

**Project on Cybercrime**  
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)



Economic Crime Division  
Directorate General of  
Human Rights and Legal Affairs  
Strasbourg, France

Version 25 June 2008 (FINAL)

**Cooperation between  
law enforcement and  
internet service providers  
against cybercrime:  
towards common guidelines**

Prepared by  
Cormac Callanan (Ireland)  
Marco Gercke (Germany)

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

## Contact

For further information please contact:

Economic Crime Division  
Directorate General of Human Rights and Legal Affairs  
Council of Europe  
Strasbourg, France

Tel: +33-3-9021-4506  
Fax: +33-3-9021-5650  
Email: [alexander.seger@coe.int](mailto:alexander.seger@coe.int)

This study does not necessarily reflect official positions of the Council of Europe or of the donors funding this project

## Contents

<b>1</b>	<b>Introduction.....</b>	<b>4</b>
1.1	Scope of the study .....	4
1.2	Overview.....	5
1.3	Why create the study? .....	6
1.4	Structure of the study .....	9
<b>2</b>	<b>Background.....</b>	<b>10</b>
2.1	Illegal activity on the Internet.....	10
2.2	Legal/regulatory response .....	15
2.3	Profile of Internet service industry.....	17
2.4	Profile of law enforcement agencies.....	28
2.5	Current relationships .....	32
<b>3</b>	<b>Working together/ processing requests.....</b>	<b>41</b>
3.1	Processing data-related Requests .....	41
3.2	Analysing different kind of requests.....	43
3.3	Carrying out search and seizure procedures.....	48
3.4	Interception and collection of data.....	51
3.5	Additional instruments .....	53
3.6	Exchange of knowledge and expertise.....	55
<b>4</b>	<b>Issues which arise .....</b>	<b>57</b>
4.1	General issues .....	57
4.2	Bad practices.....	58
4.3	Conclusion.....	59
<b>5</b>	<b>Guidelines .....</b>	<b>60</b>
<b>6</b>	<b>Conclusion .....</b>	<b>67</b>
	<b>Appendices.....</b>	<b>68</b>
	<b>Appendix 1 – Working Group Members .....</b>	<b>69</b>
	<b>Appendix 2 - Relevant Legal Instruments .....</b>	<b>70</b>
	<b>Appendix 3 - Extract procedural provisions of the Convention on Cybercrime.....</b>	<b>73</b>

# **1 Introduction**

## **1.1 Scope of the study**

The idea of launching the present working group came out of the work of the "Project against cybercrime". This project, launched in September 2006 is currently funded from the budget of the Council of Europe and a voluntary contribution by Microsoft Corporation.

It is the view of the Council of Europe that participants of the first meeting of the working group have already demonstrated through their day-to-day work with law enforcement authorities a willingness to support them in the fight against cybercrime, to the extent they practically and legally can. This support has taken the form of the establishment of processes or policies in responding to legal requests from law enforcement authorities ("criminal compliance"), or in responding to other types of requests on the development of trainings and tools for law enforcement.

A working group was established to support the drafting of a study regarding the cooperation between law enforcement agencies and providers. The output of the study will be a set of guidelines aimed at improving the cooperation between law enforcement agencies and service providers against cybercrime based on good practices or processes already established by industry, both in terms of criminal compliance and in terms of other types of cooperation.

The guidelines should function as a policy paper for requests for cooperation against cybercrime generally but also provide very practical guidance on criminal compliance to law enforcement and service providers of all sizes and all countries. For example, advising ISPs that it is a good practice to provide a designated point of contact to handle the relationship with law enforcement, or advising law enforcement that it is good practice to train their personnel on which information and how to request information from ISPs, and understand the differences between them. Other examples would be reminding ISPs that they have to define which law is applicable to the request, that it is good practice to provide guidance to law enforcement on how to make a request, that ISPs should articulate what information they are able to provide and disclose, whether they have after hours emergency procedures or not, reminding law enforcement that they should - to the extent possible - limit the interactions with ISPs to trained personnel, and where possible prioritize their requests so that the service providers may address those that are most important first. etc.

These guidelines may subsequently become a Recommendation, that is, a soft law instrument of the Council of Europe. It is obvious that cybercrime investigations will need to be based on legal regulations established by the applicable laws of each country. The guidelines are not designed to substitute the existing legal structures but to give basic guidelines with regard to their application and are subject to all aspects of national law.

The study is focusing on the international standards defined by the Convention on Cybercrime. Due to the differing national legal standards and a lack of detailed comparative law analysis in this field it is necessary to draft the guidelines on criminal compliance on a level that is concrete and precise enough to be applicable in carrying out investigations on the one hand side and to be abstract enough to ensure

that the guidelines are not in conflict with existing legal standards. The guidelines should also provide a framework for cooperation against cybercrime in general.

## **1.2 Overview**

The Council of Europe Cybercrime unit is often approached by international parties to describe what should the ideal relationship between law enforcement and Internet industry be. This study should provide valuable guidelines in this area.

The study reflects the good / common practices which have already been developed in some countries but endeavours not to be country specific. The guidelines are designed not to create substantial burdens on either party since the relationship between Law Enforcement and Internet Industry needs to operate smoothly and efficiently in both directions.

### **Bidirectional Communication**

Analysis systematic structures of the cooperation shows, that it is bidirectional in nature:

- Law Enforcement is on the one hand responsible for the prevention and investigation of crime and on the other hand knowledgeable on cybercrime trends.
- Internet industries are on the one hand victims of crime and on the other hand knowledgeable about some cybercrime trends and hold data about their customers who are perpetrators or victims of criminal acts.

### **Legal Framework**

Generally the Internet industry and Law Enforcement Agencies (LEAs) recognize a common interest in the prevention, detection and investigation of cybercrime and threats to national security and information infrastructure generally. Online safety, security and reliability of the internet are dependant upon early detection of criminal activity that might undermine the achievement of these objectives. However, this requires effective legislation that is balancing investigation instruments and fundamental rights as the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities.

This requires all parties to act in the respect of established principles that ensure a balance between Rights, stated in the Convention for the protection of Human Rights and Fundamental Freedoms. This is especially true of "qualified rights" such as the right to respect for private and family life and freedom of expression. These can only be restricted if a clear legal basis states this possibility, if the restriction seeks to achieve one of the legitimate aims set out in the Convention and if the action is necessary in a democratic country, which means that the action must be in response to a "pressing social need" and must be no greater than that necessary to address the social need (proportionality principle).

The purpose of the study is to develop guidelines that support the cooperation within the given legal framework. It does not intent to develop new legislative approaches. In addition study will *not* focus on issues associated with data retention or data protection which are covered extensively in other studies and documents. It will

focus on the relationship between Law Enforcement and Internet Industry in relation to cybercrime issues and will not deal with the relationship of either party with other parties relating to other types of content investigations.

#### 1.2.1 Working Group

The working group includes member with different backgrounds (provider/law enforcement, industry/public sector and practitioner/academic).

In order to ensure that the recommendations are applied in the every day work of cooperation, it is necessary that representatives of all relevant areas are involved. The involvement of associations that represent a significant number of businesses in relevant areas is essential as their input will be able to support the acceptance of the recommendations within the businesses they represent.

#### 1.2.2 Who will the guidelines help

The guidelines are designed to help Law Enforcement at a national and international level to understand best of breed relationship structures which work with Internet Industry around the world.

The guidelines are also designed to help Internet Industry to understand best of breed relationship structures which work with Law Enforcement Agencies around the world.

### 1.3 Why create the study?

There are no globally applicable comprehensive descriptions available which outline how law enforcement agencies and personnel can interact with internet industry organisations and personnel during the course of a cybercrime investigation.

#### Few guidelines for cooperation

Regarding criminal compliance specifically, there is a lack of clarity on the very *concept* of cooperation between industry and law enforcement agencies. Often the perception is that it is purely a *legal* issue when a law enforcement agency requests customer related data which is needed for an investigation from an ISP. If law enforcement has legally the right to obtain information, it will obtain it. In other countries, typically in North-America, industry must also define and publish its privacy policy as part of its business ethos which in turn has an impact on the level of information it can share with law enforcement agencies without breaching this ethos.

#### Raising awareness for fundamental principles of cooperation

An essential requirement for a cooperation is respecting the fundamental principles of the parties involved.

- Service providers must constantly balance the responsibility to protect customer information and comply with established privacy principles alongside cooperation efforts with law enforcement to protect and promote public safety. In this context, service providers typically establish criminal compliance programs to help maintain that balance by evaluating demands

and requests from law enforcement consistent with its legal obligations in applicable jurisdictions.

- Law Enforcement agencies are mandated to investigate crime at a national level. Cybercrime by its international dimension and constantly changing nature requires substantial cooperation between national law enforcement agencies in different countries and access to knowledge, expertise and log records in the process of the crime investigation. The level of such knowledge and expertise varies within agencies and between agencies in different countries. The range of criminal procedural law is also very different.

### **Overcoming national and regional differences**

Criminal compliance programs vary greatly from one provider to the next depending on a number of factors, including, without limitation, the types of services offered and the location where customer records are stored. In some countries, therefore, certain providers will not offer any criminal compliance support, while in other regions the same providers may have elaborate compliance programs in place. Notwithstanding these differences, in countries where such support is offered, service providers should consider implementing the best practices set forth herein in an attempt to bring some level of uniformity to the manner in which providers work with law enforcement.

### **Developing the foundation for a cooperation**

An effective fight against cybercrime therefore requires a carefully considered approach from industry and law enforcement. With the complexity and speed of development of new technologies such as new services being offered online for free, Service Providers are increasingly being asked to engage in a more active way in addition to responding to requests from law enforcement. Law Enforcement do not have the capacity to develop internally all the expertise which is required and cooperation with the private sector is not necessarily something done routinely. Law Enforcement can gain and maintain an understanding of new technology areas from Internet Service Providers. Industry and Law Enforcement need to share their expertise and concern.

At the very least, such cooperation takes place when law enforcement requests information from Service Providers. With experience Service Providers can learn to understand which agencies are entitled to request information and in which form. In return law enforcement will learn what is the best time or best way to obtain the information they are looking for. At the best Service Providers, which are filing complaints against fraudsters or abusers in order to protect their business services, this can understand the need to go beyond the raw criminal complaint and, in an appropriately sensitive way, provide, on a legal basis, further intelligence that help law enforcement better investigate the specific case reported by the Service Provider. This also helps Law Enforcement better investigate cybercrime generally.

Regarding cooperation against cybercrime, there is a need for providing a framework that will ease this cooperation and make its value better understood for both sides, as well as for the general public.

## **Key objectives**

With this study there is an opportunity to achieve something very practical and useful. It is important that there is a minimum common approach for law enforcement and industry in every country. There are particular problems faced by organisations which host services in one country but which are used by citizens of a different country.

A set of guidelines would also raise awareness within the Internet Industry about their role in helping to fight cybercrime and protect citizens by assisting law enforcement investigations, protecting customers of ISP's from criminal activities (such as anti-spam and anti-phishing initiatives) and providing a collection of knowledge about best practices in this area. Internet Service Providers can answer promptly to properly documented and legitimate requests from Law Enforcement and provide technical expertise when needed.

The purpose of the study and its underlying study group is to therefore create a new ongoing dialog and reasonable cooperative working environment between law enforcement and service providers at a national and international level. The early results of this dialog is to ensure mutual understanding of the roles and responsibilities of each other followed by deeper appreciation and knowledge of how each sector can work with the other.

This study will work to create a collection of best-of-breed work practices which might then be used as good practice guidelines to ensure that there are clear policies and procedures to the satisfaction of both industry and law enforcement agencies having regards to standards of confidentiality and privacy afforded to users of the Internet. These transparent mechanisms will ensure that there is a clear understanding on both sides as to what the procedures are and promote positive relations between law enforcement and the Internet Service industry.

