The Information Commissioner's (United Kingdom) comments on

Protecting consumer privacy in an era of rapid change: a proposed framework for business and policymakers

Preliminary FTC staff report

The Information Commissioner for the United Kingdom (ICUK) has responsibility for promoting and enforcing the UK Data Protection Act 1998 (DPA) and the UK Freedom of Information Act 2000. The Information Commissioner is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICUK does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The ICUK's comments on this report are primarily based on the practical experience he has gained in regulating compliance with the DPA, as well as his contributions to the ongoing debate and policy development in Europe on the future of data protection legislation and regulation.

The ICUK welcomes the opportunity to comment on the preliminary staff report on protecting privacy and commends the FTC for its thorough and thoughtful work in this area. The report is timely and complements work being done in various parts of the world to consider how to update privacy protection to make it fit for purpose and able to respond to the privacy issues and challenges associated with 21st century technology and business practices.

The ICUK intends to provide general comments on aspects of the proposed framework where he feels he can be helpful and constructive, rather than addressing each of the specific questions in turn.

General comments

The ICUK commends the FTC for setting out clear and coherent principles to underpin the proposed privacy framework. The three major elements of the proposal: transparency by business, getting the right information to individuals at the right time, and privacy by design are all key components of an effective privacy framework. The core elements of the fair information principles are also common to the EU and UK legislation and it is right that these sound principles remain and are enhanced where appropriate and necessary to protect consumers. The self-regulatory approach can be very productive, but it does not always provide adequate solutions and strong enforcement action is needed to reinforce the principles and promote best practice. It is therefore desirable that the proposed framework enables the FTC to continue its strong enforcement action, with its powers reinforced and strengthened where necessary. It is also helpful that aspects of the proposed framework are enforceable.

Scope

The FTC asks questions about excluding certain types of companies from the scope of the proposed framework and the feasibility of the framework applying to data linked to a specific consumer, computer or other device. The ICUK can see the benefit of reducing the administrative burden by excluding companies processing non-sensitive

data. However, he considers that, given the ever changing nature of business and technology, there is scope for data to become sensitive depending on the context in which it is processed. To exclude certain businesses requires decisions on what the criteria for exclusion (or inclusion) are. An inclusive approach is more future proof and an emphasis on scalability ensures that business are not unduly burdened by the requirements of the framework.

Applying the framework to data that are not just linked to a person, but to a specific computer or device is a progressive approach that recognises the reality of modern business practices regarding the collection and use of data. The ICUK considers it good practice to safeguard data which could be linked to an individual in a consistent manner, which is also easier for business than attempting to separate out data that is currently linked and that which is not but could be. The FTC will need to do further work on defining whether data is linkable, and it may find useful work done at European level on questions of identifiability and the effect on an individual resulting from the use of their data.

With regards to anonymisation, this is also a priority area for the ICUK. We are aware of emerging work at the level of ISO and in multinationals regarding technical standards. The Information Commissioner's Office (ICO) is currently working on issues relating to small-area statistics and anonymisation, including an event in March 2011. This will examine the extent to which true 'anonymisation' is still possible in an era of search engines and increased computing power and the implications of this for individual privacy.

Incorporate substantive privacy protections

The substantive protections identified by the FTC reflect existing protections in UK and EU legislation and the ICUK fully supports these. In addition, the FTC might want to consider protections relating to further transfers of data, whether at domestic or international level, as well as the concept of reasonable expectations of the individual. This concept could contribute to defining 'specific business purpose'. The ICUK supports evidence-based decision making and it is on this basis that organisations in the UK decide appropriate retention periods that are proportionate and justifiable.

The FTC asks questions about the application of the framework to legacy data systems and this is an area the ICO has experience of as companies were required to implement data protection legislation in 1984 and then transition to a new framework from 2000. In principle any new framework should apply to legacy systems. Business should not be able to avoid reasonable obligations simply by failing to update their systems. However, when the UK law changed it provided for a transitional period for existing systems, and the ICUK has recognised the need for time to make changes in his approach to enforcement.

The ICUK fully supports the FTC proposals on privacy by design. The current review of the European data protection legal framework has brought repeated calls for a more explicit requirement for a privacy by design approach to be included in the legislation and the ICUK supports this call.

