ARTICLE:

INTERNATIONAL PHISHING GANGS AND OPERATION PHISH & CHIP[1]

By **Francesco Cajani**

In this article, I set out in brief detail how the prosecuting authorities in Italy worked with their counterparts in Romania to investigate a large and damaging phishing operation, organized by two criminal gangs in Romania.

Background

The Phish & Chip operation outlined in this article can be described as a second generation investigation about phishing. In Italy, the first phishing e-mail occurred in March 2005. It was a little attack against Poste Italiane, the government-owned postal service that offers financial services across Italy. I had the luck to coordinate the first investigation, which began in May 2005, when we had a bigger attack against Banca Intesa and three other Italian banks that had their registered offices in Milan. At that time, it was not understood why the money was not moving directly abroad (from where the phishing e-mails were sent), but from the defrauded bank accounts to other people living in Italy. We searched ten homes across the country, and discovered how the money was transferred abroad, in particular to St Petersburg in the Russian Federation, using the Western Union money transfer system. The thieves sent two types of e-mail. The phishing e-mail was sent out to obtain the data of legitimate on-line current accounts of those that responded. Another e-mail was sent, offering work to people as a financial manager. When they had a sufficient number of 'financial mangers' and the details of a sufficient number of on-line bank accounts, the thieves then authorized the transfer of funds from the victim's account, and paid it in to the account of the newly-recruited financial manager. When the money had been successfully transferred, the thieves then directed the financial manager to transfer the funds abroad.

It is for this reason that it is important to profile a cybercrime during the investigation: in this case, as soon as we found out how this new criminal method worked, I reached, in my capacity as the Italian Judicial Authority, an agreement with Western Union Inc. in the United States of America. They told us it was the first time any prosecuting authority had approached them, and we reached an agreement[2] called 'international seizure warrant'. According to the agreement, Western Union was requested to delay the suspect money transfers for 48 hours, which gave sufficient time to verify whether the transfer was genuine. We provided Western Union with a list of the names of people, and destination countries, and they contacted us, in real time, to give us the MTCN (Money Transfer Control Number)[3] of the suspect transaction. This was a very demanding exercise, and it was partly thanks to another group of the Military Financial Police in Milan (Gruppo Repressione Frodi - Antifraud Group), in particular to Gerardo Costabile and Giuseppe Mazzaraco, over 250,000.00 euro was seized in two months, all of which was intended for the Russian Federation.

Further developments

In 2006, we had the first case of people entering Italy from East Europe to collect money by themselves from phishing attacks, rather than through Western Union (whose operations were monitored by us). In Milan, we arrested two Latvians whose purpose was to open bank accounts in several banks with false passports and

[1] *This article has been prepared from a presentation given by the author at the Digital PhishNet Conference 2008 in San Diego California on 30 September 2008 (many thanks to Luisa and Valeria Viganò for the review). The power point presentation is available at http://www.osservatoriofinanziario.it/of/DPN2008_Phish&Chip.pdf. For more information about phishing and misappropriation of digital identity in Italy, see F. Cajani, G. Costabile and G. Mazzaraco, Indagini informatiche e sicurezza bancaria ('Phishing and digital identity theft. IT investigation and bank security'), (Giuffrè editore, Milan, 2008) and http://www.osservatorio finanziario.it/of/newslarge.asp?id=636.*

[2] *It can be considered a 'gentleman's agreement' rather than one issued under articles 12 and 13 of the Convention of the United Nations against Transnational Organized Crime. Every time we get the information required from Western Union, we make a request to a judge to seize the suspect money transfer, in accordance with Italian Law.*

[3] *This is the numerical code of the transfer, formed by ten digits, given to the sender of the transfer, and the beneficiary must have it to simplify the transfer identification process at the moment of the money is collected.*

documentation. In the beginning of 2007, a new method of cybercrime was immediately discovered through the Phish & Chip operation. To begin, it is worth setting out how the cybercrime worked: the individual aims to remain in their own country, sending phishing e-mails and receiving money without using the Western Union. They can do this with a large number of prepaid credit cards bought in Italy by a group of people directly managed by the criminal, and is described in more detail below.

The Phish & Chip operation

The Phish & Chip operation started in February 2007, when the managers in charge of preventing fraud at Poste Italiane reported some unusual operations concerning prepaid credit cards (called Postepay cards[4]) bought in Milan. I was responsible for coordinating the investigation held by the Provincial Command of the Military Financial Police in Milan, the Guardia di Finanza, Gruppo Pronto Impiego,[5] with the cooperation of the Romanian investigators of the brigata de combattere a criminalitatii organizate (the brigade to combat organised crime).

