



“EU upset by Microsoft warning on U.S. access to EU cloud” (July, 2011)

This recent headline reflected the concern at the admission by Microsoft that, as a US-registered company, they would be obliged to allow access to any and all data within their control, in the event that a disclosure request was submitted by the US authorities under the USA Patriot Act. This included data held by the company in the US, but extended to data held by affiliates of Microsoft in other countries. This raised concerns because of the sheer volume of personal data being held by US service providers and commercial organisations across every industry.

It also confirmed what many had suspected for years: that data held by US companies, including those based in Ireland, Europe and the rest of the world, could be accessed by the US authorities, particularly those investigating terrorist or fraudulent financial transactions. As we have the 10-year anniversary of those terrible events of September, 2001, it is worth checking on the impact of these rights of access.

Let's start with the USA Patriot Act, a descriptive and evocative title that represents the entire anti-terrorist culture that dominates our nightly news, our travel plans and the past ten years of geo-political activity. The title is actually an acronym (pub-quiz aficionados will nod smugly at this point) for **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act** of 2001. Has quite a ring to it.

Back to the Microsoft story (and Google, and Amazon, and Bank of America, and Disney, and every other US-based organisation which might have our data): There was the usual round of “Shock! Horror!” responses – how can they? How dare they? That's OUR data, after all - they have no right! Now that we have had time to calm down, and with the benefit of mature reflection (a phrase borrowed from another old political campaign), we can see that there is no real news here. As a matter of fact, Ireland has retained a similar right to demand

access to personal data held by any organisation; Section 8 (e) of the 1988 Data Protection Act states:

"Any restrictions in this Act on the disclosure of personal data do not apply if the disclosure is... required by or under any enactment or by a rule of law or order of a court....."

We should not forget that Ireland and the UK already have quite extensive anti-terrorist laws that can provide the Government with authority to gain access to data, e.g. the Irish Offences Against the State Act and the UK's Regulation of Investigative Powers Act.

So should we be worried by what Microsoft has recently announced? Of course, there is always the concern that our data could be accessed unlawfully, or used for purposes other than those for which we provided our data in the first place. This is precisely why there are provisions within the legislation to prevent this from happening, including:

1. Where US companies are concerned, the 'Safe Harbor' scheme has been in place since 2000 to ensure that US firms, who subscribe to the scheme, observe a set of principles similar to the eight Data Protection Rules under Irish law. To date, c. 3000 US firms have signed up to 'Safe Harbor'.
2. More recently, some questions have been asked about the value of Safe Harbor, so Irish Data Controllers can avail of a further set of criteria to establish the adequacy of the protection their data will receive at its destination. These criteria can be referenced on the Commissioner's website at:
<http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3ma.htm&CatID=56&m=y#adequate> .
3. There is the further requirement that a contract must be in place between a Data Controller and any third party with whom the personal data is shared. The legislation does not say what this contract should stipulate – that should be the focus of standard legal and commercial negotiations between the contracting parties. At a minimum, an Irish Data Controller should require that their data will be managed in a manner that is compliant with the Irish Data Protection legislation.
4. Model contracts - template-based contracts which set out the minimum standard to which organisations must comply in order to meet expectations of safety and data security.

Taken together, therefore, there are several measures available to Irish Data Controllers to ensure that their data is protected and secure when it is stored outside the European Economic Area (the 30-country region which forms the primary jurisdiction for our data protection legislation). Next pub quiz question will be to name all 30, but that's for another day.

Back to the concerns about data disclosure. In the context of the events of September, 2001, we must acknowledge the right of any sovereign state to protect its borders and to prevent a recurrence of those harrowing attacks. The US could hardly be labelled a rogue state, and we must take on faith that where the USA Patriot Act is invoked, there are adequate and valid reasons for doing so.

In the meantime, and to echo the opinion of the Data Protection Commissioner in a recent response, there are bigger and more troublesome issues to be concerned about – the policies and processes of those organisations who legitimately have our data; the likelihood that a member of staff fails to show the appropriate level of awareness or respect for that data; the risk that a well-intentioned but forgetful employee will lose a lap-top/inadvertently send unencrypted e-mails/throw sensitive documents in a skip without shredding them beforehand, etc. In other words, the common or garden screw-ups and errors which form the basis for 95% of our data protection breaches, regardless of what continent, country or jurisdiction the data is being held in.

We should focus on the day-to-day safety and security of our data, rather than get over-excited about the (thankfully) rare and unlikely event that the guys from Homeland Security come knocking.

Hugh Jones is a Data Protection consultant, a member of the IDMA Regulatory Sub-Committee, and an associate member of the Irish Computer Society (ICS). The Society offers training and consultancy in Data and Privacy protection at its offices in Lower Mount St.