Maintain comprehensive data management procedures

The ICUK considers that the combined approach of guidance, education and awareness raising with strong enforcement provides incentives for business to develop and deploy PETs. We have already seen privacy become a competitive advantage in some sectors, and increasing awareness will lead consumers to 'vote with their feet'. It is good business practice to make sure the data you hold is accurate, relevant to

your needs, and not kept longer than necessary. The protections in the framework lead to reduced costs and increased effectiveness for business. The ICUK's approach has always been to make it easier for the majority of organisations who seek to handle personal information well, and tougher for the minority who do not. Those taking their obligations and responsibilities seriously face less attention from the regulator.

Many individuals do not use the privacy choices available to them on their browser software or on other websites such a social networking sites. This might be down to the difficulty in finding and understanding them and a general lack of awareness regarding the implications of low privacy settings. Industry participants could address the misconceptions surrounding security and make it easier to change privacy settings, explaining the implications associated with the various levels of security. A general awareness of security is important as more people go online using various devices.

Simplify consumer choice: commonly accepted practices
The commonly accepted practices identified by the FTC are similar to the conditions for processing found in European and UK legislation, so it is clear that there is common ground with regard to our approaches to reducing undue burdens on business.

With regards to first-party marketing, an important consideration is the relationship the company has with the individual and their reasonable expectations of what will be done with their personal information. Even where a consumer has a direct relationship with a company, giving them opportunities to decline further marketing is a way of putting them more in control of the use of their information and ensures companies don't waste resources on those who won't respond.

The nature and content of online first-party advertising is determined by the previous behaviour of the user on that website, for example, what they have bought or browsed during past visits to the website. Any advertising placed on the website by an affiliate (a member of the same advertising network) is third-party advertising. Therefore, the ICUK considers that marketing by commonly-branded affiliates should not be considered first-party advertising.

The FTC asks questions about data enhancement and the ICUK considers transparency to be key here. Consumers are likely to expect choices where the outcome of the enhancement may have an adverse or detrimental affect on them, or where the sources of the data are unexpected.

Practices that require meaningful choice
Consent is a difficult area and one that the European Commission is seeking to clarify with regards to the future EU data protection legal framework. The ICUK believes that consent should be sought in circumstances where a consumer has received a proper explanation of the consequences of their actions and are genuinely free to exercise choice. Experience shows that consent is being used in contexts where it is inappropriate, because the processing needs to happen regardless of the individual's wishes; this can amount to an indemnification exercise for companies and can also be deceptive for consumers. There is a risk of confusing consent and transparency: telling someone about something and gaining their agreement to it are quite different. There are also issues of withdrawal of consent, and how this is respected and dealt with by business.

The ICUK considers that methods of consent should be appropriate to the context and consideration should be given to what consumers want: do they want separate 'informational' choices or consent to be implied from their relevant actions? The online and mobile worlds also open up great possibilities for the exercise of complex information choices and consumer control. It allows better means of explaining information systems and can make privacy an activity. We should embrace the positive aspects of the online world.

With regards to the mobile context, mobile advertising is a growth area that will continue to expand in the coming years. Mobile customers represent a huge target market for advertisers, mainly due to the popularity of the smartphone. This raises issues over gaining consumer consent and online security. In principle, using uniform icons or graphics appears to be a good idea. If a consumer understands the meaning of an icon they would understand what they are consenting to and could quickly accept, or refuse, terms and conditions. However, this would mean universal terms and conditions which may not be practical for all websites and platforms.

The FTC questions whether the 'take it or leave it' approach could ever be inappropriate, and the ICUK considers that it would be in circumstances where the consumer has no real alternative but to use the service offered.

Special choice for online behavioural advertising: do not track

With regard to a universal choice mechanism, perhaps more could be done with privacy settings to make them truly reflect what consumers want to do. However, there may be a significant knowledge gap in the public's understanding of how behavioural advertising works. Perhaps if this were tackled it might promote a more privacy conscious online user and help remove some misconceptions about behavioural advertising. A granular approach would perhaps be more privacy friendly and promote good practice, however, consumers may not accept levels of granularity that cause them to spend significant time and effort to understand and change settings.

