Facebook's privacy policy--sea change or business as usual

08/06/2015

IP&IT analysis: What can we expect from Facebook's data protection policy in the future, and what impact might pan-European regulation have in this area? Stephanie Pritchett, a specialist data protection lawyer and principal at Pritchetts Law, considers a new report from the Belgian Data Protection Authority regarding Facebook tracking and the use of social plug-ins.

Original News

Facebook only accepts supervision by the Irish Office of the Data Protection Commissioner (ODPC) and the application of Irish law and has resisted attempts to be bound by the national privacy legislation of Belgium, the Netherlands and Germany, a report by the Belgian Privacy Commission (BPC), also known as the Belgian Data Protection Authority (BDPA) has found. A detailed study commissioned by the BPC examined the ways in which Facebook processes the personal data of its members, as well as of all internet users who come into contact with Facebook.

What is the background to this report, and what are the findings?

Towards the end of 2014, Facebook announced its intention to redraft its data use policy (DUP) and terms of service, with plans to launch a new version from 30 January 2015. A European Task Force, led by data protection regulators in the Netherlands, Belgium and Germany was then formed to analyse these new policies and terms.

On 13 May 2015, a recommendation was published by the BDPA in relation to various issues, including the use of social plug-ins by Facebook.

Among other matters, the BDPA states that:

- Facebook uses social plug-ins, such as its well-known 'Like' button, to track user's internet browsing patterns and activities
- it is hard for users to stop this happening as they are expected to navigate Facebook's complex web of settings in search of possible opt-outs

Collecting and storing data

The BDPA had previously stated that 'Facebook tramples on European and Belgian privacy laws' and have expressed their view in the Recommendation that if Facebook is to continue tracking user internet activities It should not routinely collect and store information about all websites that individuals visit which contain social plug-ins--especially where individuals have not even interacted with the social plug-ins on those websites.

It should also not collect information on those individuals who are not registered Facebook users and those individuals who have either deactivated their Facebook account or logged out of it--without getting explicit opt-in consent beforehand.

Research commissioned by the BDPA found that the 'Like' button had been placed on more than 13 million websites, including government and health websites. Tracking cookies associated with those plug-ins would then send detailed information back to Facebook.

It also found that Facebook has for a long time been tracking website users who visit any website page owned by Facebook.com--including fan pages, profile pages and other parts of the Facebook site which you can visit without being a registered user.

Transparency

Facebook should be very clear and transparent about the use that they do make of tracking cookies and social plug-ins via more prominent Facebook privacy and cookie policies.

Obtaining prior consent

In relation to active registered Facebook users, Facebook should obtain the specific informed and unambiguous consent of those users before dropping or obtaining the cookies--including those via social plug-ins--to collect or use information about that user, particularly where the intended use is marketing or distribution of adverts using behavioural advertising methods.

It is the view of the BDPA that the current measures used by Facebook are not sufficient to obtain the prior explicit consent which must be obtained by Facebook before dropping a cookie or performing tracking, unless it is necessary:

- for either the networking required to connect to the service, or
- to provide a service specifically requested by the user

Neither applies to tracking for marketing and adverts.

Extra compliance measures

It should be recognised by Facebook that extra compliance measures should be in place owing to the fact that they are in a unique position compared to most other organisations that carry out third party website tracking. This is because Facebook has the ability to match up user website browsing habits to the real identity of those individuals, as well as to their social network interactions and sensitive personal data--including medical information, religious, sexual and political preferences.

The BDPA also states in its Recommendation that website owners and hosts using Facebook's social plug-ins should:

- make sure that social network 'like' buttons are only activated once consent has been obtained by the user of that page
- consider the use of SocialSharePrivacy which is a jQuery Plugin that allows buttons of social networks to be added to websites in a privacy-friendly way by ensuring that buttons are inactivated and that no data is transferred to or from third party websites until after the user has clicked on the social plug-in button
- ensure they implement a two-stage click-through process so that any website users who do not want to interact with Facebook are not required to do so

It was also recommended that individual users should use privacy-enhancing software like Privacy Badger, Ghostery or Disconnect to help block the invisible sites that track their search and browsing history.

What role does the ODPC have?

Facebook Ireland Ltd is understood to be the organisation responsible for most of the Facebook group's activities with consumers outside of North America and Canada.

Facebook has responded to the Recommendation stating that: ... 'there is nothing more important to us than the privacy of our users and we work hard to make sure people have control over what they share and with whom. Facebook is already regulated in Europe and complies with European data protection law, so the applicability of the Belgian Privacy Protection Commission's efforts are unclear. But we will of course review the recommendations when we receive them with our European regulator, the Irish Data Protection Commissioner'.

As yet, the ODPC has declined to comment.

Some European member states have previously accused Ireland of being too soft on the multinational firms headquartered there, especially major US technology companies such as LinkedIn, Apple and Facebook.