Accordingly, the present working group aim at fighting cybercrime through effective cooperation between industry and law enforcement agencies and establishing the framework in this document for that cooperation. The participants believe this can be achieved by exploring ways for the parties to partner in their battle against cybercrime, including:

- 1) the definition of best practices aimed at establishing a level of uniformity in the manner in which Industry and Law Enforcement interact both in terms of day-to-day relationship and long term cooperation
- 2) the development and coordination of training programs targeted at Law Enforcement on trends in cybercrime and effective means to address it;
- 3) the support and coordination of conferences for the parties to share their collective learning on combating cybercrime;
- 4) the creation and/or support of tools to assist Law Enforcement through the different steps of the investigation, typically the collection and preservation of data during the raid or on seized computers, management of investigations, transmission of evidence requested by law enforcement.

## **1.4 Structure of the study**

The study is structured in the following way.

This study offers a background review of four key areas:

- Illegal Activity on the Internet
- Legal/regulatory Response
- Internet Industry
- Law Enforcement Agencies

The study then looks at what broad range of data is considered and what other types of relationships might occur.

- Current Relationships
- Working Together/ Processing requests
- Issues which arise

Finally the study offers an overview of guidelines which are considered examples of the best of breed of international practice today.

- Draft Guidelines

## 2 Background

### 2.1 Illegal activity on the Internet

In addition to standard criminal behaviour, which has now moved online, the Internet has seen a new range of crimes emerge. Even since the first generation of computer- and network-related attacks took place new scams were discovered. These crimes such as "phishing"<sup>1</sup> and "identity theft"<sup>2</sup> require new methods of investigation and rely heavily on data and information in the hands of Internet Industry to achieve a successful prosecution. A lack of cooperation can seriously hinder the investigation.

The "crime scenes" are as varied as the crimes themselves. Criminals use all opportunities offered by society, economy and technology for their illegal purposes. The World Wide Web, Usenet, Internet Relay Chat File sharing, eMail, even online games such as World of Warcraft are targeted by them.

The Internet has also caused phenomenal growth in new services such as Social Networking which has become increasingly popular as a means for people to keep in touch, meet new people, share photos, music and videos.<sup>3</sup> There are many benefits to using such a network; however, people need to be aware of the dangers that may exist when using a social network site. For example, many users may display personal information which could be misused. Very often the registration process in those Social Networking Services goes along with the disclosure of private information that can be abused by perpetrators. Due to the fact that the majority of Internet users use a limited number of very popular services as well as the availability of search engines that are specialised on the detection of private information about a person<sup>4</sup> it is rather easy for a perpetrator to collect those information and use them for criminal purposes.<sup>5</sup> In November 2006, CEOPS (UK Child Exploitation and Online Protection (CEOP) Centre) stated "Notwithstanding the fact that online social networks have utterly revolutionised social interaction, this new environment can facilitate new forms of social deviance and criminality. Its ability to collapse the conventional social barriers that govern sexual behaviour has compounded this situation, presenting new opportunities for sexual expression and deviance both to young people and to adults with a sexual interest in this group. This has resulted in a very real series of risks to the welfare of young people that socialise in this environment."

---

<sup>1</sup> Regarding the phenomenon „phishing“ see. *Dhamija/Tygar/Hearst, Why Phishing Works* – available at: [http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf); Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006 – available at: [http://www.usdoj.gov/opa/report\\_on\\_phishing.pdf](http://www.usdoj.gov/opa/report_on_phishing.pdf)

<sup>2</sup> Regarding the phenomenon „identity theft“ See for example: See: *Gerccke, Internet-related Identity Theft, 2007* – available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf); *Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions*, *Lex Electronica*, Vol. 11, No. 1, 2006 – available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited: Nov. 2007); *Peeters, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection*, *MMR 2007*, 415; *Givens, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions*, 2000 – available at: [http://www.privacyrights.org/ar/id\\_theft.htm](http://www.privacyrights.org/ar/id_theft.htm) (last visited: Nov. 2007).

<sup>3</sup> Examples for such services are [www.myspace.com](http://www.myspace.com) and [www.facebook.com](http://www.facebook.com).

<sup>4</sup> See for example [www.spock.com](http://www.spock.com).

<sup>5</sup> Having access to true identity-related information can be from great interest of the offender even if these information do not enable him to act by using this identity. The offender can especially use the information to improve synthetic identities by mixing generated data with existing data. Regarding the importance of synthetic identities in identity theft scams see: *ID Analytics*, [http://www.idanalytics.com/assets/pdf/National\\_Fraud\\_Ring\\_Analysis\\_Overview.pdf](http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf) (last visited: Nov. 2007).

Another example for new services that are very popular because of their approaches in improving online communication on the one hand side but are also related to criminal activities are Online Games.<sup>6</sup> Internet Games and Gambling are a one of the fastest growing areas in the Internet business. Current researches see a growth potential from 3.1 Billion US\$ in 2001 (estimated online gambling revenue) to 24 Billion US\$ in 2010 for Internet gambling.<sup>7</sup> Compared to the revenues of classic gambling these numbers are still relatively small.<sup>8</sup> Linden Labs, the developer of the online game Second Life reports that nearly 10 million accounts have been registered.<sup>9</sup> Current reports<sup>10</sup> show that those games were used to commit crimes like exchange and presentation of child pornography<sup>11</sup> and fraud.<sup>12</sup> Tracing back those offenders and taking down phishing sites requires a close cooperation between law enforcement agencies and the providers involved.

A close cooperation between law enforcement agencies and service providers is required in other areas too and not only with regard to new, highly sophisticated scams. Internet investigations do in general go along with unique challenges that do especially require the close cooperation between law enforcement agencies and providers. One example is the international dimension of the network. The process of transferring illegal content from one offender to another might involve a number of providers that could be based in different countries. Tracing back the route from one to the other offender requires the close cooperation between law enforcement agencies. Those investigations very often require immediate action. The transfer of an e-mail from one country to another only takes seconds. This rather short period of time is a challenge for the national Law Enforcement Agencies involved in the fight against Cybercrime as the traditional investigation instruments are designed on a different background with regard to the time available for investigations.<sup>13</sup>

### 2.1.1 Common legal standards

One essential advantage and in general even requirement for a close cooperation of private businesses and law enforcement agencies in criminal investigations are common legal standards. This includes substantive criminal law as well as the procedural law.

A number of countries have based their mutual legal assistance regime on the principle of "dual criminality".<sup>14</sup> Investigations on a global level are therefore in general limited to those crimes that are criminalised in all participating countries. Although there are a number of offences that can be prosecuted anywhere in the

---

<sup>6</sup> One example is [www.secondlife.com](http://www.secondlife.com).

<sup>7</sup> Christiansen Capital Advisor. See [http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet\\_gambling\\_data.htm](http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm).

<sup>8</sup> The revenue of US casinos in 2005 (without Internet gambling) was more than 84 Billion US – See: *Landes, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation*, page 915 – available at: <http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf>;

<sup>9</sup> Number of accounts published by Linden Lab. See: [www.secondlife.com/whatis/](http://www.secondlife.com/whatis/). Regarding Second Life in general: *Harkin, Get a (second) life*, Financial Times – available at: <http://www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html>.

<sup>10</sup> See Heise News, 15.11.2006 - available at: <http://www.heise.de/newsticker/meldung/81088>; DIE ZEIT, 04.01.2007, page 19.

<sup>11</sup> See for example BBC News, 09.05.2007 Second Life 'child abuse' claim – available at: <http://news.bbc.co.uk/1/hi/technology/6638331.stm>.

<sup>12</sup> See *Leapman, Second Life world may be haven for terrorists*, Sunday Telegraph, 14.05.2007 – available at: <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml>; *Reuters, UK panel urges real-life treatment for virtual cash*, 14.05.2007 – available at: <http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/>.

<sup>13</sup> *Gercke, The Slow Wake of A Global Approach Against Cybercrime*, CRI 2006, 142.

<sup>14</sup> The difficulties the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member State (2002/584/JHA).

world regional differences play an important role. An example is illegal content. The criminalisation of illegal content differs in various countries.<sup>15</sup> Material that can lawfully be distributed in one country can easily be illegal in another country.<sup>16</sup>

It is likely that the cooperation between law enforcement agencies and ISP will go along with difficulties if it is uncertain if the request is related to an act considered to be a criminal act. Uncertainties related to the legal situation are in general more likely to be a problem for the cooperation between law enforcement agencies and ISP within international investigations.

### 2.1.2 Council of Europe Convention on Cybercrime

Common standards in Internet-related investigation are defined by the Convention on Cybercrime. The European Committee on Crime Problems (CDPC) decided in 1996 to set up a Committee of experts to deal with Cybercrime.<sup>17</sup> In difference to the situation in 1985 the idea of going beyond working on principles for another recommendation and draft a Convention was present at the time of the establishment of the Committee of experts.<sup>18</sup> Between 1997 and 2000, the Committee held 10 meetings in plenary and 15 meetings of its open-ended Drafting Group. The Assembly adopted the draft Convention at the 2nd part of its plenary session in April 2001.<sup>19</sup> The finalised draft Convention was submitted for approval to the CDPC, and afterwards the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature. The Convention was opened for signature at a signing ceremony in Budapest on November 23, 2001, during which 30 countries signed the Convention (including the four non members of the Council of Europe Canada, United States, Japan and South Africa that participated in the negotiations). Until October 2007 43 states<sup>20</sup> signed and 21 states<sup>21</sup> ratified<sup>22</sup> the Convention on Cybercrime. Until now the Council of Europe Convention on Cybercrime<sup>23</sup> is apart from the UN Resolutions 55/6324 and

---

<sup>15</sup> The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Convention on Cybercrime but addressed in an additional protocol.

<sup>16</sup> With regard to the various national approaches to criminalise child pornography see for example *Sieber, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet*.

<sup>17</sup> Decision CDPC/103/211196. The CDPC explained their decision by pointing out the international dimension of computer Crimes: „ By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."

<sup>18</sup> Explanatory Report of the Convention on Cybercrime (185), No. 10.

<sup>19</sup> The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: [www.coe.int](http://www.coe.int).

<sup>20</sup> Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Romania, Serbia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

<sup>21</sup> Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia Lithuania, Netherlands, Norway, Romania, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

<sup>22</sup> The need for a ratification is laid down in Article 36 of the Convention:

*Article 36 – Signature and entry into force*

1) *This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.*

2) *This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.*

<sup>23</sup> Convention on Cybercrime, European Treaty Series - No. 18. The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: [www.coe.int](http://www.coe.int).

<sup>24</sup> A/RES/55/63. The full text of the Resolution is available at: [http://www.unodc.org/pdf/crime/a\\_res\\_55/res5563e.pdf](http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf) (April 2006)

56/12125 the only complex international legislative solution in the fight against Cybercrime. It has become a true model law for Cybercrime legislation. Countries like Pakistan, India, Philippines, Nigeria, Morocco and Argentina, that have not yet signed or ratified the Convention on Cybercrime have nevertheless used it as a model law while updating their Cybercrime-related legislation.

With regard to the offences mentioned in the Convention as well as the procedural instruments a cooperation between law enforcement agencies and ISP within international investigations have a solid basis in those countries that brought their legislation in line with the Convention on Cybercrime.

### 2.1.3 Cooperation outside common legal standards

There are two potential difficulties related to missing common standards:

- One country (either the one where the ISP is based or the country that is carrying out the investigation) has no sufficient legislation in place
- The investigations are related to an offence that is not covered by the Convention on Cybercrime

Especially the second aspect is from great practical importance. Although the Convention does cover the most serious computer-related and internet-related offences there are scams that are not yet covered. Classic examples are phishing and identity theft.

