Project Cybercrime@Octopus

Conference

Article 15 safeguards and criminal justice access to data

19 – 20 June 2014, Council of Europe, Strasbourg, France

Scenarios for discussion*

www.coe.int/cybercrime

*These typical scenarios have been drafted based on actual situations to stimulate discussions. They do not necessarily reflect official positions of the Council of Europe or the Parties to the Convention on Cybercrime.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

Scenario 1

In a kidnapping case being investigated by European country A, ransom notes are coming from an email address that originates with a US provider. Country A wants to know the accountholder's information.

An IP address is considered personally-identifiable information by Country A. A is not permitted to provide personally-identifiable information directly to US providers because they are private parties, not governmental parties. The notes threaten to kill the victim in two days if conditions are not met.

Should A be permitted to send the information to the US provider because it is an emergency (and because identifying an accountholder would be only the start of the investigation)?

If yes, may A's law enforcement authorities send it immediately, or must it undergo data protection review? If it must undergo data protection review, what would the review entail? Should A be required to establish procedures for emergency data protection review?

2

Scenario 2

A teenager who is close to her parents telephones them to say that she is walking home from a party but then disappears. The police would like to examine her numerous social-networking accounts, which are run out of several different countries. The distraught parents cannot find her passwords. The girl is not an adult under the law of her country.

Should her parents be permitted to give consent to the police to search the account?

3

Scenario 3

Investigators in Country A are investigating a massive fraud. Several hundred people lost all their savings when they tried to purchase certain items using an Internet service originating in Country B. The items were never delivered.

A founder of the group who has administrator privileges on its website, hosted in B, is arrested while on vacation in A. He wants to cooperate with the authorities of A to disclose IP addresses of participants, financial documents, the network tools that were used, and similar evidence. Such cooperation would reduce his prison sentence and his attorney is advising him to cooperate. The authorities want the disclosures in order to shut down the network and locate unknown victims.

4

Scenario 3 cont'd

The Article 29 Working Party states that consent is freely given only in the absence of several factors, including "significant negative consequences." Should the arrested man and his counsel be allowed to consider his cooperating to reduce his prison sentence? Would it violate the arrestee's human rights to deny him the possibility of reducing a prison sentence? What about the rights of the victims to possible restitution?

Similarly, the Article 29 WP letter discusses what constitutes "consent" or "lawfully obtained credentials" under EU data protection law. Criminal law inside and outside the EU may define "consent," "lawfully obtained credentials," and other terms differently than data protection law does.

If criminal law and data protection law would yield different results, which law governs? What if a country with inadequate data protection laws is involved?

5

Article 15 safeguards and criminal justice access to data
Scenarios

Scenario 4

Police-to-police passage of information is favored by law enforcement because it can keep an investigation moving, even though it may be foreseen that a formal mutual legal assistance request may be needed to obtain evidence that is usable at trial. Is police-to-police passage of data impermissible if the data would go to a country judged to have inadequate data protection rules by EU standards?

6

Scenario 5

A group has collected and posted public information, including home address, photographs, children's schools, etc, about a group of policemen from Country A. While the information is public, it gives a very complete picture of the policemen's lives when the information is aggregated. They are frightened for themselves and their families. There are no explicit threats of violence but an investigation is opened.

The website is hosted in the US to take advantage of a) US Constitutional hurdles to searches by the US government and b) difficulties of cooperation between EU countries and the US.

The police in A, a civil-law country that is a Party to the Budapest Convention, have arrested someone who wants to cooperate voluntarily and seems to have the lawful authority to consent to disclosure of data from the website. The police in A know that the US is a Party to Budapest and would like to do a search of the website pursuant to Article 32 b.

Data protection authorities in A tell the police in A that they must follow the suggestion of the Article 29 Working Party and, therefore, apply US law in determining whether they have valid consent under the Budapest Convention.

7

Article 15 safeguards and criminal justice access to data
Scenarios

Scenario 5 cont'd

The police and justice authorities swiftly become confused about US law. It is not statutory but case law; they are unfamiliar with the distinction between the law of US states and US federal law; they don't know which federal district is relevant to the place where the website is hosted; and, while they know which federal circuit to research, they are unaware that a leading case on consent has just been decided in a different federal circuit court.

Recently, there have been daily postings of photos of children of these police officers on their way to school, but no explicit threats. Since the authorities are increasingly worried that there may be a tragedy at any time, what should they do?

They have been advised by the US government that this is probably not an emergency, so they have decided not to apply for help from the US provider on an emergency basis.