The first step of the investigation was to discover the meaning of this unusual buying pattern. Two connected organizations were identified, made up of Italian and Romanian citizens. The operative framework was the same: members of the organization activated the prepaid cards (they also used Banca Intesa cards, called Intesa flash cards); the phisher sent e-mails, and collected the relevant data to enable them to gain access to on-line bank accounts; the 'boss', whose duty was to collect the prepaid cards, paying 50.00 to 100.00 euro for each, gave the phisher instructions in order to prepay the cards, and to withdraw the money once each card was topped up. The method used was called the 'Casinò system'. The withdrawal of illegally transferred funds was carried out through a particular mechanism: some of the members of the criminal organization went to Italian and foreign casinos (mainly in Germany, Austria and Greece) and they purchased 'chips' for the maximum permitted amount with the cards 'charged' illegally. In this way they managed to launder 3,000.00 euro per withdrawal, instead of the mere 250.00 euro at ATMs.

Interception of mobile telephones

Further to the monitoring of the prepaid card activations within the territory of Milan, we analysed all the IP addresses of the illegal on-line bank transfer operations, in order to find – as it later happened – a vulnerability in the framework used by the phishers. At the beginning of the investigation, success seemed a long way off: the criminal bosses used a number of aliases and sophisticated electronic tools. For instance, the complete and accurate identification of one of the bosses was obtained thanks to an intercepted telephone conversation on 11 April 2007, during which the person under investigation contacted a car dealer and asked for information concerning the transfer of ownership of a Porsche Boxster motor car purchased a few weeks previously. A further investigation into the ownership of the car showed that it belonged to the wife of the person under investigation, and he had underwritten, in her name, the insurance for the car. The operators of the the Guardia di Finanza - Gruppo Pronto Impiego (judicial police) investigated the credit card used for the payment of the premiums of the insurance, and the mobile telephone number given to the bank when the current account was opened that was linked to the credit card. They not only made use of false documents, but one shop in Milan, prepared not to ask questions, provided numerous SIM cards which were registered to fictitious Greek citizens.

The mistake that led to the arrests

The plan devised by the criminals was perfect in theory, as in the film 'The Italian Job',[6] when to achieve their purpose, the English criminal gang manipulated the computers that controlled the traffic lights in Turin, causing the traffic to stop moving through the city, enabling the thieves to effect an agile escape from the Italian police. In this instance, and for a very short period, the criminal association committing the crimes used the same SIM card to carry out their illegal activities via the internet as well as for the conversations between the people taking part in the crime. This mistake enabled us to intercept these

[4] The prepaid 'Postepay card' is a payment or withdrawal instrument that can be used in two ways: either Postamat or Visa Electron. One of the characteristics that make a Postepay card different from the other credit cards, is that they can be issued to the person requesting them, even if the latter does not have a current bank account.

[5] A number of people continuously offered important contributions to the investigation, under the direction of Major Edoardo Viti: Chief Mar. Davide D'Agostino (Commander of the Section, who moreover materially drafted most of the Judicial Police's informative reports), Chief Mar. Giuseppe Gorgoni, Mar. Stefano Santoro and the Lance-Corporal Massimo Raone.

[6] Written by Troy Kennedy Martin, produced by Michael Deeley, directed by Peter Collinson, music composed by Quincy Jones, and released in 1969, starring Michael Caine and Noel Coward.

fellows (since we identified an IP address used by them for the illegal operations over the internet) and to continue the investigation successfully. It was for this reason that the operation was called 'Phish & Chip'.[7] A mixture of house searches, telephone interceptions and the analysis of the content of internet chats that occurred among the various targets in Italy and Romania during the first phase of the investigation guaranteed a precious collection of digital evidence and important confirmation relevant to the investigative hypothesis.

Execution of warrants of arrest

Five months after the operation began, in July 2007, the Guardia di Finanza executed 26 warrants of arrest for those people belonging to the two criminal associations that took advantage of the home banking service personal access codes of the customers of Poste Italiane,[8] and Banca Intesa, one of the most important banks in Italy. The judge for the preliminary investigations, Guido Salvini, indicated in the order of custody, that this is:

> ... (l'attività) condotta dalla Procura di Milano e svolta grazie ad accertamenti assai complessi, vista la materia trattata, svolti con grande impegno dal Gruppo Pronto Impiego della Guardia di Finanza di Milano, costituisce forse il primo tentativo di affrontare in modo organico sul piano investigativo ed anche contestando reati associativi il fenomeno delle organizzazioni criminali dedite sistematicamente all'attività di phishing
>
> ... (activity) conducted by the Prosecutor of Milan and carried out through very complex investigation, given the subject matter, conducted with great commitment by Gruppo Pronto Impiego of Guardia di Finanza di Milano, is perhaps the first attempt to face the phenomenon of the criminal organizations apt to the systematic attempt of phishing in an organic manner, both from the investigative point of view and also contesting offences of association.