#### 2.1.3.1 Phishing

The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information.<sup>26</sup> Very often the offenders are sending out e-mails that look like an e-mail from a legitimate financial institution used by the victim.<sup>27</sup> The e-mails are designed in a way that it is impossible or at least difficult for the victim to identify it as a falsified e-mail. The classic e-mail-based<sup>28</sup> phishing scam contains three phases:

- First of all the offenders identify a legitimate company who’s customers are targeted – e.g. a financial institution.<sup>29</sup>
- In a second step the offenders design a website by copying characteristic elements of the website used by the legitimate company (“Spoofing Site”).<sup>30</sup> The intention of the offender is to direct the victim to this website and pretend that it is the original website of the legitimate company. This will enable the offenders to get in possession of the personal information the user entered during the log-in (e.g. the bank account number and the password for the online banking

---

<sup>25</sup> A/RES/56/121. The full text of the Resolution is available at:  
<http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf>.

<sup>26</sup> The term “phishing” originally described the use of emails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. See *Gercke*, CR, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks – available at:  
<http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf>.

<sup>27</sup> With regard to this aspect the “phishing” scam shows a number of similarities to spam e-mails. It is therefore likely that those organised crime groups that are involved in spam are also involved in phishing scams as they have access to spam databases.

<sup>28</sup> Other phishing scams are including voice communication. See: *Gonsalves*, Phishers Snare Victims With Voip, 2006 – available at: <http://www.techweb.com/wire/security/186701001>.

<sup>29</sup> With regard to the fact that most phishing scams are Internet related scams the offenders are focussing on legitimate companies that offer online services and therefore communicate by electronic means with their customers.

<sup>30</sup> With regard to the intention of the offenders to mislead the victims the websites are called “Spoofing Sites”

system). In order to direct the user to Spoofing Site the offenders in general send out millions of copies of e-mail that looks like an e-mail from a legitimate company.<sup>31</sup> Today the e-mails are designed in a way that it is impossible or at least difficult for the victim to identify it as a fake e-mail. In the e-mail the recipient is ordered to log-in immediately to his account with the legitimate company. The offenders developed the techniques to prevent the user from realising that he is not directed to the original website to a very high level.

- After going through the fake log-in process the offenders can use the obtained data and for example transfer money. Especially with regard to bank transfers the offenders are causing additional difficulties for the law enforcement agencies by including so called "financial managers" in the scam.<sup>32</sup>

The increasing number of attacks and the success of them demonstrate the potential of this scam.<sup>33</sup> More than 55,000 unique phishing sites were reported to the APWG<sup>34</sup> in April 2007.<sup>35</sup> It is important to highlight that the scam is not limited to getting access to passwords for online banking. Offenders are aiming for access codes to computers and auction platforms as well as social security numbers.

The Convention does not contain an individual provision criminalising phishing attacks but it contains a number of provisions that criminalise the most relevant parts of the phishing scams. One example is Art. 7 Convention on Cybercrime. In protecting the security and reliability of electronic data Art. 7 Convention on Cybercrime aims to create a parallel offence to the forgery of tangible documents in order to fill gaps in criminal law related to traditional forgery provisions that might not apply to electronically stored data.<sup>36</sup> This provision can be applied with regard to the creation and use of the falsified e-mails.

### 2.1.3.2 Identity theft

The term identity theft describes criminal acts where the perpetrator fraudulently obtains and uses another person's identity.<sup>37</sup> These acts can be carried out without the help of technical means<sup>38</sup> as well as online by using Internet technology.<sup>39</sup>

---

<sup>31</sup> With regard to this aspect the "phishing" scam shows a number of similarities to spam e-mails. It is therefore likely that those organised crime groups that are involved in spam are also involved in phishing scams as they have access to spam databases.

<sup>32</sup> The term "financial managers" is used to describe people that support the offender (in most cases without intention) by offering their bank account for money transfers. For more information see: *Gercke, The Development of Cybercrime Legislation in 2007, ZUM 2007, page 288.*

<sup>33</sup> In some phishing attacks up to 5 percent of the victims provided sensitive information on the fake website. See *Dhamija/Tygar/Hearst, Why Phishing Works* – available at: [http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf), page 1 that are referring to *Loftness, Responding to "Phishing" Attacks*. Glenbrook Partners (2004).

<sup>34</sup> Anti-Phishing Working Group. For more details see. [www.antiphishing.org](http://www.antiphishing.org).

<sup>35</sup> Phishing Activity Trends, Report for the Month of April 2007 – available at: [http://www.antiphishing.org/reports/apwg\\_report\\_april\\_2007.pdf](http://www.antiphishing.org/reports/apwg_report_april_2007.pdf).

<sup>36</sup> Explanatory Report to the Council of Europe Convention on Cybercrime No 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

<sup>37</sup> Peeters, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415;

<sup>38</sup> One of the classic examples is the search for personal or secret information in trash or garbage bins ("dumpster diving"). For more information about the relation to Identity Theft see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit Insurance Corporation, 2004 – available at: [http://www.fdic.gov/consumers/consumer/idtheftstudy/identity\\_theft.pdf](http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf) (last visited Nov. 2007); Paget, Identity Theft – McAfee White Paper, page 6, 2007 – available at: [http://www.mcafee.com/us/threat\\_center/white\\_paper.html](http://www.mcafee.com/us/threat_center/white_paper.html) (last visited: Nov. 2007).

<sup>39</sup> Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than

Especially internet-related identity theft cases are to a large extent based on highly sophisticated scams that demonstrate the capability of automated attacks<sup>40</sup> on the one hand, and show the difficulties that law enforcement agencies are faced with when investigating such offences on the other.<sup>41</sup> Current surveys show that identity theft is not only a serious challenge for societies as well as law enforcement agencies with regard to the number of offences but also with regard to the losses suffered<sup>42</sup> In general there are different legal approaches to criminalise identity-theft:

- The creation of one provision that criminalises the act of obtaining, possessing and using identity-related information (for criminal purposes)
- The individual criminalisation of typical acts related to obtaining the identity-related information (like illegal access, the production and dissemination of malicious software, computer-related forgery, data espionage and data interference) as well as acts related to the possession and use of such information (like computer-related fraud).

Unlike for single-provision approaches<sup>43</sup> the Convention on Cybercrime does not define a separate cyber-offence of the unlawful use of identity-related data.<sup>44</sup> Nevertheless most of the acts that are related to identity theft like accessing a computer system to obtain person information and using someone's identity in computer-related fraud activities are criminalised by the Convention.<sup>45</sup> Similar to the situation with regard to the criminalisation of obtaining identity-related information the Convention is as a result not covering all possible acts related to the unlawful use of personal information. With regard to those acts that are covered by the Convention the criminalisation is not limited to acts that involve the unlawful use of personal information.

## 2.2 Legal/regulatory response

Although the relation between law enforcement agencies and internet service provider is based on bidirectional interaction the law-makers focus on defining the role of service providers in investigations. The chapter gives an overview about existing provisions regulating the cooperation of LEA and ISP.<sup>46</sup>

The evaluation of possibilities to improve the cooperation between Law Enforcement Agencies and Internet Service Providers based on soft law requires the identification

---

electronic channels. In the cases where the methods were known, less than 15% obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report – available at: <http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf> (last visited: Nov. 2007). For further information on other surveys see Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006 – available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited: Nov. 2007).

<sup>40</sup> Regarding the Challenges related to the automation see below 3.4.

<sup>41</sup> Regarding the Challenges for Law Enforcement Agencies see below 3.4.

<sup>42</sup> See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

<sup>43</sup> For an overview about the different legal approaches see: Gercke, Internet-related Identity Theft, 2007 – available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf).

<sup>44</sup> See as well: Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29 – available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited: Nov. 2007);

<sup>45</sup> See: Gercke, Internet-related Identity Theft, 2007 – available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf).

<sup>46</sup> For a more detailed overview about the function of the different instruments provided by the Convention on Cybercrime see below, Chapter 3.

of existing (mandatory) obligations provided by law. Soft law<sup>47</sup> can be an important source in areas where legal provisions are missing or procedures are not defined as precisely as necessary but it will in general not be capable to improve the cooperation between LEA and ISP if they are not in line with the obligations and procedures provided by law.

One important source with regard to the cooperation of LEA and ISP are the criminal procedural law provisions related to the investigation of Internet-related offences. Within the scope of this study it is not possible to analyse the legal framework developed by the criminal procedural codes in each country. The report will therefore primarily focus on the legal framework provided by the Budapest Convention on Cybercrime (CoC) that is currently the only international agreement that provides the necessary legal components with regard to substantive criminal law, criminal procedural law and international cooperation.<sup>48</sup>

With regard to investigations, that are an important area of cooperation between LEA and ISP not only the investigation instruments are an important source for regulatory approaches. Another important source are the safeguards. National, regional and international legal frameworks define clear limitations for the application of investigation instruments. One example is Art. 15 Convention on Cybercrime. Art. 15 which is based on the principle, that the signatory states shall apply those conditions and safeguards that already exist under the domestic law. If the law provides central standards that apply to all investigation instruments these principles shall apply to the Internet-related instruments as well.

Further limitations can be found in decisions of different courts. The European court of Human Rights has for example undertaken efforts to more precisely define standards that govern especially electronic investigations and especially surveillance. This case law has become one of the most important sources for international standards related to investigations related to communication.<sup>49</sup> It especially takes regard to gravity of the interference of investigation<sup>50</sup>, its purpose<sup>51</sup> and its proportionality.<sup>52</sup> Fundamental principles that can be extracted from the case law are:

- A sufficient legal basis for investigation instruments are necessary<sup>53</sup>
- The legal basis must be clear with regard to the subject<sup>54</sup>

---

<sup>47</sup> Non-legislated documents such as recommendations, codes of practice, etc

<sup>48</sup> Regarding the Convention on Cybercrime see: *Gercke*, CRI, 2006, 140 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, *Entertainment Law Review*, 2002, No. 1 – available at: <http://elr.ils.edu/issues/v23-issue1/aldesco.pdf>; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005 – available at: <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf>; *Broadhurst*, Development in the global law enforcement of cyber-crime, in *Policing: An International Journal of Police Strategies and Management*, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, *International Journal of International Law*, Vol 95, No.4, 2001, page 889 *et seq.*

<sup>49</sup> ABA International Guide to Combating Cybercrime, page 139.

<sup>50</sup> "interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of *Kruslin v. France*, Application no. 11801/85.

<sup>51</sup> "the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of *Malone v. United Kingdom*, Application no. 8691/79

<sup>52</sup> "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of *Klass and others v. Germany*, Application no. 5029/71.

<sup>53</sup> "The expression "in accordance with the law", within the meaning of Article 8 § 2 (art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of *Kruslin v. France*, Application no. 11801/85.

- The competences of the law enforcement agencies need to be foreseeable<sup>55</sup>
- Surveillance of communication can only be justified in context of serious crimes<sup>56</sup>

The various safeguard restrict the competence of LEA to apply certain instruments and by this limit the obligation of ISP to support the investigations. Respecting those safeguards must be the basis for any investigation by LEA as well cooperation between LEA and ISP.

## 2.3 Profile of Internet service industry

It is important to understand the various players in the industry and their role in relation to the carrying, processing and storage of information on its journey throughout the Internet.

These roles will help identify areas of responsibility and control and will aid in the writing of guidelines to manage the level of responsibility *or ability* in the fight against illegal and harmful use of the Internet. Harmful content will only deal with the type of content currently considered legal for adults but considered inappropriate/ illegal for children to access.

### 2.3.1 Internet players

The roles can be broken into seven main areas:-

- Consumer
- Telecommunications Provider
- Internet Access Provider
- Facilities/Hosting Providers (include Web Farm)
- Content Providers
- Broadcasters
- Mobile Operators – included in either (b) or (c) above?

