The Information Commissioner's Office response to the Competition & Markets Authority's call for information on the commercial use of consumer data

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003.

He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to this call for information on the commercial use of consumer data and we look forward to working with the Competition and Markets Authority (CMA) during the course of its study. We reaffirm our offer to provide advice and support to the CMA in understanding the areas falling within the ICO's remit.

Not all of the questions posed are ones that the ICO can make evidenced submissions on. Accordingly we have only responded to those questions where we feel we can add value to the research being undertaken.

Section A
Consumer data collected, bought, sold and its value

A1 What types of information do firms collect on consumers and how is this collected?

A1.1 Firms collect a wide variety of data on consumers for a number of different reasons. At the most basic level firms may need to collect consumer data in order to supply products ordered and receive payment. This most basic commercial activity, especially in an online environment, will often necessitate the collation of customer contact details, such as phone numbers, email, and geographic addresses.

A1.2 Sometimes more detailed information is needed by a firm in order to provide a price or tailor the goods or services to be

offered. A classic example exists in relation to purchase of insurance whereby the insurer makes an assessment of risk, and hence the premium to be charged, based upon actuarially significant information provided by the consumer.

A1.3 Consumer data may be used for to help ensure advertising is effective and targeted, or more broadly by businesses to understand how they are performing and how consumers are interacting with them. Details of a consumer's shopping purchases may be routinely recorded, analysed and, in some cases, shared, by retailers. In e-commerce it is common for individual customer accounts to be created, linked to which may be a whole host data which has value to the business. In the physical environment consumer purchases and preferences may be recorded and analysed through use of loyalty schemes such Nectar and Tesco Clubcard.

A1.4 In some cases data is collected in the course of accessing goods, services or facilities offered by the firm. For example automatic number plate recognition (ANPR) technology, which until relatively recently was the preserve of law enforcement, is now increasingly employed within private car parks for parking enforcement purposes. In addition to identifying errant motorists, the data captured from such systems may also be analysed to provide information and insight into consumer behaviour.

A1.5 Likewise, we have observed the use of "ID scanning" in bars, nightclubs and other premises where customers may be required to produce a form of ID, such as a driving licence, in order to gain access to the venue. The consumer's credentials are then scanned into a computer system and retained, ostensibly for the prevention and detection of crime and disorder, but the information obtained may also be used for direct marketing[1].

A1.6 Consumer data may also be collected when consumers respond to "lifestyle surveys" or competitions. Indeed, the marketing of such surveys and competitions are, in themselves, a significant source of complaints made to the ICO[2].

A1.7 In an online context, data about consumers' activity may be used for the purposes of behavioural advertising. Behavioural targeting uses information linked through cookies to create a profile of a user. Cookies may record which affiliated sites have been visited and may also record location and past searches.

[1] <http://nightclub.co.uk/downloads/DataProtectionNotice-A3_d.pdf> accessed 03/03/2015

[2] "Lifestyle surveys" accounted for 2,499 complaints reported to the ICO between Oct 2014 - Dec 2014

A1.8 The ICO recently led an international study looking into the use of cookies on 478 websites[3]. The study found that:

- The average website set 34 cookies on a device during a person's first visit. UK websites placed the highest number of cookies within the study, averaging 44 cookies during a person's first visit.
- 70% were third party cookies set by websites other than the one being visited.
- 86% were persistent cookies which remain on a person's device after use.

A1.9 It is worth noting that data collected on consumers may not necessarily be 'personal data' for the purposes of the DPA. For example the data may be anonymised, or pseudonymised, to the extent that it does not constitute personal data when in possession of the firm in question.

A2 What data and analysis do firms acquire from third parties and at what cost?

A2.1 An entire industry exists around the supply of data, analysis and related tools. Industry would be in the best position to advise on the associated costs and the value it adds.

