Communication interception regarding Google, Microsoft & Yahoo! tools and electronic data retention on foreing server: a legal prospective from the State which is conducting an investigation

Octopus Interface Conference
Council of Europe, Strasbourg
11 March 2009

WELCOME TO THE CYBERSPACE!

CYBERSPACE= A SPACE WHERE…

- ✓ the traditional country borders are **cleared** during the action made by the cyber criminal

- ✓ the traditional country borders **come back** only later, when the detectives try to trace that action searching digital traces maybe left by the author and so useful for the investigations

"A space with law but a cyberspace without law, just because it is cyber !"

Google Microsoft YAHOO!

"no server no law" opinion

vs.

"no server but law" opinion

The ***"no server no law"* opinion** is the one that prefers the place where the web servers are based: and often, they are outside the European Community.

This layout sustains that our respective laws (national or European) couldn't be enforced just because there aren't any web servers neither in Italy nor in Europe.

The ***"no server but law"*** **opinion** says that it's crucial the place where the web services are offered, no matter where the web servers are, even to the purpose of the law enforcement.

Besides, this layout is in line not only whit a correct application of any European laws but also whit the internet jurisdiction analysis executed by the American Courts.

We need to verify if these societies have **the availability of**

a) communication channel
b) communication data

Google Microsoft YAHOO!

a) a society with communication channel availability

Google Microsoft YAHOO!

national Internet Service Provider

intercepted account

judicial police account

Court Order

Google Microsoft YAHOO!

(server abroad)

Internet Service Provider

Court Order

"We are sorry but the servers are in USA, so please ask for the interception with a rogatory!"

Google YAHOO! Microsoft

b) a society with communication data availability

Google Microsoft YAHOO!

This hypothesis refers data regarding the Internet access, such as log files.

At first the these three societies requested a rogatory to provide all these data but then they changed their minds and, generally, they only need the request from the Italian Public Prosecutor.

For some of these societies an important problem regarding this data retention must be taken into consideration.

Some preliminary enquiries

In order to face the problem better as investigators, we need to know

- ✓ where the society has his own **web servers**
- ✓ where the society has the **main legal registered office**
- ✓ if the society has **an operating branch in the State where the investigation is conducted** (and which law this branch is subjected to)
- ✓ if there are some people, by these operating branches, who have **the chance of a concrete management**

"*Internet law and regulation*": the Internet jurisdiction analysis executed by the American Courts

U.S. courts have developed two general lines of analysis in determining whether jurisdiction can be exercised in cases involving Internet activity:

- ✓ The first, a "**sliding scale" approach**, seeks to classify the "nature and quality" of the commercial activity, if any, that the defendant conducts over the Internet *[Zippo Manufacturing. Co. v. Zippo Dot Com. Inc., 952 F Supp 1199 (WD Pa 1997)]*
- ✓ The second analysis (called **"effects test"**) seeks to determine to what extent a defendant's intentional conduct outside the forum state *[Calder vs Jones, 465 U.S. 783 (1984)]*

<< The cases discussed above demonstrate that a foreign Internet entrepreneur, although lacking "continuous and systematic" contacts with any U.S. forum state sufficient to subject him or her to general jurisdiction, may nonetheless be subject to personal jurisdiction in the U.S. based on two broad theories of "specific" personal jurisdiction.

Under the *Zippo* "sliding scale" analysis, a U.S. court will classify the "nature and quality" of any commercial activity that the defendant conducts over the Internet and place it on a continuum ranging from "passive", where no business is conducted, to "clearly conducting business". **The closer the Internet activities are to "clearly conducting business", the more likely that a U.S. court will exercise personal jurisdiction.**

Courts may also apply the *Calder* "effects test" to determine whether the defendant's intentional conduct was calculated to cause harm to plaintiff within the forum state. **Where a defendant "purposefully directs" his activities at the jurisdiction, he may be liable to suit for any injury relating to or arising from those activities** >>

[G.J.H. Smith, "Internet law and regulation", Sweet and Maxwell, 2002 (3rd edition), pp. 347-349]

Google Microsoft YAHOO!

Which obligations and national laws can we expect observance of?

Google Microsoft YAHOO!

