Privacy notices — clarity and effectiveness

Olivia Whitcroft, Principal of OBEP, gives some solutions regarding how to present uses of personal data in a privacy notice in a clear and readable way

We frequently see the phrase 'Please tick here to confirm you have read and agree to our privacy policy' when registering on websites, filling in forms, installing software and logging into apps. But how many of us can honestly say we always click through to the privacy policy and read the terms? Do we all need a lawyer on hand to help us to understand the complex provisions? Should an organisation be able to do whatever is written in its policy merely because we had the opportunity to read it and were forced to accept it?

In relation to the first question, surveys undertaken over the last couple of years, including by the UK Information Commissioner's Office, ('ICO'), consistently report that the majority of individuals do not read privacy notices. We probably could have guessed this anyway.

On the second, lawyers should not be needed to help interpret terms and notices governing the use of our data, yet many are drafted in such a complex way that we would be forgiven for thinking that they are. A recent report by the UK House of Commons (discussed further below) likened reading terms of use to 'engaging with Shakespeare' and considered that a lot are drafted 'for use in American court rooms'.

Finally, whilst a lot of organisations believe they are entitled to do whatever is written in a privacy notice, unfortunately this is often not the case. In addition to ensuring clarity in the notices themselves, the proposed processing needs to be assessed against all the other data protection rules before determining whether or not to proceed.

Having said all this, elements of good practice in privacy notices and terms are emerging. These seek to address the practical as well as legal hurdles in providing clear information on data use, and encourage individuals to read privacy notices. This article recaps on the basics of privacy notices and discusses some recent developments.

Why we have privacy notices

In the UK, it is a legal requirement under the Data Protection Act 1998 ('DPA') for data controllers to provide 'fair processing information' which informs individuals of:

- the identity of the data controller;
- the purposes for which data are intended to be processed; and
- (the rather more vague requirement) 'any further information which is necessary…to enable processing… to be fair'.

This forms part of wider data protection goals (in many jurisdictions worldwide) associated with transparency of data processing and enabling individuals to understand how their data are used.

The primary purpose of a privacy notice (or 'privacy policy' or 'data protection notice') is therefore for an organisation clearly to inform individuals how their personal data are being used in relation to the relevant website, app, forum or other activity.

For standard and unobtrusive uses of data (for example collecting a name and address to deliver a package), this may involve a short statement at the bottom of a form outlining who the organisation is and how to contact them, briefly what the details are used for, and confirming the data will not be disclosed to any other parties. For less obvious or more intrusive uses of data (for example data analytics, behavioural monitoring, direct marketing and data sharing), an organisation may need to provide more detailed information about the relevant activities.

Information within privacy notices or other notifications may also be part of a mechanism to obtain consent to a data processing activity. (In the UK, consent is condition 1 of the legitimising conditions in Schedule 2 of the DPA). However, as highlighted in the next section, the mechanism needs to be thought through in the context of the specific processing activity, such that the individual understands the choices they have and to what they are consenting.

With all this in mind, a privacy notice must be clear and understandable for the reader or it does not achieve its main purpose. Cultural and

(Continued on page 4)

Olivia Whitcroft leads the session 'Social Media — Legal Risks and How to Address Them', with courses dates in London, Glasgow and Manchester.

See the website www.pdptraining.com for further details.

(Continued from page 3)

technological advances have enabled multiple and complex uses of data, meaning that organisations often struggle to explain and present what is happening in a clear and readable way. Some ideas to assist with these difficulties are discussed below.

What a privacy notice does not do

There is a common misconception amongst organisations that a privacy notice acts as a mechanism to enable them to use an individual's data. In other words, if they write what they want to do with personal data in a privacy notice, this then allows them to do just that. Linked to this, if they have included a little box that an individual is obliged to tick, the individual has consented to such use, so cannot object to it going forward.

This is not the case. Unfair or unlawful processing does not become fair and lawful simply because it is documented within a privacy notice. Before a privacy notice is written, an organisation needs to perform a separate assessment on whether the proposed use of data is fair, lawful, relevant, not excessive, and so on, in accordance with all the rules of data protection. Once this has been done, the privacy notice then seeks to inform individuals how data are being used in accordance with such rules.

"Unfair or unlawful processing does not become fair and lawful simply because it is documented within a privacy notice. Before a privacy notice is written, an organisation needs to perform a separate assessment on whether the proposed use of data is fair, lawful, relevant, not excessive, and so on, in accordance with all the rules of data protection."

Similarly, including a little tick-box next to a link to a lengthy privacy policy is unlikely to be an appropriate way to gain an individual's consent to specific uses of data. Consent is not always required, but where it is (for example, for many marketing, monitoring and data sharing activities), an organisation must demonstrate that it is specific, informed and freely given. This usually involves a separate mechanism focussed on the specific processing which requires consent.

