An Taoiseach Enda Kenny TD
Department of an Taoiseach
Government Buildings
Merrion Street
Dublin 2

4 November 2014

RE: Law Enforcement Access to Data in the Irish Cloud

Dear Taoiseach,

As you know, the American Chamber of Commerce Ireland has close working relationships with the global American Chamber network. This network represents the interests of American multi-national companies across the world. The American Chamber of Commerce Ireland is one of the largest chambers in Europe as a result of the large base of American companies located in Ireland. These companies provide benefits, and economic growth in Europe, and several are technology companies that offer cloud-computing technology to European customers.

Europeans can derive many benefits from widespread adoption of cloud computing technology. However, many Europeans may be hesitant to embrace cloud services because of lack of clarity about how their data is stored in remote data centres, many of which are located in Ireland. As a result of a number of matters that have been widely reported, such as the Snowden disclosures, European citizens have become more sensitive to ensuring respect for their right to privacy, including controls over how and to what extent data relating to them might be accessed by law enforcement authorities. The multijurisdictional dimension of cloud computing presents a number of legal challenges in this regard.

This letter addresses one of the specific concerns - **the extraterritorial reach of law enforcement authorities to access data in the context of routine criminal investigations.** We believe that this concern can be effectively addressed by the Irish and US governments, to enhance the public's trust while also increasing the effectiveness of law enforcement.

A recent US court case[1] has highlighted an approach taken by US law enforcement authorities towards access to personal data stored in Irish data centers that we believe is inconsistent with

[1] *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 13 MJ 2814, US District Court, Southern District of New York.*

national as well as European law and principles. In this specific case, a US district court judge in New York has upheld a warrant requiring a global cloud provider to deliver a customer's email content, stored in Dublin, to US prosecutors for a criminal investigation.[2]

The case raises concerns about how to balance the needs of law enforcement in an Internet-connected world with the sovereignty of individual nations. Of particular concern is the failure to use agreed international protocols to obtain the information. The Mutual Legal Assistance Treaty (MLAT) between Ireland and the US establishes procedures of cooperation for law enforcement authorities that the Court should have considered. By using clear and agreed procedures, law enforcement authorities can (and routinely do) obtain evidence they need; citizens can be sure that laws in their own countries are respected; and companies can provide assurances to governments and to citizens that they are not subject to action by law enforcement authorities in another country without respective checks and balances of the country that receives the request and where the data are stored.

Citizens and companies expect that governments will use procedures agreed in MLATs where they apply, and such practices can help provide a greater degree of confidence in cross-border cloud services. If MLAT procedures do not function as efficiently as is necessary to protect public safety, respect for national sovereignty requires that such procedures be improved, rather than set aside. The result will not only be more respect for national laws, but also improved coordination in cross-border criminal investigations or other government requests for data access in a third country.

The Chamber is extremely concerned about the implications for this court action for the data sector in Europe and future interactions between Europe and the US. We would welcome the Government's engagement on this issue. Should Government share our concerns we understand that it can express these concerns by filing an amicus brief with the appellate court in New York, utilizing the procedure created under U.S. law to ensure that courts have the benefit of this type of information before making a decision**.** In addition, we recommend that Government calls for a multilateral dialogue with the aim of: 1) encouraging governments to respect sovereign boundaries, and, therefore, to use MLATs when seeking data stored in another country in furtherance of routine criminal investigations in non-exigent circumstances; and 2) calling for further investment in the development of MLAT processes so that they function effectively, which will increase the effectiveness of law enforcement, and obviate the need for cross-border demands directly to providers.

Maintaining the trust of our citizens by protecting their privacy and guarding against unreasonable government intrusions is fundamental to the European data sector. We understand that

[2] This judgment is being appealed to the Second Circuit Court of Appeals.

governments have a need for legitimate access to user data in confronting crime and in strengthening national security, but a better balance must be struck that allows governments to address criminal threats while at the same time preserving the right to privacy.

The American Chamber of Commerce Ireland supports efforts to clarify rules relating to law enforcement access to data governed by the laws of another country. We observe with concern that, increasingly around the globe, governments are adopting law enforcement access laws with extraterritorial reach. As noted above, we firmly believe that the preferred route is multilateral agreement on the "rules of the road" for obtaining digital content across borders that respect privacy, ensure law enforcement swift access to the evidence it needs, and that respect national sovereignty. Legislation recently introduced in the United States Senate [3] highlights some helpful principles that could perhaps inform this debate.[4]

We would greatly welcome the Government's engagement on this critically important issue for Ireland's and Europe's data sectors.

If you or your officials require any further information on this issue please let me know.

Yours sincerely,

Louise Phelan

Louise Phelan
President

[3] See The Law Enforcement Access to Data Stored Abroad (LEADS) Act, http://www.hatch.senate.gov/public/index.cfm/releases?ID=8e28c3f9-842b-4d96-83b7-9f71cf40bc07

[4] The bill's main principles are: governments should access data stored in their own territory only through appropriate legal process; governments should not unilaterally reach across international borders to access email or other private content; when governments need data in another country, they should use established international legal channels like MLATs; MLAT processes should be made more efficient; In limited circumstances, if a government is going to use domestic processes to reach across its borders, it should confine that power to accessing the content of its own citizens; an international convention on government access should be based on respect for human rights, individual privacy and respect for the laws of other countries.