A2.2 It is worth considering that the services offered by credit reference agencies to other businesses extend far beyond simple credit referencing. Callcredit, for example, advertise the fact that they have access to "48 million marketable contacts, 37 million postal contacts, 19 million email addresses, 5 million landline numbers, 17 million mobile numbers"[4]. Experian advertise a wide range of services to "optimise your marketing campaigns"[5] which utilise the analysis of consumer data. Similarly, Equifax state that they can help:

> "find and contact individuals that fit your ideal demographic profile, identify and target the types of motivations that stimulate product purchase; determine the right time, right channel and right level to target your communications; monitor key life events, decisions and behavioural trends to gauge when customers are ready to buy; compare key attributes of your customer base to the rest of the UK

[3] <https://ico.org.uk/media/about-the-ico/documents/1043274/a29-cookie-sweep-combined-analysis-report.pdf> accessed 03/03/2015
[4] <http://www.callcredit.co.uk/products-and-services/consumer-marketing-data/define> accessed 03/03/2015
[5] <http://www.experian.co.uk/marketing-services/products/> accessed 03/03/2015

population or another subset of consumers, so you can tailor and target your marketing strategy"[6]

A2.3 Businesses such as IBM also advertise "an extensive portfolio of customer analytics products to help you optimize your day-to-day marketing activities and help guide your future strategies". These products include social media analytics, predictive customer intelligence and data collection[7].

A2.4 Retail analytics services are also a developing area. Retailers may buy in expertise from firms which have the capability to track customers in the real world environment having identified wifi signal from a mobile device. This data, in an aggregated form, can be used give to give retailers insight into consumer behaviour and help inform their marketing strategies.

A2.5 Data may also be obtained from publicly available sources, for example we were recently made aware of a case in which an estate agent had obtained details of the owner of a property in the local area from Land Registry records in order to market their services direct.

A3 To what extent do firms collecting consumer data licence/sell to, or exchange it with, third parties and what contractual arrangements apply (including pricing?)

A3.1 In one investigation undertaken we found that the firms involved had signed confidentiality agreements with data brokers resulting in them being completely unaware that they were within a chain/cycle.

A3.2 In another investigation we identified a consumer credit lender was passing on details of applicants who did not meet their risk profile to other potential lenders via a lead generation firm. The contractual arrangement provided that 50% of net revenue generated from selling or marketing the data would be passed back to the lender identifying the lead.

A3.3 One firm we recently dealt with either licence or sell the data they have collected to other organisations for specific purposes. They then assess that the data is being used in accordance with the contracts in place regarding the use of data. The firm stated that they are a data aggregator with huge trading relationships and contracts already in place, meaning that many data brokers prefer to go to them rather than go direct to the marketers.

---

[6] http://www.equifax.co.uk/business/find_new_customers/target_marketing/en_gb accessed 03/03/2015

[7] http://www-01.ibm.com/software/uk/analytics/rte/an/customer-analytics/products.html accessed 03/03/2015

A3.4 We have observed data being traded in chains, so that data controllers will provide data they have obtained to a list broker who, in turn, will supply that data to other list brokers and so on. These steps in the supply chain mean that identifying the provenance of data can be very difficult, and compliance risks are introduced as a result.

A4 For how long do different types of consumer information retain value for firms?

A4.1 We cannot give a definitive answer, but suspect there is a wide variance within the market. One organisation we dealt with advised us that they keep data for a maximum of 7 years, whereas another claimed not use data any older than six months - albeit that appears to be the exception. We suggest that different types of data may hold their value in different ways.

Section B
Uses of consumer data, restrictions in gaining access and controls available to consumers

B5 How do firms use consumer data and analysis, and for what sectors is access to this data most important?

B5.1 As set out at A1.1, the use of consumer data is a fundamental aspect of commerce for many types of business. Firms use consumer data and analysis for different reasons in order to satisfy their varied commercial interests, or in some cases to meet regulatory requirements.

B5.2 The ICO regularly publish statistics and an analysis of the complaints received regarding nuisance calls[8] and texts[9]. The CMA may consider this to be illustrative as to the areas in which consumer data is used for the purpose of direct electronic marketing. The subject of nuisance calls and text messages commonly includes green energy (boiler replacement, solar panel installations, loft insulation), claims management (payment protection insurance, personal injury), debt management, payday loans, "lifestyle surveys", competitions, gambling, laser eye surgery and adult content.

B5.3 Some industries, for example financial services, make extensive use of consumer data to determine whether to lend money to an individual and, if so, on what terms. Whilst creditworthiness has traditionally been assessed by reference to an individual's credit file held by a credit reference agency, we envisage that other

[8] <https://ico.org.uk/action-weve-taken/nuisance-calls/> accessed 03/03/2015
[9] <https://ico.org.uk/action-weve-taken/spam-texts/> accessed 03/03/2015

sources of consumer data will increasingly be used to undertake assessments. This may be driven in part by regulatory requirements placed upon lenders, but also by greater opportunities to access and analyse consumer data. There is a real challenge in ensuring firms are acting fairly and ethically when using analytics to make, or inform, decisions that affect individuals.