The operation received unexpected media coverage that went beyond Italy,[9] and it was described on Italian television as 'one of the most important Information Technology investigation in Europe in the last years'. The following charges were brought against 26 people: criminal association, falsification of IT communication content, unauthorized access to IT systems, aggravated fraud, unauthorized use of credit cards.[10]

The closure of the first investigation

All the members of the first of the two criminal organizations had been living in Italy for a number of years. The information system hacker of the first group was a 22 years old Romanian boy. During his questioning at the office of the Prosecutor, which lasted most of the night, he confessed to sending e-mails as if they had been sent by Poste Italiane, and to collecting the data belonging to victims with e-mail addresses of providers operating in Italy, but with servers based abroad. The computer forensic analysis confirmed his confession. Covering the four months of this first phase of the investigation, fraudulent activity amounting to 250,000.00 euro was discovered by the investigators.

The continuation of the investigation

In April 2007, the investigators knew that the main person responsible for the second organization was returning to his home in Craiova, Romania. It was extremely important to ensure there was excellent cooperation between the Milan, Bucharest and Craiova judicial authorities.[11] The investigation was headed by the commissary, Silviu Vacaru, who ensured the efficient coordination and cooperation between the Italian Guardia di Finanza and the Romanian police. We asked for and obtained, using the necessary rogatory, the

[7] In fact everything starts from the SIM card: its internal chip gathers information that is updated by the mobile telephone company. The information contained in the chip provides a great deal of data about the life of the SIM card: external data concerning the calls and internet connections made with the SIM card – that is, everything apart from the name of the real holder, because in Milan – as was shown (again) by this investigation – it is possible to purchase false SIM cards activated in the name of a third party at a very low price close to the subway stations or in the area around the central railway station.

[8] During the first quarter of 2007, according to the quarterly report concerning the phishing phenomenon in Italy and drafted by Anti-phishing Italia, the phishing attacks on the Poste Italiane current account holders represented 87.11 per cent of the total attacks in Italy: http://www.anti-phishing.it.

[9] For instance, see John Leyden, ' Italian police net 26 in phishing takedown' The Register, 16 July 2007, on-line at http://www.theregister.co.uk/2007/07/16/phish_chip_arrests/.

[10] Article 416 of the Italian Criminal Code (Codice Penale) - Associazione per delinquere (criminal association); Article 617-sexies of the Italian Criminal Code (Codice Penale) - Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (falsification of IT communication content); Article 615ter of the Italian Criminal Code (Codice Penale) – Accesso abusivo ad un sistema informatico o telematico (unauthorized access to IT systems); Article 640 paragraph 2 of the Italian Criminal Code (Codice Penale) – truffa (aggravated fraud); Article 55 paragraph 9 of the Legislative Decree (Decreto Legislativo) 21.11.2007 n. 231 (unauthorized use of credit cards).

[11] The investigation was headed by the commissary, Silviu Vacaru, who ensured the efficient coordination and cooperation between the Italian Guardia di Finanza and the Romanian police. I must here mention the sensitivity shown by Florentina Longu, Chief Prosecutor of the Investigative Direction for crimes of organized crime and terrorism at the Dolj territorial Office, as well as of Prosecutor Adrian Gluga.

interception of communications in Romania.[12]

The exchange of information, often in real time, between the investigators in Craiova and the officials of the Guardia di Finanza in Milan, turned out to be of vital importance for the identification and the subsequent capture of the main person responsible, together with a number of fugitives who escaped to Romania during the July arrest. In the second phase of the operation, money flows from Italy to Romania had been analyzed and rebuilt: this enabled the fees that were paid to the technical experts who participated in the crime to be identified.

The two young Romanian phishers arrested

Using the result of the Romanian interceptions, in October 2007 the first of the two young Romanian phishers was arrested in Craiova. Extradited to Italy,[13] his declarations were also useful to arrest a second young man, who was much more expert and better than him. In fact, they needed to 'empty' a bank account of 100,000.00 euro, and so they called another phisher, well known in the young criminal underground because he successfully took part in the Romanian Information Technology Olympic Games in 2004. Besides this, we arrived at his definitive identification because his details were still available over the internet at the material time.[14] At this point, after having the confirmation of the exact identification data from the Romanian judicial authorities, another European arrest warrant was requested – on 13 December 2007 – which was issued by the judge for the preliminary investigation on 19 December 2007. Less than ten days later, the young phisher was found at his house in Craiova and arrested. The images which document the results of the search carried out in Craiova speak for the young boy's criminal capacities: a net connected laptop, which was still working on a chat-session, with a collection of computer programs on CDs, well-catalogued together with a large number of credit cards, and near his monitor ... there was a gun! In order to take the young 'Olympic man', currently held in Como Prison, back to Craiova, the Italian press report that 'a powerful Romanian information technology industrialist is taking action'.[15] There is no further up-date at the time of writing this article.

For the first time in a phishing case, the rules of the Italian law[16] that ratified the United Nations Convention against Transnational Organized Crime, were applied.