The FTC questions whether legislation would be the solution to business not implementing an effective universal choice mechanism voluntarily. The ICUK considers that legislation could help, but that other options, such as codes of practice, should also be explored.

Increased transparency and improved privacy practices

The US and EU have had the same experiences with privacy notices: they have become legalistic and meaningless to individuals, who frequently don't read them anyway. The EU has looked at standardised privacy notices in the past, as has the Centre for Information Policy Leadership in the US. Both concluded that while there may be areas where wording can be standardised, it is better to focus on consistency for what should be included. There may be scope for standardising what should be included, but the notice needs to be specific to the business and the context and this is not always achievable through a standard notice. Privacy notices should be clear about what happens to the consumer's personal information, what choices they have, and how to exercise those choices. The information needs to be meaningful, easy to understand and presented to the consumer at the appropriate time. Standardising what should be included (particularly across a specific sector), such as headings, would allow consumers to easily compare policies across companies.

Reasonable access to consumer data
In the UK the maximum charge for access to personal information is £10 (~ $15) and most companies charge this amount. Credit reference agencies work differently and access costs £2 (~ $3). Some businesses choose to provide access for free. The ICUK's experience is that imposing this charge does not cause undue difficulties for most consumers, but it is important that the charge is reasonable and he would not, for example, support an increase in the current UK charges. Other EU countries have a system where the first access request is free, and any subsequent access request is charged for. Some countries allow one free access request per year. The ICUK does not believe that any fee should be seen as a means of cost recovery by business; rather it should be a disincentive to trivial or repeated requests.

The ICUK considers transparency to be important also in the context of accessing information. Companies should give consumers information about where they have received data from and who they have shared it with. This facilitates greater transparency and gives individuals more of a sense of control over the use of their own information. This is particularly important where individuals are denied benefits and services as a result of data about them held or obtained by the company. Individuals should be able to challenge inaccurate data or provide more information to a company to enable well-informed decision making.

Material changes
The concept of companies making material changes to their policies and practices is similar to the EU concept of purpose limitation. The ICUK considers it important that consumers are informed and given choices, where necessary and appropriate, when the use of their personal information changes in a way that has a significant effect on them or is beyond their reasonable expectations. Positive consent will generally be required where a significant change in the use of personal information is proposed. This is on the basis that there is in effect a contract whereby the consumer parts with their personal information based on assurances given by the business about use and disclosure. A significant variation in this 'contract' requires the consumer's consent.

Consumer education
The proposal to put consumer education responsibilities and obligations on companies is a progressive idea and links very clearly to the desired outcomes of greater transparency and informed choice. Organisations are well placed to provide a better explanation to their customers of what they do with their personal information, why and when, at the point of first interaction with that customer. Industry associations, consumer groups and government can also help and how they do this will depend on the audience.

The ICUK is currently considering what role his office can play to better educate individuals and raise awareness. As well as providing extensive guidance tailored to both organisations and individuals, one idea is to involve the education sector and provide privacy education through the curriculum tailored to the audience and the contexts in which they need awareness. So, for example, rather than teaching children about privacy as a concept in itself, integrate the main principles and safeguards into lessons that teach them how to use the internet for school research and homework. Consumer groups and industry associations could take a similar approach with adults. As far as educating business is concerned, Government and the FTC in particular could contribute to education and awareness raising through guidance, business checklists, expert seminars and workshops, providing a helpline, or by recognising best practice, such as through awards or other mechanisms.

Conclusion

The preliminary staff report is a very positive step and the FTC is to be commended for its thoroughness in exploring all the issues with all the relevant stakeholders. The ICUK is looking forward to seeing the further work that will follow this report and the development of the proposed privacy framework. It is encouraging to see that different privacy regimes around the world are coming together in their thinking, and it is clear that the core principles and elements are the same. There are ideas in the FTC report that will contribute positively to the work that is underway to update and better implement the data protection legislative framework. It is important that we learn from each other, and that we strengthen and bring together the different privacy standards that exist to achieve the same outcome: better standards and practice from business, and better protection for individuals.