To summarise: a privacy notice is one element of compliance and good practice in the use of personal data, but does not allow an organisation to ignore all the other elements.

Addressing the difficulties: 'layered' notices and 'just-in-time' notifications

Transparency of data processing can be improved by providing fair processing information to individuals in more manageable chunks and at more effective times. To this end, common approaches include 'layered' notices and 'just-in-time' notifications.

The layered approach to privacy notices is often used where an organisation has multiple and potentially complex uses for an individual's personal data, and is recommended in the ICO's Privacy Notices Code of Practice (published in 2010, copy available at www.pdpjournals.com/88381).

Using this approach, at the time of data collection, a short and prominent notice is displayed to individuals. This is easy to see and read, and therefore likely to be actually read and understood. It can be displayed, for example, on a smartphone's screen, at the bottom of a form or at the top of a website privacy notice. This short notice outlines key information such as the identity of the data controller and the main purposes of data use, and flags any unusual or intrusive uses of data which require the individual's particular attention. It can then link to, or be followed by, a longer privacy notice, providing more detail for those that want to read more. There may then be further cross-references to additional sources of information, if required.

Short, focussed statements about specific uses of data (such as marketing, monitoring or data sharing) may also assist in obtaining clear informed consents for those specific processing activities.

The use of instantly-recognisable icons representing particular types of data use or sharing activities could make the short notices even shorter. Looking forward, this could be an extremely effective approach if icons could be made consistent within the UK, EU or even internationally.

A just-in-time notification is a notice of data use that appears at the time it becomes relevant, for example when a user activates a certain feature of an app, or at the time an organisation starts to use data in a particular way. This can act as a timely reminder, rather than relying on the user having read or remembered everything they may have been told at the beginning of their relationship with the data controller, for example when they first downloaded an app or completed a form. Again, the just-in-time notification can cross-refer or link to a longer privacy notice providing more detail as required.

Related to this, organisations may wish to ensure privacy notices are always available for individuals as a point of reference throughout the period for which data are being processed, and to make it clear how users can access data, and change any applicable options or consents.

This may include, for example, online portals through which information and profiles can be accessed.

Hot topics: mobile apps, Big Data and social media

Mobile apps, big data and social media continue to be hot topics presenting challenges for the presentation and content of privacy notices. Some recent developments in these areas are summarised under the headings below.

ICO guidance

In December 2013, the UK regulator published guidance on 'Privacy in mobile apps' (copy available at: www.pdpjournals.com/88382), which includes guidance on privacy notices, and cross-refers to recommendations for a layered approach within the ICO's privacy notices Code of Practice (referred to above). It also highlights that just-in-time notifications can be particularly useful for use of intrusive data such as GPS location. (See also the article 'Apps and privacy: App-lying the rules and App-easing the Users' in Volume 14, Issue 3 of *Privacy & Data Protection)*.

In July 2014, the ICO published guidance on 'Big Data and data protection' (copy available at www.pdpjournals.com/88383). This highlights that the complexity of Big Data analytics can mean that data processing appears opaque to individuals. It may be particularly unclear what data are being used by an organisation, how data are being used and how decisions are being made. This, in turn, can lead to a lack of trust and engagement with the organisation.

Whilst the culture of social media involves individuals providing more and more information about themselves within different forums, this does not necessarily mean that they are unconcerned about how these data are then used. On a similar note, as highlighted above, people often do not read privacy notices because they are too long or complex, not because they do not care. Organisations therefore need to promote transparency at an early stage and work on innovative ways to communicate clearly and concisely the purposes of data use, even if the complex analytical algorithms themselves are not explained. By way of example, the ICO guidance refers to Channel 4's use of a YouTube video accompanying its privacy notice. It may also be helpful to tell people when their personal data are not used, for example if data are anonymised for analysis.

GPEN privacy sweep

In May 2014, the Global Privacy Enforcement Network (of which the UK ICO is a member) examined over 1,200 mobile apps worldwide, including 50 top apps from UK developers.

The results were published in September 2014. The statistics back up the problems with existing privacy notices raised above. Of the apps surveyed, 85% failed to clearly explain how they were collecting, using and disclosing personal information. 43% failed to tailor privacy communications to a small mobile screen, and 30% provided no privacy information at all.

Key concerns included that too little information was available prior to the download of an app, and that it was unclear who was the data controller. Information was often provided via links to webpages with lengthy privacy policies which were difficult to access and read, and some of which required the user to log in to view the policy. Some links did not work at all.