Conviction

During December 2007, for the first time in Italy, Piero Gamacchio, the judge for the preliminary hearing, entered a verdict of guilty regarding two transnational criminal associations accused of committing offences of phishing. The main person that was responsible, arrested by the Military Financial Police in Milan after an escape attempt that lasted twelve hours, was sentenced to imprisonment for six years. The penalty was considerable, considering the accused decided to accept the summary procedure, which provides that the judge will decide the case on the basis of the investigation, and therefore without hearing the witnesses in court, but with a reduction of one third of the penalty if found guilty.

After an investigation that lasted one year, in April 2008 we had the first verdict of guilt in respect of two young Romanian men who were operating directly from Romania as an important element in the criminal

[12] *I must here mention the sensitivity shown by Ioana Albani, Chief Prosecutor of the Cybercrime Unit at the General Prosecutor's Office – Investigative Direction for crimes of organized crime and terrorism in Bucarest, as well as of the Chief Prosecutor Daniela Matei and of the Prosecutor Narcisa Danes. The investigation was carried out by the General Inspector of the Rumanian Police – Service for the contrast of IT criminality, headed by Virgil Spiridon.*

[13] *By virtue of article 6, paragraph 2 of the Italian Criminal Code (Codice Penale), there is Italian jurisdiction where the actions of the accused acted in the pursuit of the crime were partly carried out in Italy. In this respect, he obtained illegal accesses into Italy technically through the internet into IT systems that physically existed within the territory of the State, from where he then ordered the later transfers of money.*
Art. 6 Reati commessi nel territorio dello Stato
Chiunque commette un reato nel territorio dello Stato e' punito secondo la legge italiana.
Il reato si considera commesso nel territorio dello Stato, quando l' azione o l' omissione, che lo costituisce, e' ivi avvenuta in tutto o in parte, ovvero si e' verificato l' evento che e' la conseguenza dell' azione od omissione.
Art.6 crimes committed in the territory of the State
Anyone who commits a crime in the territory of the State is punishable under Italian law.
The offense is considered committed in the territory, where the action or the omission that constitutes the offense, has occurred in whole or in part, or is the consequence of the action or omission.

[14] *At http://olimpiadi.info/oni2004/partecipanti/partecipanti.htm but this URL is no longer active.*

[15] *See P. Pioppi, 'Tenta una serie di truffe in Rete Genio dell' informatica arrestato' ('Tries to commit a series of crimes on the net. IT Genie arrested') in Il Giorno, 17 June 2008; L. Grilli, 'Como, mago della truffa in cella Bucarest: liberatelo, è un genio' ('Como, genie of fraud in prison. Bucarest: free him, he is a genius') in Il Giornale, 18 July 2008. Both articles are available at: http://ilgiorno.ilsole24ore.com/como/2008/06/18/97804-tenta_serie_truffe_rete_genio_dell_informatica_arrestato.shtml; http://www.ilgiornale.it/a.pic1?ID=269857.*

[16] *Legge 16 marzo 2006, n. 146, Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall' Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001 (pubblicata nella Gazzetta Ufficiale n. 85 dell' 11 aprile 2006 - Supplemento ordinario n. 91) (Law of 16 March 2006, n. 146, Ratification and implementation of the Convention and Protocols of the United Nations against Transnational Organized Crime, adopted by the General Assembly on 15 November 2000 and May 31 2001 (published in the Official Gazette n. 85 of 11 April 2006 - No Ordinary Supplement 91)).*

environment: they were arrested in Craiova at the end of the year and extradited to Italy following the issuance of a European Arrest Warrant. Both men faced identical charges to those set out in footnote 10 above, and received a sentence of thirty-seven months imprisonment, a sentence that took into account their youth and the fact that they were the only ones to return a symbolic part of the money (5,000.00 euro each),[17] thanks to the financial contribution of their respective families, payments were made to the customers of the banks, rather than to the banks.

An important aspect for the success of the prosecution was to simplify the technical evidence to help the two judges (Guido Salvini and Piero Gamacchio) understand the nature of the evidence. The judges are among the most authoritative in the court in Milan, because they have experience of dealing with a number of significant trials, including trails against the mafia and in relation to Italian terrorism. The judgment comprises 150 pages, the counts on the indictment occupying the first fifty pages.[18]

Lessons

Finally, it will be useful to underline a few final remarks. First is what I call the agile cooperation model between the police force and legal authorities, which also happens in real time and is therefore capable of improving the efficiency of the investigation. This is what happened in the Phish & Chip operation, partly thanks to the role of Eurojust,[19] which allowed an even faster data exchange among the investigators. Second, when dealing with cyber frauds, it is not only necessary to use computers, but a strategy for investigation must be considered. Traditional methods of investigation are used, including: profiling the cybercrime, telephone interceptions, lying in wait and money flow analysis. Only after, and not before or instead of these methods, can computers and other tools be used to further the investigation.

