared_offt/business_leaflets/659703/OFT1231.pdf
- Pg 10 Websites Vary Prices, Deals Based on Users' Information – Wall Street Journal
<http://online.wsj.com/article/SB10001424127887323777204578189391813881534.html>
- Pg 11 Detecting price and search discrimination on the Internet - Universitat Politecnica de Catalunya
<http://conferences.sigcomm.org/hotnets/2012/papers/hotnets12-final94.pdf>

On Orbitz, Mac Users steered to pricier hotels - Wall Street Journal
<http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html>

On the Web's Cutting Edge, Anonymity in Name Only – Wall Street Journal
<http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html>

Want a Deal Online? Pose as a Bargain Shopper – Wall Street Journal
<http://blogs.wsj.com/digits/2013/01/10/want-a-deal-online-pose-as-a-bargain-shopper>

Behavioral Pricing: A consumer's worst nightmare, a merchant's dream – The Next Web
<http://thenextweb.com/insider/2012/01/21/behavioral-pricing-a-consumers-worst-nightmare-a-merchants-dream>

- Pg 13 Data transparency builds trust – Brand Republic
www.brandrepublic.com/research/1157134/data-transparency-builds-trust
- Pg 14 Online Performance Marketing, Cookies and You – Internet Advertising Bureau UK
www.iab-performance-marketing-explained.net
- Pg 21 midata factsheet
www.gov.uk/government/uploads/system/uploads/attachment_data/file/86519/bis-13-656-enterprise-and-regulatory-reform-bill-midata-factsheet-feb-2013.pdf
- Pg22 FTC to Study Data Broker Industry's Collection and Use of Consumer Data
<http://ftc.gov/opa/2012/12/databrokers.shtm>
- Pg 24 Communications Consumer Panel research report
www.communicationsconsumerpanel.org.uk/Online%20personal%20data%20final%20240511.pdf
- Online and computing – Information Commissioners' Office
www.ico.org.uk/for_the_public/topic_specific_guides/online
- Pg 26 The OFT's memorandum of understanding with the ICO
www.ico.org.uk/about_us/how_we_work/~/_media/documents/library/memo_of_understanding/Documents/MoU_OFT_and_ICO_110411.ashx

- Pg 28 The economics of online personalised pricing
www.offt.gov.uk/shared_offt/research/oft1488
- Pg 30 The Privacy and Electronic Communications (EC Directive) Regulations 2003
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide
- Definition of 'personal data' in the DPA
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions
- Pg 31 ICO annual survey
www.ico.org.uk/about_us/research/information_rights
- Equality and Human Rights Commission
www.equalityhumanrights.com/
- Pg 33 ASA's new rules on Online Behavioural Advertising
www.cap.org.uk/Advertising-Codes/Non-broadcast-HTML/Appendix-3-Online-Behavioural-Advertising.aspx
- Your Online Choices
<http://www.youronlinechoices.eu/goodpractice.html>
- Pg 38 IAB unveils your online choices
www.iabuk.net/news/iab-unveils-your-online-choices
- Coming Soon: Toilet Paper Priced Like Airline Tickets – Wall Street Journal
<http://online.wsj.com/article/SB10000872396390444914904577617333130724846.html>