Often a number of these distinct roles are implemented by one individual national or international organisation. Therefore the borders between roles and services are quite blurred and are not so clear in practice. The same service centres, communications hubs are used to implement multiple roles either in a fusion of equipment, services and products or in a co-location style implementation.

---

<sup>54</sup> "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application no. 50210/99.

<sup>55</sup> "it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application no. 11801/85.

"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.", Case of Malone v. United Kingdom, Application no. 8691/79

<sup>56</sup> "The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application no. 5029/71.

These roles are distinct in definition but many of the organisations will cross the boundaries for each of these and therefore play several of these roles simultaneously. For example, a telecommunications provider will provide links for use by other Internet Service Providers, will sell ISP services directly, provide facilities management services and become a content provider. In addition due to the provision of satellite services they can be considered a broadcaster. Finally, as a large employer they will sometimes have large populations of consumers of all these services. For this reason, it is important to understand that a company can perform several roles at the same time and that we define each role (and related obligations or liability) with regard to each specific service being offered.

The descriptions cover all stakeholders in the Internet space. This study will only focus on four of these stakeholders. Extending the study to other internet players could generalize the criminal activities to all kinds of service providers and internet participants. It is very important to note, that the criminal activities on the internet are not focused on access providers, telecommunications providers, hosting providers or mobile providers. The significant platform for criminal activities is based in the group of criminal users and content providers.

a) Consumer

Players: Individuals, Families, companies, Research Organisations, Universities, Schools, Government Agencies, Employees, Students

Managing the end user can be a complex mesh of Acceptable Use Policies (AUP) administered by each of the others organisations in the chain. The end consumer *might* have a direct contract with a local, regional or national Internet Service Provider for Internet Access or their academic institution or employer which may operate an AUP which places restrictions on email abuse, news group subscriptions, copyright abuse protection, slander/libel restriction, patent protection including intellectual property rights. Nevertheless, it must be remembered that AUP's are limited by the existing national legal situation and must be consistent with contract law.

Students and Employees would need to be regulated using work contracts and might be protected by the Data Protection Act or invasion of privacy provisions.

Users might bypass these restrictions by availing of an account on a non-national Service Provider which operates using a more open AUP.

Actual knowledge about illegal activity on their services:

In general the end-user can be considered to have the highest ability to know what material or information is 'flowing' though the local computer. Absolute end-users are usually the perpetrators of illegal activity on the Internet. This can be a challenge for near-end-users such as employers, school management, etc to completely restrict the activities of the absolute end-users where the Convention on the Protection of Human Rights and Fundamental Freedoms and the national law permit such restrictions. For example, Article 8 of the convention and French national law do not allow employers to monitor employees activities without following specific procedures as stated by the law. These near-end-users have limited liability for the end-user behaviour depending on their rights and obligations in that area and, when relevant, on their level of negligence.

It is also possible, however, for end-users to unknowingly receive illegal or harmful material either disguised or encrypted via eMail, Web or newsgroups and stored on their local hard disk without their direct knowledge. This can be achieved by malicious or accidental methods.

Public education programs in conjunction with support from other members of the Internet Player chain should be adopted to educate the consumer base on methods of protection available.

b) Telecommunications Provider

Players: National Operators, Pan-National operators, Satellite providers, etc

These organisations provide either access to telecommunications channels and high-speed broadband connections, dial-on-demand services via dial-up ISDN/Analog modem, permanent leased line connections and broadcast capability via regional satellite broadcasting. They often need a national telecommunications license to operate and must comply with strict rules of providing such services.

Actual knowledge about illegal activity on their services:

The sheer volume and complexity negates any wide-scale detailed analysis without prior knowledge and specific targeting of potential abuse. If performed such activities would have major consequences for rights to private life.

Information can be when a link is being created - either leased line or modem call. Source/Destinations of links can be regulated and Acceptable Use Policies can be agreed.

For these reasons Telecommunications Carriers are usually considered to have a *Common Carrier* status absolving them of any responsibility for the content and meaning of any of the electronic signals they carry.

c) Internet Access Provider

Players: Providers of on-demand or dedicated access to the Internet (and to Internet services such as eMail, News, etc. However, dedicated email providers are not access provider neither news providers. A user can also use an e-mail service not provided by the access provider.)

An industry wide Acceptable Use Policy (AUP) can be adopted by Internet Service Providers in addition to an industry Code of Practice. Many of the ISP's already operate a comprehensive set of Terms & Conditions of Access and an Acceptable Use Policy for network access.

The Internet is a collection of unregulated interconnected international computer networks bound by the common standard of using the TCP/IP protocols. Within that framework, the challenge of regulation is to find the best way to help investigations, respecting international law, fundamental Rights and commercial competitiveness.

Actual knowledge about illegal activity on their services:

The data travelling across the ISP network operations centre is usually processed automatically and unless deliberately intercepted is never seen, heard

or read by human operators. In addition to major privacy issues, the sheer volume and complexity negates any wide-scale detailed analysis without prior knowledge and specific targeting of potential abuse. Some providers have managed to implement a content-filtering service for unsolicited email (spam) or malware (virus, trojans, etc) and more recently in the area of content blocking of child pornography.

In addition, with the advent of technologies such as encryption, proxy servers, overseas accounts multi-protocol tunnelling, Internet Service Provider's may no longer be able to technically 'see' inside (deep packet inspection) the packets travelling across the Internet (though they will continue to have knowledge as to the source, destination and type of packets of information).

Internet Access Provider's are often considered common carriers (i.e. not liable for content) in those services which provide connection services to the Internet for the transmission and receipt of information.

Some customers of ISP's use closed-user-group access identical to dedicated circuits from Telecommunications Providers but with the advantage of using a cheaper secure communication across a public Internet. This would further reduce the level of regulation possible.

In specific cases of abuse and with appropriate legal instruments, the Internet Access Provider's have some capability of analysing the information travelling across their links but it is not an absolute certainty that correct analysis would always result. The accuracy would depend crucially on the services being regulated. See the section describing the services.

However, the transmission of content directly to international news servers is still possible by end users thus bypassing local law provisions. In addition, experience has shown that simply restricting a news feed strongly encourages consumers to avail of international based news servers which are not subject to the same legal regime.

The continued rapid develop of technology and communications procedures and techniques creates an environment where many of the solutions will superseded by imminent technological advances.

#### d) Facilities/Hosting Providers

Players: Organisations who permit the location of third-party computers to be directly connected to their Internet access point.

These players do not manage or operate a network connection directly but take advantage of the network in place at a registered ISP or Telecommunications Provider.

Any direct regulation could only be achieved through the adoption of a contract of service from the service provider, the provider's Acceptable Use Policy and through service Terms and Conditions contracts. In the context of web re-sale activities they can require their customers to sign AUP/ T & C/ proper-use contracts.

Actual knowledge about illegal activity on their services:

Often the computers are used as web hosting machines for third party organisations and the owner/ operator will have limited knowledge what content is being stored on the server. Each third party client can update the content on the server remotely on a 24 hour basis, 365 days per year. These updates can be performed by the client via manual operation or can be performed automatically requiring no operator intervention.

Facilities providers will have no access to the hosted equipment except by prior request from the client and as such will have no ability to directly monitor or analyse the performance of the equipment except in relation to known network problems emanating from the third party equipment. The contract usually permits the Facilities provider to disconnect client equipment pending resolution of reported problems.

e) Content Providers

Players: A content provider is an organisation/user that provides information to an Internet target audience. These can be single individuals which specific knowledge of a particular geographical region, a small group of people with specific interests or a large corporation with products for sale. With the arrival of Web 2.0 many end-users become content providers in their own right so the role of content provider needs to be divided into professional content providers such as news organisations, etc and non-professional content providers such as home users, etc.

Some services such as Web are hosted directly by the ISP's on local equipment and computers. It is possible to develop a Code of Practice for these services which would regulate the availability of illegal content.

The issue of Usenet News is more sensitive as the service can be distributed by an access provider that will only be able, technically speaking, to prevent the distribution of a specific newsgroup, and not to prevent the distribution of one specific illegal message. Such initiative could be judged as not proportionate. For example, a French court has already stated that access providers are providing a "caching" service, not a "hosting" service, when they distribute Usenet news (the difference in terms of liability is significant)

The information published by a content provider is usually directly under the control of the content provider. In most cases, any information can be checked prior to publication using well known classification standards and compliance with AUP. The sheer volume and complexity negates any extensive analysis without prior knowledge and specific targeting of potential abuse.

These is the outstanding concern relating to the classification of dynamic user-generated content especially those who use different languages, cultures and societies but wish to contribute to local content.

Actual knowledge about illegal activity on their services:

This content currently has the highest value in the Internet chain. Internet surfers have an insatiable appetite for information - from entertainment to

edutainment, from business news to product updates, from software to music, from email to chat-rooms.

Ultimately the style and meaning of content is determined by those who create the volumes of information available. However, many sites allow the public to add content remotely. This feature can be a powerful exchange tool but can be easily abused.

Content providers require procedures for the removal of proscribed content. and for ensuring that publication of local content takes place after the information is rated by content moderator. (This will have problems where content can be expanded by any user)

f) Broadcasters

Players: Organisations such as television, radio, and print organisations.

Trans-national broadcasting is inherently difficult to regulate. Nationally based broadcasters are subject to national law and can be regulated according to normal editorial control and content classification procedures. Satellite could only be regulated if the signal is delivered via encrypted downlink. The decoding equipment can sometimes be subject to licensing and regulation but this will be hard to police.

Actual knowledge about illegal activity on their services:

Much of the content of these organisations is created by third parties and the responsibility of ensuring compliance with local standards can be a significant organisational burden.

Some of the satellite companies are offering direct-to-home news feeds which would contain the complete gamut of news content in an unregulated and uncontrolled manner.

The sheer volume and complexity negates any reasonable analysis without prior knowledge and specific targeting of potential abuse. Many Internet Service Providers are also offering broadcast services over broadband – including radio and ip-tv.

f) Mobile Operators

Players: Organisations such as Vodafone, O2, T-Mobile, Orange, Telefonica, etc

Mobile operators have much the same issues as telecommunications providers. The extra layer of complexity relates to the mobility of the connection which needs to be carefully tracked in the mobile network.

Actual knowledge about illegal activity on their services:

Mobile operators keep some data related to calls sent/received. They can also keep records on all text messages sent/received. They are nevertheless not allowed to take actual knowledge of these messages but can, subject to

appropriate requests, sometimes make them available to law enforcement as part of a criminal investigation.

### 2.3.2 Internet services

An alternative method of describing the roles is to do so in terms of the Internet services provided:-

- a) email
- b) Newsgroups/Usenet
- c) Web Browsing
- d) Website Provision
- e) Chat
- f) File Transfer
- g) Peer-to-peer
- h) Social Networking
- i) Voip
- j) Market place
- k) Others

These can also be described in fewer categories if activities were groups. For example, a hosting provider can host websites, chat, news, social networks, etc. while a content provider can edit a website, write on a blog or on a newsgroup, upload a file on a P2P network. Other categories include search engines, email providers and access providers/phone operators. The distinction between "telecommunications provider" or "operators" and "access providers" is more important as regards data that can be retained.

#### a) eMail

eMail allows the exchange of messages and documents in a one-to-one, one-to-many manner. These messages are usually plain text or HTML but attached files can be graphics, spreadsheets, reports, etc. It is also possible to encrypt eMail content to prevent others from intercepting it. Email clients can be web based or computer based. In web based clients, the emails are stored on the remote web server (ala Google, Hotmail, etc) whereas with computer based clients the emails can be downloaded onto the owner's computer.