Finally, I still remember the words of the 'Olympic champion' during his last interrogation:

> I did the activities so far described on my computer, which I had in Craiova. I've never thought that in that way I could be traced, as I used a program, free, provided by America On Line and utilized to have American On Line's servers as proxy, so that all my internet navigations were referable to an American IP.

Never say never. If the computers can be programmed to remain silent, this does not very often happen with the partners you share in such an adventure. Well, reflecting on the film 'The Italian Job' as an amusing allegory of the fight between evil and good, what really counts is the investigative ability of the police and prosecutor, more than the technical potential of machines (to oppose the machines of the cyber criminals). As investigators, we surely have less powerful computers but, as for the rest, and as the English singer Alesha Dixon has sung, 'Italians do it better'!

Francesco Cajani is a Deputy Public Prosecutor in the High Tech Crime Unit at the Court of Law in Milan. He is also member of the Technical and Scientific Committee of IISFA (International Information Systems Forensics Association) – Italy Chapter (http://www.iisfa.eu).

francesco.cajani@giustizia.it

[17] *In two months they managed to withdraw 67,000.00 euro (only using Postepay cards). Regarding the first association, the investigation ascertained that almost 96,000.00 euro of illegal recharges had taken place (of which 94,000.00 euro were withdrawn); in respect of Intesa flash cards, more than 60,500.00 euro in illegal recharges had taken place (almost all this was withdrawn).*

[18] *Sentence no. 2650/07 dated 10 December 2007, filed on 29 March 2008. See the comment by R.FLOR, Frodi identitarie e diritto penale (' Identity fraud and criminal law') at http://www.penale.it/page.asp?mode=1&IDPag=730.*

[19] *During the investigation there were twelve supplements of the first request of Mutual Assistance dated March 2007, all of them were executed in relatively a short time; also thanks to the positive help given by Eurojust, in the person of Carmen Manfredda, Deputy to the Italian national representative, and of Elena Dinu, the Romanian national representative.*

ARTICLE:

INTERCEPTION OF COMMUNICATIONS: SKYPE, GOOGLE, YAHOO! AND MICROSOFT TOOLS AND ELECTRONIC DATA RETENTION ON FOREIGN SERVERS: A LEGAL PERSPECTIVE FROM A PROSECUTOR CONDUCTING AN INVESTIGATION[1]

By **Francesco Cajani**

A space is not without law just because it is cyber

In cyberspace, the traditional country borders are cleared during the actions of the cyber criminal. The borders return later, when the detectives try to trace the actions of the criminal or terrorist, searching digital evidence possibly left by the author, and so useful for the investigation. The main problem (it is even a cultural problem), is, as all detectives know, that cyberspace favours the suspects. Each time a cyber crime is reported across jurisdictions, it is necessary to ask the States affected to collaborate with the investigation, usually through a formal rogatory. Of greater importance, are the businesses providing electronic services with servers in another State, and whose servers and services the criminal act has used in some way. In theory, it is conceivable that a commercial entity will be nimble in responding to a legitimate request from another State to collaborate in tracking down a criminal. But this does not happen. The commercial sector moves at a far slower pace than our counterparts across the world. Invariably, a barrier is immediately erected to any request with the excuse that they cannot help because it is not possible according to domestic law. This is what usually happens in relation to the electronic services provided by three of the most important internet businesses: Google, Yahoo! and Microsoft. The difficulty with intercepting the flow of communications in reasonably short time is a general problem, and it does not only apply to Skype.[2]

'No server no law' v 'no server but law'

We more often find ourselves dealing with opinions that differ. On the one side, there is the 'no server no law' view. Preference is given to the geographical location where the web servers are based: and often, the servers are outside the European Community. This is the case in respect of Google, Yahoo! and Microsoft. This first point of view considers that national or European laws cannot be enforced because the web servers are in the United States of America. Of interest, regarding Skype, the servers could not be precisely identified (and therefore not intercepted), since they are organized as peer-to-peer nodes. On the other side, there is the opinion that I prefer, the 'no server but law' opinion. This view considers that the crucial point is the geographical location where the web services are offered, no matter where the web servers are, even for the purposes of law enforcement. As I usually say, *the server may be elsewhere, but the mouse is in Italy.*

[1] *This article is adapted from the speech of the author at the First Strategic Meeting on Cybercrime organised by Eurojust in Athens, 23-24 October 2008 (many thanks to Luisa and Valeria Viganò for the review). For the press release, see http://www.eurojust.europa.eu/press_releases/2008/30-10-2008.htm.*

[2] *Declan McCullagh, 'Skype: We can't comply with police wiretap requests', cnet news, 9 June 2008, available at http://news.cnet.com/8301-13578_3-9963028-38.html.*

Three scenarios

Essentially, there are three scenarios that affect the investigation of alleged crimes that include the use of networked communications. They can overlap, but the three that we need to consider can be divided into the availability of encrypted communication technology, the communication channel and communication data. Each are considered in turn below. The Italian law regulates each scenario in a different way, and there are no reported decisions in relation to these matters at the time of writing. An important problem regarding each of these is also the length of time the data is retained.