1) the **electronic communication rules** (Legislative Decree of 1st August 2003 n. 259) with EC origin in four Directives:

DIRECTIVE 2002/19/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)

DIRECTIVE 2002/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)

DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

DIRECTIVE 2002/22/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

DIRECTIVE 2002/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive)

Article 6

Conditions attached to the general authorisation and to the rights of use for radio frequencies and for numbers, and specific obligations

*1. **The general authorisation for the provision of electronic communications networks or services** and the rights of use for radio frequencies and rights of use for numbers may be subject only to the conditions listed respectively in parts A, B and C of the Annex.*

ANNEX

A. Conditions which may be attached to a general authorisation

[…]

*11. **Enabling of legal interception by competent national authorities** in conformity with Directive 97/66/EC and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

Google Microsoft YAHOO!

According to these American societies, there are some US laws that will prevent themselves from imparting anyone data regarding communications of their users.

But if the Italian Judge who authorizes the wiretap is able to testify that **the communications are involving two Italian people both on the national territory**, what kind of legal obstacle it would be?

And this kind of denial doesn't sound as an act contrasting with **the sovereignty of the applying State**?

Google Microsoft YAHOO!

2) the **data retention rules** (Legislative Decree of 30th May 2008 n. 109) with EC origin too

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Google Microsoft YAHOO!

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 **are retained for periods of not less than six months and not more than two years from the date of the communication**.

The data retention rules are the true "test bench" in order to verify the **real will, by any web society, to actually cooperate with the European Authorities and Judicial Police** to reach an efficacious contrast actions towards internet crimes

"Although Google's headquarters are based in the United States, Google is under legal obligation to comply with European laws, in particular privacy laws, as Google's service are provided to European citizens and it maintains data processing activities in Europe, especially the processing of personal data that takes place at its European center".

(Peter SCHAAR, President Article 29 Data Protection Working Party, 16 May 2007)

Yahoo! Italia vs. Public Prosecutor's Office in Milan

- ✓ his base principle is called "**Net Citinzenship**" = when the Italian user registers an account from the webpage *yahoo.it*, **he can choose which legislation to subject his e-mail box**.
- ✓ a software (called *Yahoo! Account Management Tool* and used by all the Yahoo! branches) which gives back the data of e-mail boxes (*@yahoo.it* and/or *@yahoo.com*) but **only from users who chose the Italian law**.
- ✓ we can intercept these emails **even without rogatory**.
- ✓ **30/45 days of data retention** (**against a period of 12 months**, which has already provided by the Italian Law **since 2005** before the implementation of the EU directive).

Yahoo! Italia vs Public Prosecutor's Office in Milan

Yahoo! Italia attorneys have communicated that **the society will spontaneously conform to EC Directive** and that it will retain log files for 12 months.

That will happen **not only for the Italian Judicial Authority requests but also for the ones of the other EC states** (starting from 21st November 2007).

Google Microsoft YAHOO!

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Article 3

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

The present situation regarding Microsoft data retention periods

Microsoft

The present situation, regarding the Italian experience, consists in **Microsoft data retention periods not in line with the EC Directive**, because it gives back informations about its e-mail boxes only about the last **60 days**.

Anyone has a basic experience in cybercrime investigations can understand how short this period is and how **this situation effectively creates enormous damages** to the investigations in progress in the EC States!

Conclusions

Data retention and a faster way to enable the wiretap of e-mails @*.com* needs to support costs, but **can we affirm that economical reasons can prevail over the defence of the people's rights** which were damaged by (cyber) crimes?

Reasoning in terms of balance sheet, the **business costs not supported by these societies are changing into higher social costs**.

And where are the **profits**?
In the criminal association's pockets!

The classical meaning of Freedom, which for the ancient Greeks "*was meant as the obedience to Law"*

(De Romilly, *La loi dans le pensèe grecque, p. 23*)

Google Microsoft YAHOO!

The **2001 Council of Europe Convention on Cybercrime,** which provides for two precise obligations of cooperation (artt. 33; 34 in connection with art. 21.1.b.II)

Google Microsoft YAHOO!

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Google Microsoft YAHOO!

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to **co-operate and assist the competent authorities in the collection or recording of,**

content data, in real-time, of specified communications in its territory transmitted by means of a computer system […]

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or rec data of specified communications transmitted by means of a computer system to the exte their applicable treaties and domestic laws.

The Internet as a space of freedom…

… the danger of a different concept of freedom, meant as the absence of laws

Francesco Cajani

Deputy Public Prosecutor
High Tech Crime Unit
Court of Law in Milan
Italy

francesco.cajani@giustizia.it
www.iisfa.eu