Since email messages are considered as communication between co-operating parties, the email service can be legally and technically speaking difficult to protect from threats. These parties can also encrypt the communication preventing interception and therefore criminal investigations. One aspect of eMail activity which can be better managed in recent years is that of 'spamming' - a process where volume eMail is targeted at end-users without their request - in essence 'junk' email.

Means of Knowing:

Computer based eMail travelling across the Service Provider network operations centre is processed automatically and unless deliberately intercepted is never

seen, heard or read by human operators. The sheer volume and complexity and the significant impact on privacy negates any extensive analysis without prior knowledge and specific targeting of potential abuse.

Service Provider eMail machines process millions of email messages each day in an automated manner with basic logs of activities being maintained.

Detailed analysis could be undertaken on nominated accounts but comprehensive regulation is unfeasible. There would be a strong argument for "common-carrier" status on this type of service.

b) Newsgroups/Usenet

Network News is a large distributed bulletin board system which allows the exchange of information in a many-to-many manner. There are over 30,000 (and growing) discussion groups with a DAILY volume of many GB and the number of newsgroup messages of over 1,000,000.

The newsgroups are spread across 30,000 different topics and in theory it is possible to prevent the distribution of specific newsgroups. However, there is no technical method of controlling the content of any newsgroup - it is subject to self-regulation and net etiquette.

The blocking of specific newsgroups is feasible but can not be considered as a definitive solution to illegal or harmful content.

It is possible for users to inject news messages into the news system using international news hosts thus bypassing local regulations. In addition, users can read the news database stored on international servers which would have a significant impact on international bandwidth if large numbers were to adopt this approach.

c) Web Browsing

Web browsing allows end-users using software such as Internet Explorer, Netscape Navigator, Firefox, Safari, etc. to browse information in a graphical and hierarchical manner on remote servers located in all countries of the world.

This content can span the full range of work related research material, edutainment for home education to illegal and harmful material. The wide range of dubious material has created real concerns among many Internet users. Its success continues to grow and newer technologies will enable faster and wider distribution of web content.

For example, the standards in relation to PICS (Platform for Internet Content Selection) allow choice in the categorisation of web site content. Browsing software checks each site selected for a site rating hosted on a separate server for the style and content of the selected site.

Simple rules can permit or deny access to sites based on criteria specified by the parent, manager or users themselves.

Means of Knowing:

Users can usually choose what types of content they want to see and/or hear. There are some concerns associated with pop-up content which is often displayed without choice but more recent software browsers and filtering software prevent this from happening.

d) Web Provision

Web sites can be hosted anywhere in the world and a single site can even span multi-jurisdictional boundaries. The site can contain text, graphics, video clips, music and sound clips in addition to more complex interfaces to remote databases which can be located in different geographical boundaries.

Means of Knowing:

It is impossible to reasonably know the information stored on web servers.

Hosting Providers permit the website owners to update their web site remotely using password access. Thus a site carrying acceptable material today can be remotely updated to carry illegal material tomorrow. It is also possible for sites to carry hidden files available only to those who are in the know.

There have been many reported web site hack attacks whereby the content of web sites was illegally changed without the creator's permission and knowledge. This can make the allocation of responsibility a major problem.

e) File Transfer

File transfer permits the copying of documents, graphics, video-clips, audio clips from any part of the world onto the local computer or from the local computer onto a remote computer system. The file transfer process is normally performed manually by the user but on many systems can be completely automated.

The remote files can be encoded, compressed and even encrypted. Many systems offer anonymous FTP facilities which are essentially a large volume of publicly accessible files available for download by anyone without password access. Some organisations offer controlled (username and password) access to files and documents for a fee.

Means of Knowing:

The user downloading the files would normally have the greatest understanding of the content of the item being copied onto their computer. However, the exact nature and content of any such file could only be confirmed after the copy was complete.

f) Chat

CHAT is the Internet equivalent of voice chat lines except that in this case the users participating in the forums each type their message into their computer which is then copied onto the screen of each participant in the group.

The 'conversations' can cover a very broad range of subjects including illegal and harmful areas. Many of these discussion groups are publicly advertised and

users can specify to their chat software that they are interested in taking part. It is also possible to have closed group discussions by prior arrangement.

Means of Knowing:

The users will have an idea as to the subject content when a group is joined but since the conversation is literally taking place in real-time in an interactive manner it is impossible to estimate the type of conversation that will occur. The real-time monitoring of each chat is not desirable, as people have the right to exchange information without being monitored. However, the existence and support of some support /response service (e.g. real-time moderators, etc) for sensitive people or for children can be an effective solution.

g) Peer-to-peer

Peer-to-peer connections permit direct connections between one computer on the Internet and a remote computer on the Internet. With advanced software multiple simultaneous connections can be created and maintained every second. Information is carried across the network links which cross Service Providers Network Operations Centres but do not usually transit the computer servers in the Service Providers Network Operations Centres.

Means of Knowing:

Only by direct interception of the p2p link or via reports of abuse by users of the service.

h) Social Networking

Social networking websites permit end-users to place content on the web servers of a social networking organisation such as facebook, bebo, etc. This content can be text, video, images and audio and permit other users to see this content or to comment on this content. It is possible for other users to place false information or personal information online without permission of the target user.

Means of Knowing:

The operator of the social networking website has access, technically speaking, to all areas of the site and can implement an acceptable-use-policy which all users must obey. Subject to respecting the legal framework, the operator can in practice have knowledge of the content either by searching content, moderating content or by end user complaints. However, it can also be argued that the operators of such websites could be considered as hosting providers, which would mean that they have no rights to read content where the user marked it as "private" (art. 8 CPHRFF). This is a complex legal debate which needs to take place and is outside the remit of this study. Even if it is possible and reasonable, the sheer volume and complexity negates any extensive analysis without prior knowledge and specific targeting of potential abuse.

i) Voip

Voice over IP permits internet users with the appropriate software to establish a connection with a remote computer user similar to using a standard phone

handset. This connection is usually peer-to-peer in implementation and can offer audio, video and data transfer capabilities.

Means of Knowing:

A server may keep track of which users have the software installed and will maintain a directory of which users are available to receive/establish a connection. Call records (time/date, source, destination) is sometimes available and can be logged.

j) Market place

An online marketplace is a website where practically anyone can buy or sell practically anything. They empower consumers by:

- increasing choice in terms of the wide selection of goods available in over 50,000 categories;
- making the comparison of price and services easier for the consumer through greater price transparency;
- making inefficient markets more efficient, in many cases reducing prices; and
- by empowering SMEs to access global markets and compete with larger, more established companies and traditional 'bricks and mortar' businesses.

Means of Knowing:

Operators of such marketplace are usually not involved in (i) the actual transaction between buyers and sellers, (ii) in control of the quality, safety or legality of the items advertised, (iii) in control of the truth or accuracy of the listings or the ability of sellers to sell items or the ability of buyers to buy items, (iv) at any time in possession of the goods listed; or (v) able to inspect the goods listed.

k) Others

There are a wide range of other services being developed and tested on the Internet. These include direct voice over Internet, music and radio broadcasts using the Internet, video streaming applications, video conferencing, and many others.

Means of Knowing:

Depends on the service in question.

### 2.3.3 Conclusion

The data travelling across the Service Providers network operations centre is processed automatically and unless deliberately intercepted is rarely seen, read or recorded by human operators. The volume and complexity usually negates any reasonable analysis without prior knowledge and specific targeting of potential abuse. The Right to respect for private life prohibit any ad-hoc traffic analysis except on receipt of a documented and legitimate request from an accredited Authority.

Service Providers are usually considered common carriers (i.e. not liable for content) in those services which provide connection services to the Internet for the transmission and receipt information.

## **2.4 Profile of law enforcement agencies**

Law enforcement structures are varied around the world and are based on individual national history, policies and experiences in each country so that a generally binding statement on the legal framework and structure of law enforcement agencies throughout Europe and/or the world cannot be easily made. The following description is strictly limited to law enforcement (excludes judicial systems, etc) and should be understood as an effort to describe in a very minimalist way the functioning of law enforcement based on experience whilst some other systems are left uncovered.

It would be useful to understand not only how LEAs are structured, but also which LEAs are legally empowered to request and obtain access to user information. In addition we need to review what agencies are considered part of Law Enforcement - for instance are customs, data protection authorities, consumer protection authorities, injunction from civil courts, secret services included?

### **2.4.1 Legal Framework**

When profiling Law Enforcement Authorities it is necessary to take into consideration the differences between centralised countries like France and Federal States like the US and Germany;

When describing the responsibilities of police, the two most important areas have to be mentioned: crime prevention and criminal prosecution.

- a) The first means the protection of people and property or, the assertion of public safety. In order to protect people (even from themselves) police had and will have to inquire, for example, cases where persons announce publicly (eg. in Internet fora) their suicide or plans to run-amok in a school or university.
- b) The second means the pursuit of legal proceedings, particularly criminal proceedings or, the protection of society from criminals and crime.

In both areas police might face the necessity for obtaining information or data from Internet industry.

Some countries have the Principle of Discretionary Prosecution<sup>57</sup> – for example, the United Kingdom – whereas others have the Principle of Mandatory Prosecution – for example, Germany. In case of Mandatory Prosecution law enforcement does not have the "freedom of choice" to investigate or not; in fact, once a suspicion of crime comes to the attention of law enforcement, they have to do all the necessary to clearing up the facts. This could mean that – in a

---

<sup>57</sup> Discretion is the power, held by police officers to decide whether and how, within legal bounds, they enforce the law. Prosecutors in principle have the discretion not to initiate or continue with proceedings if it is not in the public interest to prosecute. (Gooch/Williams: Oxford Dictionary of Law Enforcement, Oxford University Press, 2007)

worst case scenario – thousands of email or IP addresses have to be checked with Internet industry.

For Internet Service Providers it is not always immediately clear which law enforcement personnel are really empowered to ask for information.

#### **2.4.2 Local and National Agencies**

Some countries are centralised – like, for example, France – whereas others are Federal States – like, for example the US and Germany. Centralised countries in general have central agencies responsible for investigating on national level or, at least, coordinating investigations in an ordering/commanding capacity.

In Federal States the responsibility for law enforcement and investigations respectively is, in general, broken down to the states and their local representatives. Depending on the national law enforcement structures even small local law enforcement agencies are, therefore, entitled to contact service providers for obtaining information or data. This has to be taken into consideration when addressing the setting up structures on national level.

#### **2.4.3 National Agencies/ Centres of Excellence**

There are also many other units or departments which are part of Law Enforcement which send requests to Internet Service Providers. These include:

- Federal agencies
  - Multi-discipline task forces
  - Adhoc-investigation teams
- Specialist Agencies
  - Fraud Investigations
  - Child Protection
  - Computer Crime
  - Terrorist Investigations

#### **2.4.4 International agencies**

##### **Interpol**

Interpol is actively involved for years in combating IT crime worldwide. Within the Financial and High Tech Crime Sub-Directorate of the Interpol General Secretariat a small group of specialists from all over the world deals with all types and aspects of IT crime. The Interpol General Secretariat facilitates information exchange, provides operational police support, contributes to investigations with research and analysis on crime trends and organises conferences (eg. BotNet Task Force) and meetings on current topics (eg. Phishing). In its commitment to stop criminals and protect consumers the Interpol General Secretariat develops strategic partnership with other international organisations and private-sector bodies such as Internet Service Providers, Software Companies and Central Banks. It also provides administrative support for the Regional Interpol Working Parties on IT crime

which have been set up in Africa, Asia – South Pacific, Latin America and Europe.

Established in 1990 by the Interpol European Regional Conference, the Interpol Working Party on IT Crime – Europe (IWPITC-E) is the longest standing regional working party and meets three times a year. So far; the IWPITC-E consists of experts of IT crime units from 15 European member states. Aims of the IWPITC-E are:

- cooperation, sharing of knowledge and practical experience, discussing IT crime, finding solutions to the problems that arise and proposing recommendations with a view to assist-ing Interpol member countries to prevent, detect and combat such crime;
- promotion of standardisation of methods and procedures, special projects, training programmes and cooperation with other international organisations;
- establishment of good practice guidelines for relevant investigations and make them available to Interpol member countries (eg. IT Crime Manual).