The availability of encrypted communication technology

In the case of Skype and other Voice over Internet Protocol (VoIP) communications generally, the communication is encrypted. It is only possible to intercept a VoIP communication only when the investigating authority knows the exact location of the suspect's computer. The investigating authority will try to obtain access to the computer and install a program to enable interception to take place, and where it is not possible to reach the computer physically, social engineering techniques will be used to achieve the same aim. Naturally, it is only possible to undertake these actions with the authorization of a judge.

The availability of a communication channel

The vast flow of communications between people is now through e-mail systems. Often, the people under investigation are present in Italy, but they might use an e-mail system based abroad, such as Google or Microsoft: this occurs frequently, hence the reference to the 'no server no law' opinion. In fact it was not possible in this case to enforce an order issued by the judge. The order that could not be enforced, requested that the e-mail accounts be intercepted by having the e-mail traffic redirected to the judicial police account. This method reduces costs, and permits the interception to begin quickly. This method is used when making similar requests to the national ISPs with servers in Italy. The alternative mechanism is for the judicial police to notify Google Italia or Microsoft Italia (both with registered offices in Milan) of the interception order. However, their response is to indicate that the servers are in the United States of America, and they request a rogatory before they will implement the interception order. This is not good if the investigation concerns a murder or a kidnapping. The situation is the same as with Skype – it is almost impossible to intercept communications. Only Yahoo! Italia (their registered office is in Milan) has an item of software called 'Yahoo! Account Management Tool'. This software allows e-mail to be intercepted, but it is of limited help.

The availability of communication data

This scenario refers to data relating to the use of the internet, such as log files. In the experience of some Italian investigation agencies, Microsoft Italia was the first to provide – without a rogatory but only with a request from the Italian Public Prosecutor – such data, not only referred to @hotmail.it e-mail, but including @hotmail.com. At first, Google Italia considered it was necessary for a rogatory, but they changed their policy, and now provide all the data requested, providing the request is accompanied with an order from the Italian Public Prosecutor (not only from the Italian Judicial Police). Nevertheless, if an IP address (logged by the Google electronic systems with regard to an e-mail *@gmail.com*) is not related to an Italian server, Google does not consider it is permitted to communicate it to the Italian Judicial Authority. In comparison, Yahoo! Italia request a rogatory, but only in some cases.

Preliminary matters

In order to be better prepared to investigate alleged crimes, investigators have had to assemble lists of relevant information in relation to each Internet service provider (ISP), including: where the web servers are physically located; where the registered office of the ISP is located, and if the ISP has an operating branch in the State where the investigation is conducted. It is also necessary to know (in order to verify potential criminal liability) if the employees in the operating branches are in effective control of the local affairs of the ISP, or whether they are mere legal representatives.

Jurisdiction analysis as applied in the United States of America

If the 'no server no law' opinion is accepted, it will be interesting to know what view an American judge would take. The scenario is as follows: the ISP is an American company which also has a physical base in Europe and offers its services to European citizens; the ISP insists that their web servers are in one of the US states, for example in California, and as a result, the ISP is not

The closer the internet activities are to 'clearly conducting business', the more likely that a US court will exercise personal jurisdiction.

subject to the laws of the Member State in which they have an office. The same could be argued in reverse. An Italian ISP uses the identical argument to a Federal court in the US, that is: 'sorry, but our servers are in Italy'. Or, the same American company with servers in California summoned in a different US Court (for example: Arizona). It is debatable whether a US judge will accept such an argument. Consider how the judges in the US analyse internet jurisdiction.[3] Judges in the US 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.[4] The second analysis, called the 'effects test', seeks to determine to what extent a defendant's intentional conduct takes place outside the forum State.[5] So, for a number of years, the US state courts have been using an undisputed analysis, providing for US jurisdiction, even if the web site is based on a server in another country. This means that a foreign internet entrepreneur, although lacking 'continuous and systematic' contacts with any US forum state sufficient to subject him or her to general jurisdiction, may nonetheless be subject to personal jurisdiction in the US based on two broad theories of 'specific' personal jurisdiction. Under the *Zippo* 'sliding scale' analysis, a US court will classify the 'nature and quality' of any commercial activity that is conducted 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 US court will exercise personal jurisdiction. Courts may also apply the *Calder* 'effects test' to determine whether the intentional conduct of the party was calculated to cause harm to the plaintiff within the forum state. Where a defendant 'purposefully directs' his activities towards the jurisdiction, he may be liable to legal action for any injury relating to or arising from those activities.