B5.4 Insurance is another sector where consumer data is used to determine risk and, in turn, price. We have observed some insurance companies obtaining increasing amounts of data, for example individuals' entire medical records (with limited exemptions), when an application is made for life insurance through attempts to use the consumer's subject access rights under the Data Protection Act[10].

B5.5 In-car telematics devices – the so-called 'black boxes' - which are installed in the consumers' vehicle and used to record and transmit driving habits to an insurer are increasingly widespread. Again, this data could be analysed to produce personalised premiums based upon past behaviour..

B5.6 Firms may also collect and analyse data for the purpose of meeting regulatory obligations. For example, many regulated sectors are required to follow, and record the results of, 'know your customer (KYC)' procedures and analyse financial transactions in order to identify suspicious activity and satisfy anti-money laundering (AML) requirements.

B7 What evidence is there that consumers understand and consent to the information firms collect about them and how it will be used?

B7.1 The secondary research carried out by the ICO for our paper on *Big data and data protection*[11] identified a number of papers on consumer attitudes to privacy and their use of their data, in particular those from Sciencewise[12], the Boston Consulting Group[13] and the International Institute of Communications[14].

[10] There is already an established statutory route by which insurers may obtain medical reports under the Access to Medical Reports Act 1988. In contrast a subject access will typically result in the disclosure of an individual's entire medical record.
[11] Information Commissioner's Office, Big data and data protection. ICO, July 2014 https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf
[12] Sciencewise. Big data. Public views on the collection, sharing and use of big data by governments and companies. Sciencewise April 2014. Available from: http://www.sciencewise-erc.org.uk/cms/big-data/ Accessed 25 June 2014
[13] Rose, John et al. The trust advantage: how to win with big data. Boston Consulting Group November 2013. https://www.bcgperspectives.com/content/articles/information_technology_strate

Some common themes emerge from these. There is a lack of understanding by consumers as to how and when their data is being collected and the uses to which it may be put. This is only likely to increase as big data and the Internet of Things tend to use data that is observed, derived and inferred, rather than provided deliberately by individuals[15].

B7.2 The view that people are increasingly unconcerned about the use of their personal data is too simplistic. Research shows that people have concerns about data use and these are reflected across all demographics to some extent. There is some discrepancy between people's stated concerns and their actions, namely that people do in fact provide personal data to access products and services, but this is more likely to indicate a fatalistic mind set - a feeling that they have no alternative - rather than necessarily active participation. There is also some evidence of people adopting strategies to protect their privacy, for example by providing false dates of birth.

B7.3 It is, however, unsafe to take an assumed lack of concern as a justification for avoiding the task of telling people when their data is being collected and what it is being used for. Furthermore, to do so would ignore obligations in data protection legislation.

B7.4 It is worth noting that the vast majority of the cases handled by our team responsible for investigating breaches have involved a cyclical use of data, and this makes it extremely difficult for consumers to understand how their data is being used. In one case handled by the ICO the complainant received the following SMS in February 2014: "We can now consolidate all your outstanding debts, freeze interest & charges & reduce the total amount to repay. Txt YES for more info - txt stop2 stop". There was no identifying information in the message so the complainant replied "YES" in order to find out who sent it. He was subsequently contacted by a debt counselling company who had obtained his information from a data broker. The data broker advised they in turn had purchased the data from a third company who was the sender of the text message. The third company told the complainant that he had put himself on "the

---

gy_consumer_products_trust_advantage_win_big_data/ Accessed 25 June 2014

[14] International Institute of Communications. Personal data management: the user's perspective. International Institute of Communications, September 2012. http://www.iicom.org/open-access-resources/doc_details/226-personal-datamanagement-the-users-perspective Accessed 25 June 2014

[15] Abrams, Martin. The origins of personal data and its implications for governance. OECD, March 2014. http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf Accessed 23 September 2014

sms opt in list" after responding positively to a text message regarding pensions in January 2013. The complainant had indeed responded to a text message regarding pensions in January 2013, however that message was unsolicited and he had only responded to it in order to identify the sender. The message read: "Get a large cash sum NOW from your TRAPPED/FROZEN pension?! Achieve high growth yield. Reply PENSION for your free info". This message was eventually traced back to a fourth company.

B8 How do firms provide consumers with information on, and control over, the collection and use of their data, and what are the consequences for consumers who exercise control?