However, elements of good practice were also identified, and 15% of apps reviewed were considered to explain clearly how the app collects, uses and discloses personal data. This was achieved through the use of pop-ups, the layered approach and just-in-time notifications. They also clearly articulated what the app did not do with information, and some apps provided links to other policies of their advertising partners.

House of Commons report: responsible use of data

On the 19th November 2014, the House of Commons Science and Technology Committee published a report entitled 'responsible use of data' (copy available at: www.pdpjournals.com/88384). This focuses on social media and Big Data analytics and, following industry inquiries, considers both benefits and hurdles in use of personal data in the UK and provides recommendations to government.

The report once again highlights that terms and conditions outlining the use of data are frequently too long and complex, and, in addition, are not fit for purpose as a mechanism for obtaining informed consent. The Committee considers it vital that companies effectively communicate how they intend to use personal data, and recommends that the government drives the development of information standards under which organisations (including government bodies) commit to explain use of data to customers in 'clear, concise and simple terms'. Further, the Committee requests proposals for how the standards will be assessed and audited.

The report also indicates that the government is working towards an internationally recognised kitemark for demonstrating documents dealing with use of data have met a high standard. This is a similar concept to the 'Crystal Mark', which is a seal of approval from the Plain English Campaign on the clarity of documents. This has existed for a number of years, and, whilst not relating specifically to data protection matters, may already be used to demonstrate clarity of privacy notices and associated terms.

The big players

Big players such Google and Facebook regularly come under scrutiny for their data processing activities. The media and regulators across the European Union are quick to pick up on potential flaws in the transparency of privacy notices and

(Continued on page 6)

(Continued from page 5)

the data processing activities they describe.

In 2012, Google published a new privacy policy which consolidated privacy notices across many of its products and services. In theory, the privacy policy itself was a lot simpler to read and understand, as a user could refer to one consistent notice rather than 60 differing notices. However, this led to reservations over what Google purported to do within the privacy notice, which was to combine the data collected from across all the different services. There were concerns that the extent of data sharing and the justification for doing so were unclear.

As raised above, as well as questions over the clarity of a privacy notice itself, data processing activities proposed within the notice may also be open to challenge. Indeed, regulators in several European countries (including the ICO in the UK) have challenged Google's use of data based on this policy, which has resulted in actual or threatened fines in several countries.

Google has made several changes to its privacy policy since then. However, on 15th December 2014, it was announced that the Dutch data protection authority intended to issue a new fine of 15 million euros if Google failed to make further changes to its policy to clarify how data are used by the different services, and to obtain effective consent for certain data sharing activities.

In November 2014, Facebook published an updated version of its data policy which is to take effect on 1st January 2015. This has a completely new look, including new colourful icons and summaries for key issues such as types of data collected, purpose and data sharing, and a layered structure for obtaining further detail. It also includes a 'Privacy Basics' tutorial and tools to demonstrate how different features (such as targeted ads) work, and for users to understand and update options within their profiles.

A notice now appears at the top of the screen which introduces the changes, informing users that by using the services after 1st January 2015, they are consenting to the updated policy and (as is specifically highlighted) seeing 'improved ads based on apps and sites you use'.

It will be interesting to see the public's and regulators' reaction to these changes, including the improved clarity of notices, terms and options, and whether legal justifications and consent mechanisms are sufficient for proposed uses of data such as behavioural advertising.

Draft EU Data Protection Regulation

The proposed EU Data Protection Regulation has been in the pipeline for almost three years, and the latest indications are that we may have the final text during 2015. The Regulation is likely to extend the scope of 'fair processing information' (referred to above in relation to the DPA) which data controllers must provide to individuals, and therefore will also have an impact on the associated privacy notices.

As well as the identity of the data controller and the purposes of processing, organisations may be required to communicate the period for which personal data will be stored, rights of access, rectification and erasure, the right to lodge a complaint to the regulator, recipients of disclosures of data, details of international data transfers, whether provision of information is obligatory or voluntary, and the consequences of failing to provide requested information.

These are not dissimilar to the type of information already expected within privacy notices (even if not explicitly listed in the DPA). However, the proposed changes mean that the minimum information required by law is likely to increase, creating further challenges in communicating it concisely and clearly.

A clear message

The message is clear: rather than forcing individuals to 'accept' ten page privacy notices containing complex and confusing legalese, organisations need to work on effective ways of communicating how they intend to use data. With ever-increasing volumes and complexity of data processing activities, more innovative methods are needed, and we may see further development of regulator and government-led standards and guidance to assist with this.

Aside from legal compliance, privacy notices can be used as an opportunity to engage with customers and users in a creative way. They can empower individuals to understand what the organisation is doing, clarify where there are genuine options and choices, and build up overall trust and engagement.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.co.uk