With regard to the technical nature of IT crime, many Interpol member countries have set up specialized law enforcement units which are responsible for implementing urgent action at national level when requests relating to IT crime are circulated on international level. To ensure that the information exchanged through the appropriate Interpol channels reaches the specialized law enforcement units with the least possible delay, a list of National Central Reference Points (NCRPs) for IT crime has been compiled by the IWPITC-E. To date, 110 National Central Bureaus have designated such a NCRP.

This list of NCRPs is a fundamental part of the so-called IT Crime Manual (ITCM) which is produced by the IWPITC-E in cooperation with IT specialist from law enforcement and the private sector. It is published by the Interpol General Secretariat and available on the secure Interpol Website and on CD-ROM. The ITCM is a best practice guide for IT crime investigators and describes and lists investigation tools in detail. It covers, amongst others, the following topics: criminal threats against e-commerce, electronic means of payment, manipulation of public communications networks, internet investigations, Voice-over-IP and wireless technology.

### **Europol**

In 2002 Europol had set up a High Tech Crime Centre (HTCC) within the Department for Serious Crime. The main objective of this unit is to maintain a high level of expertise in combating high tech crime through coordination, training and operational support. The HTCC supports the member countries in the exchange of expertise and best practice and stimulates cross-border information exchange in this particular field. Furthermore, the HTCC provides strategic analysis, supports the member countries in high tech crime investigations and assists developing specialist law enforcement techniques. Hereby the focus is on research, digital forensics and cyber crime training. One

of the important vehicles to encourage the exchange of information and expertise is Europol's High Tech Crime Expert Meeting where all the High Tech Crime Units in Europe are involved. From a policy perspective the HTCC participates in initiatives on high tech crime such as the European Commission, the Council of Europe, the United Nations and other regional or global initiatives. Besides the day to day contacts with the respective units in the member countries, the HTCC cooperates with international organisations such as Eurojust and Interpol.

## **G8**

The Heads of the G8 countries (i.e. Canada, France, Germany, Italy, Japan, Russia, United Kingdom and United States of America) decided at their 1995 Summit in Halifax to set up a "G8 Senior Experts Group on Transnational Organized Crime" which should evaluate existing international agreements and mechanisms relating to the fight against organised crime and propose remedies for identified loopholes. The experts submitted a catalogue of 40 operational recommendations which were approved by the 1996 Summit in Lyon. The Summit mandated the Expert Group – called "Lyon-Group" since – to put the recommendations into practice within the G8 countries and worldwide, if possible. This Group of Experts consists of several subgroups and meets three times a year – since October 2001 together with the "Roma-Group" on terrorism.

Two achievements of the subgroup called "High Tech Crime Subgroup" have a great impact not only on the work of the G8 countries but also on a number of affiliated countries world wide: the setting up of a 24/7 Network of Contact Points and the introduction of a so-called "Preservation Order".

The G8 24/7 Points of Contact are provided for investigations involving electronic evidence that require urgent assistance from law enforcement abroad. In investigations involving computer networks, it is often important to preserve electronic data and locate suspects as quickly as possible, often by asking Service Providers to assist by preserving data. Therefore, to enhance and supplement – but not replace – traditional ways of obtaining assistance, the G8 has created this 24/7 Network of Contact Points as a mechanism to expedite contacts between participating countries.

To use this network, law enforcement seeking assistance from a foreign country may contact the 24/7 Point of Contact in their own country, and this will, if appropriate, contact the counterpart in the foreign country. Countries in the network have committed to make their best efforts to ensure that Service Providers freeze the data sought by means of a "Preservation Order" as quickly as possible and to make their best efforts to produce this information expeditiously. So far, 50 countries have joined that network.

## 2.5 Current relationships

Many relationships between Internet service industry and Law Enforcement have been operating for several years. At one extreme some have been created on an ad-hoc basis and at the other extreme some have been mandated by national regulations.

### o Types of formal relationships

In November 2007, the German eCommerce Association (eco) formalised the good cooperative relationship with the BKA (Federal Criminal Police Office in Germany) and signed an agreement with the BKA at the annual conference of the BKA to cooperate with regards to dealing with illegal material. eco also organizes technical and legal workshops for Law Enforcement in Germany. The next workshop is planned for April 2008.

eco as co-operator of the complaint hotline IBSDE ([www.internet-beschwerdestelle.de](http://www.internet-beschwerdestelle.de)) is member of "Deutschland sicher im Netz" ([www.sicher-im-netz.de](http://www.sicher-im-netz.de)) the largest safety initiative in Germany. "Deutschland sicher im Netz" (DSIN) is a coalition of several large enterprises and associations of the internet industry. The aim of the initiative is to give the general public tools and information to use the internet in a safe and secure way. On 19th June 2007 the collaboration agreement between DSIN and the German Federal Ministry of Interior was signed at a press conference, that was highly featured. The Federal Minister, Dr. Wolfgang Schäuble, is now the patron of the Association and DSIN is the official private partner of the Ministry in security matters.

In the USA, eBay Inc. established the Fraud Investigations Team (FIT) to promote the safe use of its platforms and to collaborate with local, state, federal and international law to enforce policies, prosecute fraudsters and help keep the community safe. Law enforcement agencies in North America seeking assistance and records for investigations that relate to either the eBay marketplace or PayPal financial transactions may contact the Fraud Investigations Team directly, or for use the automated First Responder Service provided by eBay partner [leadsonline.com](http://leadsonline.com). Law enforcement can:

- Search eBay listings and obtain eBay records fast by registering online.
- Call eBay's automated information number to learn more about the types of records available from eBay and PayPal.
- Fax a request for information to eBay/PayPal FIT
- Email eBay to obtain information on how to accurately request records.

The French Internet Access and Service Providers Association (AFA) has been involved since 2003 in training sessions about co-operation between ISPs and LEA, organised by the NTEC (specialized investigators in High tech crimes) and the French National School for the Judiciary.

Internet Service Providers use technology and other valuable resources to support the efforts of Law Enforcement Agencies to disrupt the operations of cybercriminals:

- **Technology**

eBay Law Enforcement CD Project. The eBay/PayPal Fraud Investigation Team has developed a Windows interactive CD to assist law enforcement with the information received for each legal request. A copy of the CD is sent by a member of the Fraud Investigation Team with each request for information. Any law enforcement agency which has not received a copy of the CD, can request a copy by sending a letter request on department letterhead to eBay.

Microsoft Child Exploitation Tracking System (CETS). Microsoft has worked with countries to implement CETS, which enables law enforcement investigators to easily and securely import, organize, analyze, share and search information regarding online child exploitation. CETS was initially deployed in Canada, and it already has played a part in several investigations across geographical boundaries. Since the initial deployment, other countries – Indonesia, Italy, the United Kingdom, Brazil and Spain among others -- have implemented CETS or are in the process of implementing it.

- **Policy**

Since September 2006 Microsoft supports the Council of Europe ("CoE"), a group of 44 member States, in implementing the Cybercrime Convention, which was signed in November 2001<sup>58</sup>. Under the Convention, signatories agreed to implement criminal laws against activities such as hacking, online fraud, and child pornography. They also agreed to establish appropriate tools to investigate and punish violations of these laws, including cross-border cooperation and extradition. Microsoft is the first private donor to the Council of Europe in the history of this institution. Its support is not only financial, but in providing the support from the national Microsoft teams. This includes facilitating cooperation and communication between the Council of Europe and local cybercrime experts from government, parliament and industry. This helps the Council of Europe to provide training and advise interested countries to help implement the provisions of the Convention.

- **National partnerships for Capacity Building**

eBay UK Law Enforcement Liaison. eBay's UK Trust and Safety teams include former law enforcement officials from around the world. eBay encourage the Police, trading standards and other government agencies to contact the eBay team directly.

Microsoft Memorandums of Understanding. Since 2005, Microsoft has signed 4 Memorandums of understanding with various authorities in Europe and Africa (Ministry of Justice, Ministry of Interior, Judicial Police, economic authority) for the purpose of Microsoft to provide forensics trainings on site or at events (at events like LE Tech<sup>59</sup> or the Interpol Botnet Taskforce), share its networks of experts as well as intelligence on trends.

---

<sup>58</sup> [http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/Default.asp#TopOfPage](http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/Default.asp#TopOfPage)  
<sup>59</sup> [www.microsoft.com/mscorp/safety/legislation/default.mspx](http://www.microsoft.com/mscorp/safety/legislation/default.mspx)

- **Types of informal relationships**

Examples of technical support and intelligence sharing between Internet Service Providers and Law Enforcement Authorities include:

- **Technical Support**

eBay ELBA (Elektronisches Bearbeitungssystem fuer Auskunftersuchen - Electronic LE-Requests Processing System) eBay has to handle a significant amount of data requests from many different law enforcement authorities (LEA). To establish a secure, fast and convenient communication channel between LEAs and eBay, eBay introduced ELBA in Germany, UK and Italy. Accredited LEAs can send their standardized requests online to eBay via the system. Within minutes an eBay employee checks if the requests are legitimate and then the system creates a PDF file with the data for the requesting LEA. (To ensure that ELBA meets all privacy requirements the Data Protection Authority in charge for eBay Germany has been involved in the development of ELBA right from the beginning.)

The system has become a great success. Today more than 80 authorities including BKA, different LKAs and police other units, often specialised on online crime are using it in Germany alone.

Microsoft Law Enforcement Portal. In August 2006, Microsoft has launched a website portal for law enforcement authorities around the world. The Law Enforcement Portal ([www.microsoftlawportal.com](http://www.microsoftlawportal.com)) is designed to provide law enforcement with easy access to training material and resources related to cybercrime. This portal is a response to the growing volume and variety of requests from law enforcement to Microsoft, related to its software, game or online services. The materials include summaries of various online threats – including children’s safety, phishing, spyware, spam, and malicious code – and information about organizations, partnerships, and other resources available to help law enforcement understand, investigate, prevent, and address these threats.

- **Digital PhishNet**

In December 2004, Microsoft announced the DigitalPhishNet (DPN), an alliance between law enforcement and industry leaders in a variety of sectors including technology, banking, financial services, and online auctioneering. This alliance is directed specifically at sharing information in real time about phishers to assist with identification, arrest, and prosecution. DPN is the first group of its kind to focus on assisting law enforcement in apprehending and prosecuting those responsible for committing crimes against consumers through phishing.

It provides a neutral, confidential and collaborative forum between the private and public sectors where information about instances and trends of phishing and related cyber-threats can be shared in confidence, analyzed, and referred to law enforcement and various anti-phishing services, leading to aggressive enforcement and deterrence of future online offenses. It is managed by National Cyber-Forensics & Training Alliance (NCFTA), a non-profit public/private organization in the US, with staff from both law enforcement and industry. NCFTA provides training and support for LE, it

connects law enforcement with industry experts for analysis and forensics. NCFTA is funded and supported by its members. DPN is organizing closed meetings between industry and law enforcement to facilitate cooperation. After Chicago in 2005 and New Orleans in 2006, DPN expanded to Europe with Berlin in June 2007 and to Asia with Singapore in January 2008.

### **ECO Newswatch Project**

The German ECO Internet Content Task Force working group, deals with the issue of the protection of minors and combating harmful and illegal content on the Internet. In this connection, ICTF created a project called NewsWatch. This is not a public hotline but a service for business participants of the ICTF working group. In cases where the participating ISPs receive complaints from users or find suspicious material themselves on their servers, they can deliver a newsfeed to NewsWatch for content rating by legally educated personnel. The results of the rating then facilitate the decision of the ISPs whether or not to continue to offer such newsgroups or postings to their customers. A major enhancement has been the establishment of an interface to the public and the possibility for participating ISPs to request so called "cancel feed" for the auto-deletion of illegal material from their news-servers.