Obligations and national laws to observe

At this point, the important question is to identify the obligations and national laws that we can be expected to observe. In Italy, the provisions of Decreto legislativo 1° agosto 2003, n. 259, Codice delle comunicazioni elettroniche[6] (Legislative Decree of 1st August 2003, n. 259 electronic communication rules) are fundamental. These rules have their origin in four EC Directives.[7] An important step has been taken by the Italian Ministero dello Sviluppo Economico (Ministry of Economic Development and Telecommunication), in that it has recently provided a written opinion (note of 12 September 2008, following a specific request of the Direzione Nazionale Antimafia) according to which Skype connections must be included in the electronic communication rules and are therefore subject to the general authorization provided by the law.

Consequently this involves the observance of the rules about the compulsory services required by the judicial authority and, in particular, to enable a legal interception to take place by competent national authorities, as also set out in article 6 of EC Directive 2002/20/EC, the Authorisation Directive:

[3] *G. J. H. Smith, Internet law and regulation, (Sweet and Maxwell, 3rd edition, 2002), 347-349.*
[4] *Zippo Manufacturing Co. v Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa.1997).*
[5] *Calder v Jones, 465 U.S. 783 (1984).*
[6] *Pubblicato sulla Gazzetta Ufficiale n.214 del 15 settembre 2003.*
[7] *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), OJ L 108, 24.4.2002, p. 7; 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), OJ L 108, 24.4.2002, p. 21; 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 ("the Framework Directive"), OJ L 108, 24.4.2002, p. 33; 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), OJ L 108, 24.4.2002, p. 51.*

> 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. Such conditions shall be objectively justified in relation to the network or service concerned, non-discriminatory, proportionate and transparent

The relevant condition listed in the Annex is item 11:

> 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.

The combination of article 6 and paragraph 11 of the Annex could mean: if, for instance, in the future Skype decides to open a branch in Italy, this will be sufficient market conditions to enable Italian investigating authorities to require Skype to intercept communications if ordered so to do.

Secondly, we could expect the observance of the data retention rules (Decreto legislativo 30 maggio 2008, n. 109 – Legislative Decree of 30 May 2008, n. 109).[8] The provisions of articles 3 and 6 of Directive 2006/24/EC are relevant, and provide as follows:

> 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 communication 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 elephony 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.

It is clearly the opinion of Peter Schaar, President of the Article 29 Data Protection Working Party, that any EC rules can be applied to the organizations that turn their attention to provide services to European citizens:

> '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 centre'[9]

It therefore follows that the obligations of data retention also apply to Google, Yahoo! and Microsoft.

Finally, it is to be observed that the United States of America ratified the Council of Europe Convention on Cybercrime (Budapest, 23.XI.2001) on 29 September

[8] *Based on 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, OJ L 105, 13/04/2006 P. 0054 – 0063.*

[9] *Letter from Peter Schaar to Peter Fleischer dated 16 May 2007, D(2007) 6016, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf.*

2006, which provides for two precise obligations of cooperation in articles 33 and 34:

> Article 33 – Mutual assistance regarding 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.
>
> 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 recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Therefore, when a State such as Italy ratifies the Convention,[10] specific duties arise. As the ancient Romans said, and as the rules of international law remind us: agreements must be kept (pacta sunt servanda).

In particular, whereas US ISPs continue to consider that EU laws do not apply to them, the national judicial authorities will continue to act within the law in a reasonable and proper way[11] and will insist for an action[12] not only of the European administrative authorities, of the US authorities, even if it is necessary to enforce the 2001 Council of Europe Convention on Cybercrime.

Yahoo! Italia and the Public Prosecutor's Office in Milan

In 2007, the Public Prosecutor's Office in Milan had some difficulty with Yahoo! Italia around the 'Net Citizenship' concept. That is: when an Italian user registers an account from the webpage www.yahoo.it, he can choose which law his e-mail correspondence will be subject to. There is an item of software called Yahoo! Account Management Tool, which is used by all the Yahoo! branches. It returns the communications stored in e-mail boxes (@yahoo.it and @yahoo.com or both), but only in respect of those users that agree that Italian law applies. The investigation authorities can intercept these e-mails, even without a rogatory. However, these e-mails only have a retention period of between 30 and 45 days, against a period of twelve months.[13] As a result, some investigations suffer. One occasion, a Yahoo! mail box was the subject of interception without any results. This meant that no e-mails were received at all. The investigators could see that no e-mails were received. The suspect, a Romanian phisher, was arrested. He provided the access credentials to the mail box that had been intercepted. It was discovered that there were a number of messages that had been received in the period when the mail box had been subjected to interception. During the period the mail box was the subject of interception, a great number of Yahoo! employees were free to enter the Yahoo! Account Management Tool from several of the European branches of Yahoo! This fact could damage the users' privacy, and not only the police investigation. The indictment was transferred to the Garante per la protezione dei dati personali (Italian Privacy Authority), who confirmed the technical investigation and that the

