Hearing

Criminal justice access to electronic evidence in the cloud

Strasbourg, 30 November 2015

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Question 1: Domestic production orders for subscriber information when "offering a service on the territory" of a Party

Considering Article 18 paragraph 1.b. of the Budapest Convention and its explanatory report (see appendix):

a. When do you, as a service provider, consider that you are offering a service on the territory of a State?

b. Thus, when do you consider that you are subject to a domestic production order for subscriber information in the country where you are offering a service?

c. What are the criteria, conditions or circumstances that make you accept or decline such a request?

Term “service provider”

Article 1 Budapest Convention – Definitions

For the purposes of this Convention:

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Article 18.1.b

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b **a service provider offering its services in the territory of the Party to submit subscriber information** relating to such services in that service provider's possession or control.

Explanatory Report para 173:

Under paragraph 1(b), … the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company).

Question 2: Direct cooperation between criminal justice authorities (such as police, prosecutors or courts) and foreign service providers

Transparency reports published by many service providers indicate that service providers often respond to request for data that they receive directly from criminal justice authorities. Thus:

a. What are your policies and practices, criteria, and conditions for responding directly to a request for (a) subscriber, (b) traffic, and (c) content data from a foreign police agency, prosecution service or court?

b. What are your policies and practices regarding criminal or non-criminal emergency requests?

c. Do you have written guidelines for cooperation with criminal justice?

Question 2: Direct cooperation between criminal justice authorities (such as police, prosecutors or courts) and foreign service providers

Transparency reports published by many service providers indicate that service providers often respond to request for data that they receive directly from criminal justice authorities. Thus:

d. Do you require permission from the authorities of your country before responding to a request from foreign criminal justice authorities?

e. What are your policies and practices regarding informing the customer of a criminal justice request? What are your requirements for not informing the customer?

Re Question 2e: "What are your policies and practices regarding informing the customer of a criminal justice request" (Information provided by a law enforcement officer of a European country that faced terrorist threats in November 2015):

1. On someone's [Social Media Account], we see that someone writes in the name of ISIS that [CITY] will be attacked on [DATE]
2. We also found these postings on the [Social Media Account]
3. [Social Media Provider] disclosed subscriber and login information based on our emergency request. So far so good.
4. We could see that there's a [Webmail] email connected to that [Social Media Account].
5. So, in order to have more information, I did a similar request to [Webmail provider].
6. They sent me their new policy where they write clearly that also for imminent physical threat procedures they have the right to advise their client.
7. So we asked for more clarification... "ONE QUESTION ABOUT THE [Webmail Provider] DISCLOSURE POLICY: WHAT INFORMATION ABOUT THE REQUESTER WOULD YOU PROVIDE TO THE ACCOUNT HOLDER? WOULD IT BE SOMETHING RELATIVELY GENERAL LIKE "THE AUTHORITIES OF [COUNTRY]" OR WOULD YOU DISCLOSE THE ACTUAL NAME AND EMAIL ADDRESS OF THE PERSON WHO SIGNED THE EMERGENCY DISCLOSURE REQUEST. WE WOULD LIKE TO KNOW THIS AS THIS MAY MEAN THAT A POTENTIAL TERRORIST MAY RECEIVE PERSONAL INFORMATION OF A LAW ENFORCEMENT OFFICER.
8. They called me back, telling me that they understand the situation, <u>but they cannot guarantee that after 90 days my contact information won't be given to the client</u>.