Large multi-national firms relocate user data to Ireland

Twitter recently announced that its Dublin-based entity Twitter International Company would take over all services for non-US users. With effect from 18 May, all non-US user data has been moved to servers in Ireland and Twitter International Company is the contracting party with all such users. Ireland is now the European headquarters for a significant number of large multi-national digital companies, including Microsoft, Facebook, LinkedIn and Google. Paul Lavery, Partner at McCann FitzGerald, considers the possible reasons why large digital companies have made such changes to their data storage arrangements, the potential benefits of storing non-US data in Ireland and the legal implications of such a move.

There has been much conjecture about the reasons for relocating non-US data to Ireland. According to such conjecture:

- Twitter may have decided to move its data to a secure location which is subject to European data protection laws. Depending on the outcome of the *Microsoft* case in New York, this will mean that access by US authorities to such data will be more constrained; and
- Twitter may have taken into consideration the on-going review of the adequacy of the Safe Harbor regime and the potential that the regime, in its present form, may not survive such review. If Safe Harbor were to be suspended or terminated, it could have significant implications for companies dealing with EU nationals who store data relating to such nationals in the United States.

Twitter, like other digital companies, has not confirmed the reasons for relocating non-US user data to Ireland. Data protection and privacy considerations are not necessarily the main reasons why Twitter would decide to move non-US user data to Ireland. By rearranging its business so that its Irish company, Twitter International Company, took over all non-US services, there should be a significant ramping up of Twitter's staffing and operations in Ireland. Ireland has a history of attracting multi-national corporations to its shores for a number of reasons, including a low corporation tax rate, an educated English-speaking work force, easy access to other markets within the European Union and a developed legal system which has clear laws in relation to the digital economy and the protection of intellectual property rights.

Storing data in Ireland - access to data by US and other authorities?

As the US Twitter entity will no longer be the contracting party with non-US users and will not retain responsibility for dealings with such users or their data, US law will not govern the processing of this personal data. Instead, Irish law will govern matters and access sought by US and other foreign authorities should be subject to Irish law restrictions. This should ensure that the data is protected from disclosure unless the proper legal procedures in Ireland for seeking access to the data are followed.

Where foreign law enforcement agencies or courts seek access to data stored in Ireland, the only legal basis for disclosure may be through the mutual assistance regime. The Irish Criminal Justice (Mutual Assistance) Act 2008 (the 'MAA') provides for various forms of mutual legal assistance to foreign law enforcement agencies and courts.

The MAA gives effect to international agreements and instruments that provide for mutual legal assistance, including the 2003 Agreement on Mutual Legal Assistance between the European Union and the US and the related bilateral instrument to give effect to the Treaty on Mutual Assistance in Criminal Matters between Ireland and the US. Requests can be made in accordance with the following process:

- Requests for mutual legal assistance may be made by courts, tribunals and other authorities which have the power under their national law to make requests for mutual assistance.
- The Central Authority for Mutual Assistance at the Irish Department of Justice, Equality and Law Reform is responsible for receiving and dealing with requests for mutual assistance.
- If the Central Authority is satisfied that the request relates to an offence that has dual criminality, and the relevant provisions of the MAA apply, it will send the request to An Garda Síochána (the Irish Police Force) for consideration.
- A member of An Garda Síochána not below the rank of Inspector will apply to a Judge of the Irish District Court for a search warrant or order.

The *Microsoft* case

The above is, however, subject to the outcome of the on-going *Microsoft* case in New York. In December 2013, Judge Francis of the United States District Court issued a warrant for the search and seizure of information associated with a specified web-based email account that is 'stored at premises owned, maintained, controlled, or operated by Microsoft

Corporation, a company headquartered at One Microsoft Way, Redmond, WA.'

The information which was the subject of the warrant is stored on servers owned and operated by Microsoft Ireland Operations Limited. Microsoft sought to quash the warrant on the basis that it directed the production of information stored in Dublin, and that courts in the United States are not authorised to issue warrants for extraterritorial search and seizure. Microsoft's motion was denied by Judge Francis in a judgment of 25 April 2014. In order for the case to continue to the New York Second Circuit Court of Appeals on 5 September 2014 Microsoft declined to comply with the court's ruling, voluntarily entering into contempt, with any sanctions deferred pending the final outcome of the case.

Microsoft Ireland hosts the relevant data in its Dublin data centre. To the extent that information that is the subject of the search warrant contains personal data, Microsoft Ireland's processing of that personal data is subject to Irish data protection law. Compliance with the search warrant (without following the mutual legal assistance route) would place Microsoft Ireland in breach of Irish data protection law.

Numerous *amicus* briefs have been filed in support of Microsoft by technology and media companies, including Amazon.com, Apple, AT&T, eBay, and Verizon Communications. More than a dozen trade groups and 34 computer science professors have also signed onto briefs supporting Microsoft. Ireland also filed an *amicus* brief in the case on 23 December 2014.

The Snowden affair and potential implications for Safe Harbor

Twitter's move of non-US user data to Ireland may therefore be designed to give comfort to non-US users that their data may not be as easily accessible to organisations such as the NSA

A further potential reason for moving data to a location within the EU such as Ireland may be due to the fallout from the Snowden affair. In June 2013, Edward Snowden, a former contractor to the US National Security Agency ('NSA'), revealed that the NSA had been involved in the interception of internet and telecommunications messages on a global scale as part of its Prism surveillance programme. Snowden alleged that the NSA was secretly accessing users' private data held by various internet and social media providers, including Facebook. Similar allegations were also made in respect of other national security agencies, including GCHQ in the UK.