B8.1 A key requirement of data protection is that that processing of personal data is fair, and a central facet of fairness in this context is a consideration of the method by which the data is obtained, and whether any person has been deceived or misled as to the purpose or purposes for which they have been obtained and will be used. Often this information is to be found within a privacy policy or notice.

B8.2 There is a danger that privacy policies can become complex, legalistic documents laid out in a way that is off-putting and impenetrable to even the most diligent and well-educated consumer. It can be especially challenging for an organisation to provide a clear explanation when the processing being undertaken is complex and it may require a consumer to have a background understanding; for example an appreciation of the way that the internet works and the function of cookies.

B8.3 In 2013 the ICO, together with 19 other Data Protection Authorities, participated in a Global Privacy Enforcement Network (GPEN) sweep of 2,186 privacy notices. The sweep found that 23% of the sites were reported to have no privacy policy at all, and of those that did, a third were considered to be difficult to read, and many weren't tailored to the website concerned[16].

B8.4 The rise of big data and the Internet of Things mean that personal data is often collected and analysed in unexpected ways, for example phone location data and metadata from social media. For instance, do people understand that Twitter data is sold via third parties even if they have read Twitter's privacy policy?

[16] https://iconewsblog.wordpress.com/2013/08/16/ico-blog-global-privacy-study-gives-international-view/

B8.5 We acknowledge that it is not always straightforward matter to deliver privacy notices, for example when people are downloading apps, but in our view this highlights the need for innovative approaches to delivering information. This could be through the use of graphics to help clarify lengthy terms and conditions. Privacy information can also be delivered in-product and in-time when an app needs to access additional personal data using a layered approach. Our guidance on Privacy in mobile apps[17] includes some examples of how this can be done. There can also be a value exchange, in which people receive some additional benefit in return for sharing more data.[18]

B8.6 Another aspect of this is people's access to their own data. Under the Data Protection Act, people have a right to obtain the personal data that is held about them by making a 'subject access request' (SAR). Firms should design their systems to enable them to retrieve the necessary information.

B8.7 There are also benefits to providing information to consumers proactively so that, for example, customers can log on to 'My Account' and see the data that is held about them. This approach is complementary to, and not a substitute for meeting statutory SAR obligations, since the data that is made available in this way is likely to be key account data rather than a record of every interaction they have had with the company. In some ways the government's midata programme is a development of this, since it is intended to allow individuals to export and share this data with other bodies, and this should give individuals a greater measure of control over their personal data.

B8.8 Researchers at the University of Sheffield, L'Hoiry & Norris, have recently conducted empirical socio-legal research on exercising democratic rights under surveillance regimes which may be of interest. Their headline findings include the fact that 20% of data controllers could not be identified before submitting an access request, 46% of requests did not result in obtaining access to personal data and in 56% of requests there was not adequate information regarding third party data sharing. They conclude that:

---

[17] Information Commissioner's Office. Privacy in mobile apps. Guidance for app developers. ICO, December 2013 https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

[18] International Institute of Communications. Personal data management: the user's perspective. International Institute of Communications, September 2012. http://www.iicom.org/open-access-resources/doc_details/226-personal-datamanagement-the-users-perspective Accessed 25 June 2014

Citizens, in their role of data subjects, encounter a wide range of legitimate but not always convincing and straightforward restrictions in their attempts to exercise their rights. These legal restrictions are further undermined by illegitimate actions enacted through a series of discourses of denial practiced by data controllers or their representatives.[19]

Section D
Policy implications and possible future developments

D12 What measures are firms taking to raise consumer awareness about the collection and use of data, while ensuring that both firms and consumers benefit from the use of consumer data?

D12.1 The examples of innovative approaches to privacy notices referred to in response to question B8 are relevant to this question. More generally, we are seeing some evidence of a growing recognition by companies of the need to adopt an ethical approach in order to promote transparency and build trust.

D12.2 In our research for our big data paper, some respondents told us that building trust was essential to adding value, both for the company and the customer. They want informed customers, who understand how their data is being used and are happy to share data because they can see a benefit from it. For example, Aimia, the loyalty card company, has a set of data values[20] which includes telling customers about data collection and use in an easily understandable format and giving customers control by telling them who it's being shared with and allowing them to opt out.

D13 What potential competition, policy, legal or regulatory changes might help to ensure or enhance the benefits for consumers and firms from the commercial use of data?

