REGERINGSKANSLIET

17 February 2016

Ministry of Justice
Police Division
Sweden

Swedish contribution to the Presidency Conference Crossing Borders: Jurisdiction in Cyberspace

I. Introduction

The Dutch Presidency has invited participants to submit papers that provide further insight into possible courses of action in order to improve the effective international enforcement of the rule of law in cyberspace. In responding to this invitation, the Swedish Ministry of Justice wish to address issue 2. Conflicting regulations hamper cooperation with private parties.

II. Improving cooperation with private parties

i) The issue

In its invitation to the conference, the Presidency has observed that conflicting regulations hamper cooperation with private parties. The Swedish view is that a primary concern as regards cooperation with private parties is the access to non-content data. The lack of access to such information frequently hampers or stops further investigations into not only cross-border crimes, but also solely Swedish-based crimes.

According to Swedish legislation, the threshold for accessing certain non-content data (subscriber information) is simply connected to the fact that there is a suspicion of a crime and hence a criminal investigation open. However, a particular challenge is that completely domestic, Swedish investigations are hampered by a far too less developed international cooperation as regards accessibility of information and evidence held by private enterprises in a jurisdiction other than the Swedish. It often occurs that a Swedish criminal investigation must be

closed due to non-content data not being disclosed from private enterprises in such jurisdictions.

The Swedish experience confirms that cooperation with in particular US and US-based corporations are key if we are to succeed in fighting cybercrime. Since it is within the legal powers of these corporations to voluntary disclose non-content data, Sweden has sought to establish agreed ways and procedures of requesting and accessing such information from a number of US-based corporations. In some cases these efforts have been successful, in other cases less successful.

Overall, it is believed by Sweden that it is possible to improve the accessibility of this information for EU law enforcement purposes while at the same time achieving a more effective and secure cooperation from the perspective of a private, US counterpart. To this end, further developments of a common EU-approach and a constructive dialogue with US-based corporations are proposed to be organised in an appropriate sequence and context.

ii) *Proposal*

Sweden proposes that work is initiated at EU-level, as a first step, to elaborate a common EU law enforcement approach on this issue in a convenient EU-context. EC3 should be invited to contribute on the basis of its insights of current state-of-affairs at EU-level and beyond. The work must take into account current developments such as the Directive on data protection of individuals in the field of fighting, preventing and investigating crime and the EU Internet Forum.

As a second step, the EU law enforcement community should engage in a dialogue with a set of US and US-based corporations playing leading roles in the functioning of the Internet in order to identify in as clear terms as possible a joint understanding on how and when non-content data can be made accessible to EU law enforcement agencies. On the US side, US DoJ, FBI and DHS should also be invited to take part in such a dialogue.

iii) Positive experiences in Sweden/best practice

A key element in the successful efforts by Sweden to establish cooperation with private, US counterparts has been to channel all requests and responses through a Single Point of Contact (SPOC). Applying the SPOC-concept has many advantages both for the Swedish Police and a private, US counterpart. On the side of the Swedish Police this means that the desk at the Swedish Cyber Crime Centre, the SC3, maintains an overview and gain experience over time on how to manage the cooperation in the best possible way. It also allows for an appropriate supervision of data protection issues. On the side of the private, US counterpart, the use of a SPOC allows for smoother processing in that

the law enforcement SPOC can provide the credentials necessary for requesting non-content data and receiving voluntary disclosed information.