In light of the Snowden affair, an Austrian student, Max Schrems, complained to the Office of the Data Protection Commissioner in Ireland ('DPC') alleging that since the Snowden revelations suggest that there is no effective data protection regime in the US, the DPC should exercise its statutory powers to prohibit the transfer of personal data from Facebook Ireland to its US parent company in the US. The DPC declined to investigate the matter on the basis that Facebook was a member of the Safe Harbor regime and the European Commission had already determined in its July 2000 decision that Safe Harbor provided a valid legal basis for the transfer of personal data to the US. The DPC considered itself as being bound by the decision of July 2000.

Mr Schrems applied for judicial review of the DPC's decision. In the Irish High Court case of *Schrems v. Data Protection Commissioner*, Justice Hogan held that due to the supremacy of EU law, the DPC was bound by the Commission Decision on the adequacy of the Safe Harbor regime and therefore the application for judicial review must fail.

Justice Hogan commented that the applicant's real objection was to the terms of the Safe Harbor regime itself and not the manner in which it had been applied by the DPC. The question, however, was whether Directive 95/46/EC and the Commission Decision of July 2000 on the adequacy of the Safe Harbor regime needed to be re-visited. Justice Hogan therefore referred this and a number of related questions to the Court of Justice of the European Union including whether the DPC may conduct his own investigation into the adequacy of Safe Harbor in light of the Snowden revelations.

The case is significant in terms of its potential impact on the validity of the Safe Harbor regime which, if suspended, could have major ramifications for the digital economy and international trade.

In the aftermath of the Snowden affair, the Civil Liberties Commission of the European Parliament called for an immediate suspension of Safe Harbor and made a number of recommendations on how it should be improved, including a call on the US and EU to prohibit blanket mass surveillance activities and the bulk processing of personal data. Whilst Safe Harbor has not been suspended, the EU Justice Commissioner, Vivian Reding, has confirmed that her office is reviewing the adequacy of the Safe Harbor regime.

Twitter's move of non-US user data to Ireland may therefore be designed to give comfort to non-US users that their data may not be as easily accessible to organisations such as the NSA and to deal with the possibility that the existing Safe Harbor regime may not survive in its current form.

Legal implications of Twitter's

move

By moving its data to Ireland and providing that Twitter International Company would take over all services for non-US users, Twitter International Company has become the data controller with responsibility for such data. The Irish Data Protection Acts 1988 and 2003 therefore govern the collection, use, disclosure and other processing of the data. This includes the following obligations, which are in line with the EU Data Protection Directive:

- The collection, use and disclosure of personal data relating to non-US users must comply with fair collection and processing obligations under Sections 2(1)(a) and 2D of the Irish Data Protection Acts. This requires Twitter to ensure that data subjects are made aware of the uses being made of their data and the parties to whom it may be disclosed. Any relevant privacy and data protection notices will need to comply with such obligations;
- Twitter must maintain appropriate, robust security measures in accordance with Sections 2(1)(d) and 2C of the Data Protection Acts. The DPC will also expect Twitter to comply with the DPC's Personal Data Security Breach Code of Practice, which provides for the potential reporting of data security breaches to affected data subjects as well as to the DPC;
- Twitter will need to ensure that it does not retain data for longer than necessary in accordance with Section 2(1)(c)(iii) of the Data Protection Acts;
- Twitter also has obligations to ensure that data is accurate and relevant and that processing is proportionate in accordance with Sections 2(1)(b) and (c) of the Data Protection Acts;
- Any use of data for marketing purposes will be subject to compliance with the Data Protection Acts and the EC (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. The 2011 Regulations provide for opt-ins in respect of certain forms of marketing and opt-outs for other forms. Breach of the 2011 Regulations is a criminal offence and the DPC has not been shy about instituting proceedings (and securing criminal convictions) for breach of these Regulations; and
- The DPC will be the main data protection regulator, charged with overseeing Twitter's data protection compliance in Ireland and dealing with any data protection complaints from Twitter users.

Criticism of Ireland's data protection laws or regulation

Ireland has been the subject of some criticism, including from certain politicians in other EU jurisdictions, alleging that Ireland has lax data protection laws and enforcement and that this is one reason for digital companies moving data to Ireland. For the most part such criticisms have been mainly political sound bites and have not necessarily included detailed justifications for such criticism.

Whilst there may be a culture in Ireland of seeking to foster compliance by persuasion before needing to resort to a big stick, Irish data protection law itself and the approach of the DPC to oversight and enforcement does not necessarily bear out these criticisms. For example:

- Ireland appears to have fully implemented the EU Data Protection Directive through the Data Protection Acts 1988 and 2003. There have been no findings at an EU or other level that Ireland did not properly implement the Directive. Indeed, in respect of certain matters such as data access requests there would appear to be fewer exemptions in Ireland than apply in some other jurisdictions;
- Irish case law has recognised an un-enumerated constitutional right to privacy under the Irish Constitution; and
- Contrary to perception of 'lax' regulation, the DPC has been one of the busier regulators in Europe in respect of marketing breaches. For example, a number of organisations, including large telecoms companies, have been convicted in the Irish courts for marketing breaches on foot of proceedings instituted by the DPC.

It is likely that the reasons for Twitter and other digital companies moving data to Ireland are a mix of data protection considerations, including concerns over further potential fallout from Snowden, and the usual business reasons for multinationals to establish a greater presence in Ireland in order to better service and have easier access to other European markets.

Paul Lavery Partner and Head of the Technology & Innovation Group
McCann FitzGerald, Dublin
Paul.Lavery@mccannfitzgerald.ie