### **ECO SpotSPAM Project**

The Spotsam project, a pilot project financially supported by Microsoft EMEA and the EU's Safer Internet Programme facilitates the cross-border fight against unsolicited electronic communication. Project partners eco and NASK have established a prototype database to collect information relevant to the prosecution of spammers based on end-user complaints and other relevant data. The complaints are gathered through national spamboxes, which can be operated either by public or private bodies, such as hotlines. The SpotSpam database provides information to facilitate legal action against spammers and their beneficiaries. The idea of SpotSpam is to provide those parties that take legal action with a resource of numerous end-user complaints originating from different countries that they otherwise would not have received to make their cases stronger. Hence the SpotSpam database helps to grab the root of the problem by encircling the spammer and spammer's helpers on an international level, and enables the victims, may it be individuals, trademark owners, banks or ISPs to successfully enforce applicable laws.

### **French "Signal spam" project**

"Signal spam" is a French association, with AFA as a founding member, created in November 2005 thanks to the platform of public/private works of dialogue lead by the Media Development Direction, a service of the Prime Minister. The aim of the association is to gather the efforts of most public and private French organizations concerned by the issue of spam. It notably provides users with a set of recommendations and a reporting mechanism, aimed at enabling public authorities and the Internet Industry to fight spam according to their respective field of competence.

### **AFA Hotline against illegal activities**

Since 1998, AFA operates a hotline/tipline against illegal activities on the Internet and is founding member of INHOPE – the global network of Internet

hotlines. In that framework, AFA has contacts with many French Police forces. On a day-to-day basis, Point de Contact cooperates with the Central office against cybercrime (OCLCTIC). Point de Contact forwards to OCLCTIC reports on illegal content as child pornography and incitement to racial hatred assessed as potentially illegal.

- **Technical Guidance on Methodology of Investigations**

Microsoft has developed materials to help law enforcement officials understand the ways in which available technology and software can be used to investigate cybercriminals. These materials include information relating to the technical details of Microsoft's products and guidance for conducting investigations on computers and other devices using Microsoft software.

Internet Service Providers offer training to government officials and field agents to assist with their efforts against cybercrimes:

- **Trainings organized by Internet Service Providers**

In October 2006, Microsoft has hosted the "LE Tech 2006" conference at Microsoft headquarters in Redmond, Washington. Gathering around 300 international law enforcement officers from over 45 countries, the event has introduced law enforcement officers from around the world to Microsoft's newest efforts to assist in cybercrime investigations, including the Child Exploitation Tracking System (CETS), Microsoft's new Law Enforcement Portal, and Microsoft's enforcement programs.

In Germany, eco organizes regularly legal and technical workshops for the abuse teams of ISPs. These seminars are now regularly delivered since they have been considered very useful by the staff participating.

For 2008 eco plans in cooperation with the Federal alliance of the German detectives (Bund deutscher Kriminalbeamter – BDK) a technical and a legal workshop as a road show throughout Germany for the staff of LEA. eco has developed a range of technical and legal materials to help law enforcement officials and detectives better understand the specific internet technical issues and to discuss together the current legal trends and topics.

- **Trainings supported by Internet Service Providers**

The Microsoft supported, Computer-Facilitated Crimes Against Children training seminar was designed to provide law enforcement around the world the tools and techniques needed to investigate Internet-related child-exploitation cases. This initiative was launched in December 2003 at Interpol Headquarters in Lyon, France. ICMEC has organized trainings in 26 other cities in every corner of the world: San Jose, Costa Rica; Brasilia, Brazil; Paarl, South Africa; Zagreb, Croatia; Hong Kong, China; Bucharest, Romania; Madrid, Spain; Amman, Jordan; Buenos Aires, Argentina; Moscow, Russia; Wellington, New Zealand; Bangkok, Thailand; Istanbul, Turkey; Tokyo, Japan; Oslo, Norway; Dalian, China; Sofia, Bulgaria; Brisbane, Australia; Muscat, Oman; New Delhi, India; Vilnius, Lithuania; Rabat, Morocco; and Doha, Qatar; Panama City, Panama; Manila, Philippines; and Warsaw, Poland. As of September 2007, 2,413 officers from 106 countries have been trained.

The four-day seminar, which ICMEC conducts in conjunction with Interpol, includes the following modules: Computer-Facilitated Exploitation of Children, Conducting the Online Child Abuse Investigation, Managing the Law-Enforcement Response to Computer-Facilitated Crimes Against Children, and Technical Aspects of the Investigation, and Tools and Techniques for the Prosecutor. Trainings co-organized with participating law enforcement agencies

#### Europol

In January 2008, Microsoft and eBay/PayPal/Skype provided a five day trainings to more than 40 experienced computer related crime investigators from the European Union Member States on malware and botnets<sup>60</sup>. In June 2006, Microsoft organized with Europol a 4 day training course for 24 high tech crime investigators from 15 members countries and in addition 12 people from Europol High Tech Crime Center and other specialized units of Europol. The training covered advanced Windows XP Forensics above and beyond what the available tools cover, MS Office Metadata and Hiding Techniques, Botnet Malware Detection and Analysis, Windows Vista Security Preview and Demo as well as the ICI team's response to the malware threat. Access was granted. Microsoft Windows Vista BETA was also discussed<sup>61</sup>.

#### European Union

eBay has signed a partnership declaration with Europol to support all future European Law Enforcement trainings in 2008.

Microsoft has partnered with Interpol, the EU and 15 EU Member States to help fund the AGIS Project, which emphasizes cooperation among public and private entities in fighting cybercrime. The Project promotes standardized training programs and information networks across participating countries. The AGIS project came to its conclusion, and its successor is ISEC, under the new programme "Prevention of and Fight against Crime as part of the general programme Security and Safeguarding Liberties"<sup>62</sup>. Microsoft is working to participate in this new program.

#### National trainings, a few examples

In October 2007, Microsoft partnered with the Office of the Massachusetts Attorney General Martha Coakley to deliver Internet safety investigations training to law enforcement officers. Over 300 law enforcement officers from across Massachusetts attended the training at Microsoft's Waltham campus.

In August 2006, a Windows Mobile Forensics forensics class has been completed in Stralsund, Germany, in August 2006, covering Windows Mobile 5 and Smartphone architecture, memory mapping, file system, registry, security, and forensic data acquisition approaches. 38 students has been trained, all being experienced forensic examiners with a very high level of technical knowledge from several German investigative agencies as well as some Swiss police. In February 2005, LKA Lower Saxony, German Federal Armed Forces and Microsoft jointly organised a 5 day forensics and botnet training for 140 officers from 7 countries in an Army Officer Academy of the German Federal Armed Forces.

---

<sup>60</sup> <http://www.europol.europa.eu/index.asp?page=news&news=pr080117.htm>

<sup>61</sup> <http://www.europol.europa.eu/index.asp?page=news&news=pr060615b.htm>

<sup>62</sup> [http://ec.europa.eu/justice\\_home/funding/isec/printer/funding\\_isec\\_en.htm](http://ec.europa.eu/justice_home/funding/isec/printer/funding_isec_en.htm)

Initiatives taken by eBay include:

- o The Nigerian Economic Financial Crimes Commission
- o Training of 60 criminal judges/prosecutors organized by Berlin Senate of Justice.
- o A Joint Training Session /conference conducted by eBay, CBI and Interpol for Top 350 LE officials in India.
- o The majority of detectives within the UK's Serious and Organised Crime Agency (SOCA) have been trained throughout the year and continuing into 2008.
- o National Magistrates Institute, Bucharest Romania – "Train the trainers" session for 2 groups of judges and prosecutors.
- o Europol's High Tech Crime Expert meeting at The Hague. Also a member of the Europol Working Task Force, currently developing training curriculum for '08.
- o Trained investigators from all over world at the Digital Phish Network, Berlin – a private/public forum, cosponsored by PayPal.
- o Chisinau, Moldova – one week joint training with FBI. As a result, a network of mules moving high value items from Moldova to Romania was stopped

Microsoft directly assists in investigations and enforcement actions against cybercrime:

- o In November 2006, Microsoft announced that it took 129 legal actions – including 97 criminal complaints and 3 civil settlements – in Europe, Middle-East and Africa against phishers targeting MSN Hotmail users. Of the 97 criminal complaints, 50 have been filed in Turkey, 28 in Germany, 11 in France. Most phishers have been located in Turkey, France, Morocco, as well as in Italy, UAE and the Netherlands.
- o In January 2006, Microsoft helped Bulgarian authorities arrest eight members of an international criminal network known as the Microsoft Billing Account Management (MBAM) Gang. The group spoofed emails and created fake web pages in as part of a coordinated attack in eleven countries to induce MSN customers to reveal their personal information. The operation resulted in over US\$50,000 in fraudulent purchases and money transfers. Microsoft provided investigative and technical assistance to Bulgaria's National Services to Combat Organized Crime (NSCOC) agency, who ultimately identified and apprehended the phishers.
- o In August 2005, Microsoft provided technical and investigative support to Turkish and Moroccan authorities in the arrest of the Zotob and Mytob worms<sup>63</sup>.
- o **Strengths/weaknesses of both**

Formal cooperation is more sensitive than informal cooperation, as it requires formal endorsement at the highest level from both sides. Once a formal cooperation is set up, it has more chances to resist to the change of staff within the company or the authority. In addition to a more robust framework, it pushes

---

<sup>63</sup> <http://www.microsoft.com/presspass/press/2005/aug05/08-26ZotobArrestPR.msp>

both sides to adopt a more political and strategic approach to the issue of cooperation on cybercrime. It broadens the topic from a technical topic for experts (lawyers, investigators, abuse teams) to a political commitment.

### **2.5.1 Industry Comments**

Most internet Industry have traditionally a good relationship with Law Enforcement especially investigating security breaches, Child Pornography investigations and believe very strongly in the effectiveness and balanced approach of the EU eCommerce Directive.

There is still much confusion between both sides about the legal and technical situation. What can be done legally? What is required to be done legally? What is technically feasible? A simple/ common form for requests and responses would improve existing level of information exchange – technically and legally. Knowledge building workshops would also be helpful.

There is a need to build on existing knowledge – without too much detail about regulation – which will help promote the relationship further.

Law enforcement should consider implementing the best practices set forth below to help establish uniformity in the interactions between law enforcement and service providers and to encourage law enforcement to make the best use of service provider resources.

### **2.5.2 Law Enforcement Comments**

Internet industry holds information which is essential to solve cybercrimes and prosecute cybercriminals. Working with national private sector entities is easier since it is defined in national law. The challenge therefore is how law enforcement can work with non-national organisations. Co-operation of LEAs in one country with ISPs in another country causes particular problems in investigations:

#### a) Admissibility of evidence

In most countries evidence has to be obtained through appropriate channels and by formal legal assistance. Evidence cannot be used in court if not obtained by formal legal assistance. Thus, information or data acquired by direct contacts between law enforcement and a service provider abroad is useless and can even imperil the investigations.

#### b) National sovereignty

National sovereignty is affected when foreign law enforcement contacts domestic service providers in order to obtain, for example subscriber information or traffic data. Such a request is regarded as examination of a victim and therefore requires appropriate legal assistance procedures.

#### c) Lack of awareness of law enforcement

Law enforcement in the country of the service provider contacted from abroad would not be aware of foreign investigations affecting the own country. Domestic investigations could be affected if, for example the foreign and domestic investigations target the some criminal. On the contrary if domestic law

enforcement were aware of these investigations abroad proceedings could be coordinated and/or harmonized.