D13.1 We believe that privacy impact assessments are a particularly important tool for organisations to use where consumer data is being processed in new, novel or unexpected ways such as within a big data context. Companies need to identify the real benefits of what they are trying to achieve, rather than simply

[19] http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Executive-Summary-for-Press-Release.pdf

[20] Johnson, David and Henderson-Ross, Jeremy The new data values Aimia, 2012. http://www.aimia.com/content/dam/aimiawebsite/CaseStudiesWhitepapersResearch/english/WhitepaperUKDataValuesFINAL.pdf Accessed 25 June 2014

doing the analytics because it's possible, and assess their real impact on data subjects.

D13.2 The use of PIAs is an integral aspect of organisations adopting 'privacy by design' (PbD) approaches to compliance. Businesses need to be looking at a range of technical and organisational measures, including data minimisation, anonymisation, functional separation (between analytics to identify general correlations and making decision about individual customers) and building privacy controls (eg records of consent) into metadata.

D13.3 Given the difficulties of 'notice and consent' in a big data / IoT context, certification and assurance are important in ensuring data processing complies with DP requirements. Existing legal mechanisms such as consent and privacy policies are being superseded by technological developments. As data use grows exponentially[21], it is vital to give consideration to new regulatory solutions, within the existing legislative framework to protect the rights of individuals, in an easy to understand, effective way.

D13.4 In this respect, the ICO is exploring new types of regulatory approaches. For example, as you may know, the ICO is seeking to develop a public facing privacy seal scheme in the UK. A recent European Commission report explains that '[p]rivacy seals function as privacy and data protection guarantees. They inform consumers about an organisation's privacy policies, operations, practices and adherence to certain privacy and data protection standards. They notify consumers about how an organisation may collect, use or share data'[22]. The privacy seal will be awarded to organisations who can demonstrate compliance with the Data Protection Act, good privacy practice and high data protection standards that go beyond the requirements of the Act. Schemes will be operated by accredited third parties. The ICO will decide which schemes can award the ICO seal. A recent survey by our office showed that 80% of people approve of the introduction of such a symbol.

D14 What do you see as the main developments expected in the next 3 years in the collection and use of consumer data for commercial purposes? What are the likely implications of these developments?

D14.1 We foresee that the amount of data being collected will increase as the costs of storage and collection fall even further, and the range of sensors and devices capable of collecting and recording data become more prevalent.

[21] Science and Technology Committee report: Responsible use of data (November 2014).
[22] *EU privacy seals project: Inventory and analysis of privacy certification schemes* p13 <http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/>

D14.2 The government's Smart Meter Implementation Programme will see smart meters, capable of recording energy consumption at half hourly intervals, being installed in all homes in the UK. It is not entirely clear at this stage what uses developers may find for all the data generated by smart meters.

D14.3 The government has recently issued a call for evidence on data sharing and open data in banking,[23] which seeks to explore whether an individual's financial transaction data could be obtained from their bank and transferred to a third party by means of an open application programmable interface (API). We foresee that such initiatives will lead to more consumer data becoming available. It will be essential that organisations, and regulators, understand the risks arising when processing individuals' personal data in such volumes and with such variety. It is important to understand that analysis of financial transaction data to make conclusions about individuals, and then to use this data to make decisions has the potential to be unfair (or unethical), and appropriate care should be exercised."[24]

D14.4 No discussion about future developments in this area would be complete without reference to the Data Protection Regulation which is currently being debated in Europe. At the time of writing the EU institutions are yet to enter into trilogue, but there are some key themes arising from the texts. We have previously commissioned research looking at the potential impact of the Regulation[25], and have published an article-by-article analysis of the proposals.[26] Some areas that may come to fruition and have impact in this area include strengthened rights for individuals, a need for richer information to be provided in response to subject access requests, a clearer approach to consent and liabilities being placed upon data processors.

D14.5 From April 2015 the ICO will be given the power to fine organisations found to be in breach of PECR up to £500,000 without needing to prove that either "substantial damage" or "substantial distress" has been caused. The ICO has called for the removal of this threshold for some time, and we believe this will have a positive outcome on compliance in terms of nuisance marketing by phone and text message.

---

[23] Call for evidence on data sharing and open data in banking https://www.gov.uk/government/consultations/data-sharing-and-open-data-in-banking-call-for-evidence/call-for-evidence-on-data-sharing-and-open-data-in-banking accessed 19/02/2015

[24] https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1043375/ico-consultation-response-data-sharing-open-data-in-banking-20150225.pdf

[25] https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

[26] https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-regulation-analysis-paper-20130212.pdf