8

Scenario 6

Often computers inside a country are networked with computers outside it. As long as they have a valid legal basis for a domestic search, an increasing number of countries (including EU countries) permit themselves to search foreign networked computers.

This permission is based on statutes or court decisions but also on frustration with mutual legal assistance.

If such practices violate data protection law, may a country carry out such networked searches?

9

Scenario 7

Mr A cyberstalks Ms B. Becoming nervous about being discovered, he asks the relevant provider to delete a certain posting. He tells the provider that B is his mistress and it would be embarrassing and destructive of his private life if his wife became aware of the posting. The provider rejects the request, so A applies to his data protection authority. Without consulting B, the data protection authority orders the provider to delete the posting.

Law enforcement is eventually alerted by B. When law enforcement seeks the posting from the provider, it is irretrievable.

Is the data protection authority liable for damages or some type of sanction because it acted without obtaining the full facts, particularly by not consulting B?

10

Scenario 8

In a serious criminal investigation, Country A seeks preservation of data from Country B. Both are Parties to Budapest. However, unknown to law enforcement authorities in A or B, the data protection authorities in B have ordered the provider to delete the same data that Country A is seeking. The provider has not acted yet, so this is still an open question.

Should the data be preserved or deleted?

Scenario 9

During criminal investigations your law enforcement agency has acquired via an "informant" knowledge of the username, login and password of an e-mail account in which e-mails were present containing information on drug trafficking to your country, including details of modus operandi and dates of smuggling these drugs into your country. The data is not stored in your country. Urgent action is required.

What options:

1. **A prosecutor issues a production order to a foreign service provider requesting email data related to a specific email account?**
2. **The prosecutor instructs the police to access the email account via "webmail"?**

Scenario 10

During criminal investigations into a child pornography case your law enforcement agency detects servers on which there were very violent child abuse images. Via a bulletin board on the servers it is even possible to "order" the execution of "hands on" sexual child abuse and the recording of the abuse in images which are to be sent to the person placing the order. The location of these servers is unknown ('hidden services').

a) A search of so-called TOR (The Onion Router) servers that were known NOT to be located in your country is ordered with the consent of a magistrate.
b) Digital copies of the incriminating information to be used in the criminal case later on are made in the process of search and seizure of the TOR servers, and the data on the servers is destroyed.

13

Scenario 11

Mr A, who was a resident but never a citizen of Country 1, was tried and convicted by Country 1 for complicity in the murder of 3,000 people in Country 2. He served a prison sentence in Country 1, he had no relatives, and he's dead.

Should data protection rules prevent his digital personnel records from being made available to foreign prosecutors who are conducting related investigations?

If his personnel records should be unavailable for data protection reasons, what is the public interest being protected?

14

Scenario 12

Transborder access to data in another Party with consent (Article 32b)

A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

15

Scenario 13

Transborder access to data in another Party with consent (Article 32b Budapest Convention)

A suspected drug trafficker is lawfully arrested while his/her mailbox hosted in another country – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device.

If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.

16

Scenario 14

Transborder access to data with consent but not necessarily in another Party

A suspected drug trafficker is lawfully arrested while his/her mailbox that is likely to be hosted abroad – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device.

If the suspect voluntarily consents that the police access the account but if the police are NOT sure that the data of the mailbox is located in another Party, may the police proceed and access the data?

17

Scenario 15

Transborder access to data without consent

A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device or the police has obtained the access credentials during a lawful search.

The suspect does not consent. Can the police access the account under domestic procedural rules even if the data are likely to be located in another State?

18

Scenario 16

Transborder access to data without consent in good faith or in exigent or other circumstances

1. Your are in country A and doing a search without consent in a well-known provider in your own country A. Without your knowledge, the provider has changed its network architecture and moved the data to country B.

2. In an emergency situation (e.g. a kidnapping investigation), law enforcement has lawfully acquired the access credentials to an email account under a domestic procedure and uses the credentials to search the account.

Scenario 17

Transborder access by extending a search from ones territory to another territory

A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device or the police has obtained the access credentials during a lawful search.

The suspect does not consent. Can law enforcement search the device and extend it to data hosted abroad under domestic procedural rules (e.g. domestic court order)?

Scenario 18

Power of disposal as connecting legal factor in situations where territoriality cannot be determined

A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device or the police has obtained the access credentials during a lawful search. The suspect does not consent.

It is not known where the data is located. The data may be moving or fragmented over different locations/jurisdictions. Or the provider doesn't know where the data is located.

Can the police carry out the search under domestic procedures (possibly with a court order) since territoriality cannot be determined based on the fact that the suspect is under the jurisdiction of the police and has the power to dispose of the data?