COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, 17 December 2015 T-CY (2015)25

Cybercrime Convention Committee (T-CY)

Cloud Evidence Group

Hearing on Criminal justice access to electronic evidence in the cloud

Strasbourg, 30 November 2015

Summary

Parties and Observers to the Cybercrime Convention Committee (T-CY) and representatives of Apple, AT&T, Deutsche Telekom, Facebook, Microsoft, and NOS Comunicações as well as the Anti-Phishing Working Group and the Max-Planck Institute for Foreign and International Criminal Law participated in a hearing aimed at identifying solutions to the challenges faced by criminal authorities when accessing evidence in the cloud within specific criminal investigations.

The hearing was held by the T-CY's Cloud Evidence Group which is tasked to propose options to the Cybercrime Convention Committee by November 2016.

Discussions focused on the two specific questions, namely (a) the production of subscriber information, and (b) direct cooperation between service providers and foreign criminal justice authorities.

With regard to question (a) that is, when is a service provider offering a service on the territory of a Party and thus subject to a domestic production order (in line with Article 18.1.b Budapest Convention),

- the situation seems rather clear with respect to providers of electronic communication services which are registered and licensed in a Party in that they are subject to domestic law, including coercive measures;
- the situation is less clear with regard to providers of other types of services such as hosting or content providers even if they have a subsidiary or marketing office in a Party;
- additional complications arise given increasing convergence of different types of service provided by the same provider.

With regard to question (b) that is, direct requests sent from a criminal justice authority of a Party to a service provider in a foreign jurisdiction without going through mutual legal assistance,

- many providers with their Headquarters in the USA cooperate voluntarily and disclose information other than content upon a lawful request under certain conditions directly to foreign law enforcement;
- such cooperation combines a lawful domestic order (including coercive production orders or court orders) with voluntary compliance on the part of a private sector entity;
- this appears to address the practical problem of Article 18.1.b with respect to providers other than licensed electronic communication services;
- European providers are normally not allowed to voluntarily disclose any type of data to foreign authorities;

- cooperation by US providers is not coherent: different providers have different policies, apply them differently in Parties, and keep changing them.

The hearing suggested a common understanding that,

- clear domestic and international legal frameworks are needed to ensure greater legal certainty for law enforcement and industry and to remove obstacles for businesses.

The preparation of such frameworks will take time to achieve. In the meantime,

- current procedures should be improved while building on good practices already available;
- the Council of Europe should develop an online tool to facilitate access (a) by law enforcement to policies and tools (such as law enforcement portals) of providers, and (b) by providers to relevant legislation of requesting authorities;
- the Cybercrime Convention Committee and providers should explore the preparation of guidelines to facilitate cooperation.