The BDPA's investigation is of particular interest not only to Facebook, but to any non-EU headquartered organisations that process personal data within the EU. This is because the conclusions drawn in the Recommendation are that Facebook should be considered subject to Belgian Data Protection laws, and not simply those of Ireland, as Facebook has continued to maintain.

The issue of appropriate applicable law is an evolving one, as multinational corporations with many subsidiaries in a variety of member states have been accused of simply nominating one such entity as its EU data controller, much to the chagrin of data protection authorities and privacy rights activists. This approach has been informed by Council Directive 95/46/EC, art 4 which sets out a twofold test as to which data protection laws apply to a particular organisation:

First, there is the 'establishment test', which in very broad terms suggests that if data is processed by an organisation in the context of the activities of a subsidiary or branch office in a particular EU member state, only the laws of that EU member state will apply, even if data has been collected from people in other member states.

Second, the 'equipment test' looks at where an organisation's data processing and controlling kit is located. If an organisation uses equipment to process data in a number of member states, the laws of those member states will apply.

Facebook are continuing to seek reliance on the 'establishment test' only and arguing that only the Irish regulator has power to investigate.

The BDPA wasn't impressed with this approach. Having examined this issue in considerable detail, its view in the Recommendation is that Facebook Ireland Ltd is not the data controller in the EU, as it simply is not capable of taking sufficiently independent decisions on the processing of data of Belgian and other EU citizens.

In support of this assertion, the BDPA states that the new Facebook DUP has been implemented globally but with no amendments implemented by Facebook Ireland Ltd for its EU users. The BDPA believes that the lack of controls put in place by Facebook Ireland Ltd and the lack of challenge to a global DUP means that Facebook Inc, the US parent, is the sole data controller.

Applying the twofold test, Facebook had an 'establishment' in Belgium that was inextricably linked to Facebook Inc in the US--this is argued by the BDPA applying the tests met in the European Court of Justice's relatively recent 'Right to be Forgotten' judgment, *Google Spain SL and another company v Agencia Espanola de proteccion de Datos (AEPD) and another* C-131/12, [2014] All ER (D) 124 (May). If that approach is not accepted, then the BDPA also argues that Facebook Inc has the necessary 'equipment' in Belgium to meet the equipment test due to its use of cookies and other tracking technologies dropped on devices owned by Belgian citizens.

These approaches seem to have been confirmed in wider case law across Europe--including a previous German case which found that Ireland were not the only EU regulator for Facebook Ireland Ltd.

The BDPA therefore concluded in its recommendation that Belgian law should apply.

While a number of other European watchdogs have also continued to investigate Facebook's practices, the BDPA believes, for the reasons set out above, that it has the power to investigate Facebook's potential data protection breaches. While the BDPA may not currently have the power to fine Facebook, it could instigate legal proceedings against them. The BDPA has not been shy in saying that it will do so.

Clearly, a key message for international businesses to draw out of this Recommendation is that if they are seeking to rely on the 'establishment' test by nominating a subsidiary in an EU member state, this cannot merely be a paper based exercise. It must be able to demonstrate that the nominated entity is capable of being the EU data controller--under what is likely to be increasing scrutiny.

How kindly will the Irish take the views of the Belgian authorities?

The ODPC carried out an internationally high profile audit of Facebook Ireland Ltd and published its initial audit results in December 2011 and its follow up audit results in September 2012. As part of the extensive audit exercise carried out by the ODPC, it examined Facebook's facial recognition technology for 'tagging' individuals, its use of social plug-ins, its 'Friends Finder' application, the third party applications operating on Facebook's platform and targeted advertising by Facebook. The ODPC expressed numerous privacy concerns and recommendations for improvement in relation to all of these Facebook features. The ODPC's audit reports, totalling over 300 pages, have been published on the ODPC website for all to examine.

It is worth noting that the ODPC stated in its follow up audit report in September 2012 that most of its initial recommendations had been implemented by Facebook Ireland Ltd to the satisfaction of the ODPC. It's possible to speculate, therefore, that the recent findings of the Belgian authorities may engender the following reactions:

- slight embarrassment on the part of the ODPC that another EU regulator has categorically stated that Facebook Ireland Ltd is non-compliant with EU law
- some reticence perhaps and a lack of available resources to re-open the investigation so soon (rather like

Father Ted's Eurovision entry, it might be time for 'someone else to have a go')

- a slight nervousness perhaps from the Irish Government that high profile multinational tech companies may be deterred ever-so-slightly from establishing major EU hubs in Ireland

Time will tell.