[10] *The Convention was signed by Italy on 23 November 2001, ratified on 5 June 2008, in force on 1 October 2008; Legge 18 marzo 2008, n. 48 Ratifica ed esecuzione della Convenzione del Consiglio d' Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell' ordinamento interno (Pubblicato sulla Gazzetta Ufficiale 4 aprile 2008, n. 80; s.o. n. 79) (Law of 18 March 2008, n. 48).*

[11] *On 2 March 2009, a court in Dendermonde, Belgium, found Yahoo guilty of withholding personal account information linked to Yahoo e-mail addresses. This decision is in the process of being appealed. Note from the editor: it is antipicated that a full report on this case will be included in the 2010 issue of the journal.*

[12] *According to Article 10 of 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 OJl L 105, 13/04/2006 P. 0054 - 0063, 'Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include ... the cases where requests for data could not be met'. See also Decreto legislativo 30 maggio 2008, n. 109, which provides fees from 50,000.00 to 150,000.00 euros for failing to retain data for 12 months.*

[13] *In accordance with 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, OJ L 105, 13/04/2006 P. 0054 – 0063; implemented by Decreto legislativo 30 maggio 2008, n. 109.*

legal approach taken by us was correct. Meanwhile, the attorneys for Yahoo! Italia indicated to the Public Prosecutor's Office in Milan that the company would spontaneously conform to Decreto legislativo 30 maggio 2008, n. 109, by storing log files for twelve months in future.[14] Apparently this will be enforced across all EC states, and started from 21 November 2007. In my opinion, it could not be different: we are in presence of societies which must be included in the provisions of article 3 of Directive 2002/58/EC:[15]

> 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.

It is for such reasons, and independently from where the servers are physically located, they are required to comply with the obligations of the Italian and EC data retention rules.

Concluding comments

In conclusion, let me take a strictly personal view: each time I manage to come to Athens, I like to have a walk through the Agorà and go as far as the Monument of the Eponymous Heroes: this is the place where the legislation, decrees and announcements were shown, so that the Athenian citizens could see and know them. Well, today we have a lot of 'shown' laws, yet there are many people who pretend not to see them, hiding behind a 'cyberspace virtuality'. But this very cyberspace not only feeds such companies with their profits, but facilitates crime. There is a need to balance the rights of people that are the victims of a crime, against the econimics of the ISPs. The words by which the historian Herodotus of Halicarnassus described what Demaratos said of the Lacedemonians are relevant:[16]

> 'So also the Lacedemonians are not inferior to any men when fighting one by one, and they are the best of all men when fighting in a body: for though free, yet they are not free in all things, for over them is set Law as a master, whom they fear much more even than thy people fear thee. It is certain at least that they do whatsoever that master commands; and he commands ever the same thing, that is to say, he bids them not flee out of battle from any multitude of men, but stay in their post and win the victory or lose their life.'

Many commentators have seen in this affirmation the first statement of that 'Government of the Law', according to which the existence of a law distinguished the Greeks from the non-Greeks, and for this reason defined 'barbarians': therefore, in those times, for the Greeks:[17]

> Du Démarate d'Hérodote au Platon de la lettre VII, en passant par le Thésée d'Euripide, la tradition est bien la même. Elle implique un sens aigu de cette loi comune que les citoyens avaient su se donner et dont ils attendaient à la fois le bon ordre et la liberté. Pour eux, déja, la liberté se définissait comme l'obéissance aux lois.
>
> Of Démarate from Herodotus to Plato of letter VII, while passing by Theseus of Euripides, the tradition is the same. It implies an acute sense of this common law that the citizens had known to be given and from which they expected to both order and freedom. For them, freedom is already defined as obedience to the laws.

Today, we often talk about the internet as a space of freedom. As a Public Prosecutor, who is fond of information technologies, my wish and my hope is that this 'freedom' can really come true. The danger of a different concept of freedom, meant as the absence of laws, is a barbarity to be opposed.

Francesco Cajani is a Deputy Public Prosecutor in the High Tech Crime Unit at the Court of Law in Milan. He is also member of the Technical and Scientific Committee of IISFA (International Information Systems Forensics Association) – Italy Chapter (http://www.iisfa.eu).

francesco.cajani@giustizia.it

[14] *The Request for Archiving (not to prosecute and to close the case) was submitted to the court on 16 October 2008, and agreed by the judge, Dr Gaetano Brusa, on 25 March 2009. The Request is published at the end of this article.*

[15] *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), OJ L 201, 31.7.2002, p. 37–47.*

[16] *The Histories, VII, 104. (Translation of G. C. Macaulay, available at http://www.gutenberg.org/files/2456/2456-h/book7.htm).*

[17] *Jacqueline de Romilly, La loi dans le pensèe grecque, (1971, Belles letters, Paris), 23.*