Either way, change is afoot in Ireland, the ODPC's Annual Report back in 2011 stated the following:

'The implications of our increased European responsibilities were brought home to us forcefully in relation to our audit of the activities of Facebook Ireland. Facebook Ireland had unambiguously placed itself under our Office's jurisdiction through changes in its contractual arrangements with its EU users and the establishment of clear responsibility for the processing of their data. We therefore included them in our programme of audits for 2011. This was the most complex audit ever undertaken by our Office, involving about a quarter of our staff resources for three months and external technical assistance from University College Dublin (UCD) We clearly cannot maintain a similar level of commitment in relation to other multinational companies without additional resources. I am confident that this message is understood by the government and would hope to be allocated additional resources in the course of this year.'

Despite the hopes of the then Data Protection Commissioner, Billy Hawkes, back in 2011, it was not until January of this year that the newly appointed Irish Commissioner, Helen Dixon, announced additional resources had been confirmed to her office--an effective doubling of the budget of the Office from EUR 1.89m in 2014 to EUR 3.65m. By way of comparison, for 2015/16 the Information Commissioner's Office (ICO) is due to receive grant in aid of £3.7m--a reduction of £50k on last year's initial budget.

The significant extra resources secured for the data protection regulator for 2015 will allow for the recruitment of additional expert staff to ensure that Ireland continues to administer a first-rate regulatory and enforcement regime for data protection. Technology audit experts were recruited by the ODPC in May 2015.

With increased budget and increased numbers of specialist ODPC staff, there is no doubt that compliance enforcement and scrutiny is going to get tougher in Ireland very soon. As an advisor working on cross border issues, I do, however, question how seriously organisations will really begin to take data protection compliance in Ireland until the Irish implement a civil monetary penalty fining regime (akin to the £500K fines issued by the UK regulator).

Is there much in the way of cooperation between national authorities or do they still have materially divergent approaches to these sorts of issues?

There is still a fair degree of co-operation and sharing of intelligence among data protection regulators. For example, the Irish regulator's reports build on work already carried out by the American, Canadian and German data protection regulators, though there is no formal vehicle for cross jurisdictional investigation and enforcement.

The results of the recent BDPA findings, would, however, suggest that the regulators do take divergent approaches at times. It is worth remembering that all Member States have implemented the European Directives in subtly different ways, and so inevitably the Belgian regulator's interpretation will be driven by this at a national level.

Will the new Data Protection Regulation have an impact on Facebook in this area?

Yes, it's very likely it will because the current European Directives take horizontal effect--that is, they need to be implemented by domestic law in each EU member state. While they are implemented in a broadly similar way, there are some key differences. This has made it difficult for multi-nationals operating across Europe to know whose rules it is playing by.

It can be reasonably anticipated that the proposed new EU Data Protection Regulation, which will have direct effect without needing separate member state implementation, will make it easier for multi-nationals operating across Europe to play by one set of rules. Having said that, it looks likely there may still be a little scope in the new Regulation for some domestic idiosyncrasies, so it is unlikely to produce an entirely level playing field. Whatever way you cut it, the rules will also become more difficult and a lot more expensive to comply with in practice.

The issue of which national regulator will have authority over pan-European businesses is still far from clear. The 'one stop shop' mechanism proposed under the new Regulation has been one of its most controversial elements and has, in

part, contributed to the delay in reaching agreement on the draft legislation. The initial idea was to provide more transparency and certainty to organisations about who their 'lead' authority would be. Various rounds of negotiations have led to this certainty all but disappearing. The most recent draft proposed by the Council of the EU retains the lead protection idea but contains extremely difficult rules around when other concerned data protection regulators may be able to intervene and challenge--perhaps leading to all the same problems that we are seeing now around applicable law with this Facebook case study.

It looks likely there will be a move to explicit opt-in consent for all forms of processing, including for marketing purposes. At the moment, the Irish have a similar slightly softer approach to implied soft opt-in consents as we do in the UK. It would then become imperative to seek clear opt-in consents for all processing by Facebook.

It is currently proposed that fines of up to 5% of an organisation's annual worldwide turnover or EUR 100m will be applied for non-compliance with the Regulation.

This will be a massive sea change.

In EU member states like Ireland and Belgium, who at the date of writing have no such fine structure in place (although Belgium looks likely to receive this enforcement power soon) and for multi-national organisations, who will not be able to avoid large fines by setting up operations in a country that does not have this enforcement power.

Whatever happens with the proposed new Regulation, one can rest assured that Facebook will have been keeping an extremely close eye on the development of it. Some critics say that despite years of lobbying, the new Regulation will be out of date as soon as it goes to print--particularly given the march of technology and the creative way that technological change is harnessed by the likes of Facebook.

It will, of course, be fascinating to see how Facebook responds to some of the challenges that the proposed new Regulation will present and also to see how the various EU regulators will dance around these high tech companies--perhaps reminding them, as now, of the necessity to comply with the 'spirit and intent' of the new Regulation as technology moves apace.

Stephanie is a senior solicitor and principal of the specialist data protection and privacy law firm Pritchetts Law.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.