The German Federal Criminal Police has established a working party on botnets in which the German Federal Office for Information Security and ISP meet occasionally to improve the information exchange on national level, explore legal and technical possibilities to detect and investigate botnet activities.

### **3 Working together/ processing requests**

The success of both, national and international cybercrime investigation does heavily depend on the availability of certain data. Having access to such information can enable the law enforcement authorities to trace back to offenders or take down servers with illegal content. In the majority of cases the relevant data is not in the possession of state organisations but generated and stored by Internet Service Providers. As a result data related requests from law enforcement agencies are an important area of cooperation.

The issue of cost associated with cooperation is a major issue for both parties and the reimbursement of same is an important issue in this study. Issues of cost reimbursement or fair compensation to relevant parties should be considered.

The following chapter provides an overview about the most common requests. It focussing but not limited to the procedural instruments provided by the Convention on Cybercrime.

#### **3.1 Processing data-related Requests**

IT crimes today differ dramatically from traditional crimes seen before. They pose new challenges to law enforcement, limit their possibilities for investigations and thus re-quire new approaches to identify criminals and collect evidence.

In a "real" case, most criminals leave evidence such as fingerprints, DNA, or other physical traces when interacting with the victim and/or target. They might use cars with number plates and be observed by witnesses or cameras - at least they will have to leave in most of the cases their safe harbour for even a small activity/action.

IT crime on the contrary does not necessitate a physical presence of the criminal at the scene of the crime. He or she "virtually" (in a double sense of meaning) can commit the crime thousands of kilometres away from the victim and/or target – even from his home or office, not noticed by anyone.)

##### **3.1.1 Introduction - Reasons why data is requested**

There are usually two main reasons why law enforcement make request to Internet industry for data disclosure

- Criminal/National Intelligence gathering
- Judicial aspects of a criminal investigation

Such requests are for several different areas:

###### a) Identification of offenders and crimes

IP addresses are in most cases the only evidence/clue available to identify offenders and crimes. So law enforcement has to request the disclosure of traffic data – provided the required data have been retained by the ISP. Email address are in many cases not reliable since they can be fraudulently obtained by bogus registration using fake identities (freemailers normally do not have

verification procedures) or they are been altered by means of free available software (so-called "email spoofing"<sup>64</sup>).

b) Evidence gathering

After having identified an offender, law enforcement need to substantiate the offence, search for additional charges or exoneration and set up a chain of evidence (e.g. if several servers have been used consecutively). In those cases traffic data and/or log files will have to be gathered and analysed.

c) Exoneration of innocent third parties

Information technology enables criminals to conceal their identities from law enforcement by, for example, email spoofing; privateering computers or accounts of unsuspecting Internet users; or using proxy servers. As a result innocent third parties – being sometimes victims themselves – become a target for law enforcement. In those cases traffic data and/or log files need to be gathered and analysed in order to exonerate the wrong and charge the right.

### **3.1.2 Introduction - Reasons why data is needed urgently**

There are usually two main reasons why law enforcement make urgent requests to Internet industry for data disclosure:

a) Volatility of data

Depending on the privacy laws in the different countries especially traffic data are retained only for a certain period of time, ranging from seconds till years. The quicker law enforcement requests data disclosure from Internet industry the higher is the chance to obtain the data before destruction. There are even cases where the criminal is still on-line when asking for the traffic data.

b) Data needed for further investigations

Especially in case where the data required are the only evidence/clue available the disclosure is needed without the slightest delay in order to not imperil the success of the investigation. If the evidence shows that the computer was just used as a hop/proxy further enquiries have to be made immediately to follow the trace back to the criminal. The fact that in many or even the most cases computers abroad are implicated complicates the situation and calls for urgent reaction in order to avoid that retained data are erased (depending on the privacy laws in that country) during the generally time-consuming process of Mutual Legal Assistance.

---

<sup>64</sup> Fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used for spam email and phishing hide the origin of an email message. ([www.wikipedia.org](http://www.wikipedia.org))

### 3.2 Analysing different kind of requests

As pointed out above computer data can in different ways be necessary for investigations. LEA might order the preservation of certain content data to ensure that those information are not deleted and can be used to prosecute the suspect. This is especially relevant in child pornography cases where the ISP hosting websites with such illegal content can ensure that the offenders are unable to delete the evidence. Another example is the assistance in the lawful real time collection of traffic data. The application of such instruments can for example be necessary to identify an offender or the services that are used within criminal activities. Both request are related to different kind of data and require different action to be taken by the recipient of the request.

#### 3.2.1 Expedited preservation of data (Art. 16.1 CoC)

##### a) Introduction

The identification of an offender, who committed a Cybercrime does very often require the analysis of traffic data.<sup>65</sup> In this context especially the IP address used by the offender can be important for the law enforcement agencies to trace him back. One of the main challenges for investigation is the fact that traffic data that are relevant for the information are often deleted automatically within a rather short period of time. The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an e-mail, accessing the Internet or downloading a movie) those traffic data that have been generated during the process and that ensure that the process could be carried out are not anymore needed. With regard to economic aspects most ISP are interested in deleting the information as soon as possible. Storing the data for longer periods would go along with the need for larger (expensive) storage capacities.<sup>66</sup>

Economic aspects are just one reason why law enforcement agencies need to quickly carry out investigation. Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example for such restriction is Art. 6 EU Directive on Privacy and Electronic Communication.<sup>67</sup>

Art. 16 CoC enables the law enforcement agencies to order the preservation of traffic as well as content data ("quick freeze"). This instrument that should enables the law enforcement agencies to react immediately after becoming aware of an offence and avoid the risk of a deletion as a result of long lasting procedures.<sup>68</sup>

---

<sup>65</sup> "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155.; Regarding the identification of suspects by IP-based investigations see: *Gercke*, Preservation of User Data, DUD 2002, 577 et. seqq.

<sup>66</sup> The cost issue was especially raised within the discussion about data retention legislation in the EU. See for example: E-communications service providers remain seriously concerned with the agreement reached by EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: <http://www.ispai.ie/EUROISPADR.pdf>; See as well: ABA International Guide to Combating Cybercrime, page 59.

<sup>67</sup> 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). The document is available at: [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf).

<sup>68</sup> However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

The order pursuant to Art. 16 does only oblige the provider to save those data that were processed during the operation of the service and have not been deleted prior to the request.<sup>69</sup> Art. 16 does not force the offender to reconfigure the computer system in a way that it collects data that would normally not collected.<sup>70</sup> In addition Art. 16 does not contain an obligation of ISP to transfer the relevant data to the authorities. The provision does only authorise the law enforcement agencies to prevent the deletion of the relevant data but not to pledge the providers to transfer the data. The transfer obligation is regulated in Art. 17 and 18 Convention on Cybercrime.

b) Best practice examples:

- Precise description of the data to be preserved
- Indication if only the existing data should be preserved or future activities should be monitored (different instrument)

c) Bad practice

- Imprecise orders
- Data preservation requests that are not followed by a production order

### 3.2.2 Data Retention obligations

The challenges for investigations related to the non permanent nature of computer data can be addressed in various ways. As pointed out above the Convention on Cybercrime is based on the principle of "quick freeze". Another approach that is currently discussed is data retention. Based on a data retention obligation forces the provider of Internet services are obliged to save all traffic data for a certain period of time.<sup>71</sup> In the latest legislative approaches the records need to be saved for 6 up to 24 month.<sup>72</sup> This would enable the authorised agencies to gain access to data that is necessary to identify an offender even month after the perpetration.<sup>73</sup> A data retention obligation was recently adopted by the EU Parliament<sup>74</sup> and is currently discussed in the US.<sup>75</sup>

---

<sup>69</sup> 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

<sup>70</sup> Explanatory Report No 152.

<sup>71</sup> Regarding The Data Retention Directive in the EU see *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1 – available at: [http://eprints.law.duke.edu/archive/00001602/01/8\\_Chicago\\_Int'l\\_L.\\_233\\_\(2007\).pdf](http://eprints.law.duke.edu/archive/00001602/01/8_Chicago_Int'l_L._233_(2007).pdf); *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et. seqq.

<sup>72</sup> Art. 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.

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). The document is available at: [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf).

<sup>73</sup> See: Preface 11. of the EU Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

<sup>74</sup> 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

The effectiveness of such instrument is controversially discussed. Seen from an ISP's perspective the data preservation is a less intensive and less cost intensive instrument compared to data retention.<sup>76</sup> Based on Art. 16 the ISP do not need to store all data of all users but only have to ensure that specific data are not deleted as soon as they receive an order by a competent authority. Analysing the provision from a data protection / civil liberties perspective could as well lead to concerns related to data retention. Not only from a provider's point of view but also from the data protection perspective data preservation offers advantages compared to data retention.

The fact that information about all user communications will be covered by the Directive lead to intensive criticism from human rights organisations.<sup>77</sup> It is not necessary to preserve the data from millions of Internet users but only those that are related to the suspect of criminal investigations. But within this discussion it is as well necessary to take the investigators demands into consideration. In those cases where data are deleted right after the end of the perpetration data preservation order would – unlike a data retention obligation – not be able to prevent the deletion of the relevant data.

Concerns related to data retention obligations could lead to a review of the Directive and its implementation by constitutional courts.<sup>78</sup> In addition in her conclusion in the case *Productores de Música de España (Promusicae) v. Telefónica de España*<sup>79</sup> the advisor to the European Court of Justice Advocate General Juliane Kokott pointed out that it is questionable if data retention obligation can be implemented without a violation of fundamental right.<sup>80</sup> Difficulties with regard to the implementation of such regulations were already identified by the G8 in 2001.<sup>81</sup>

The drafter of the study analysed the status of the intensive and controversial discussion. Based on the result and the discussion with both, LEA and ISP the drafters decided to exclude this instruments from the development of recommendations. The ongoing discussion process should be observed to decide if amendments to the recommendations should be taken into consideration in the future.

---

electronic communications). The document is available at: [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf).

<sup>75</sup> See for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes - Internet StoppingAdults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007 – available at: <http://www.govtrack.us/congress/bill.xpd?bill=h110-837>. Regarding the current situation in the US see: ABA International Guide to Combating Cybercrime, page 59.

<sup>76</sup> See Gercke, The Convention on Cybercrime, MMR 2004, 803.

<sup>77</sup> See for example: Briefing for the Members of the European Parliament on Data Retention – available at: <http://www.edri.org/docs/retentionletterformeps.pdf>; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow – available at: [http://www.vibe.at/aktionen/200205/data\\_retention\\_30may2002.pdf](http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf); Regarding the concerns related to a violation of the European Convention on Human Rights see: Breyer, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et. seqq.

<sup>78</sup> See: Heise News, 13,000 determined to file suit against data retention legislation, 17.11.2007 – available at: <http://www.heise.de/english/newsticker/news/99161/from/rss09>.

<sup>79</sup> Case C-275/06.

<sup>80</sup> See: Advocate General Opinion – 18.07.2007 – available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top>. The court does usually but not invariably follow the advisors conclusion.

<sup>81</sup> In a G8 Meeting in Tokyo experts discussed the advantaged and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

### 3.2.3 Partial disclosure of traffic data (Art. 17.1b CoC)

#### a) Introduction

The Convention in general strictly divides between the obligation to preserve data on request and the obligation to disclose them to the competent authorities.<sup>82</sup> Art. 18 provides a clear classification. The provision combines the obligation to ensure the preservation of traffic data in cases where a number of service providers were involved with the additional obligation to disclose the necessary information in order to enable the LEAs to identify the path through. Without such partial disclosure law enforcement agencies would in some cases not be able to trace back the offender and preserve more relevant data when more than one provider was involved.<sup>83</sup>

#### b) Best practice

- Precise indication that Art. 17 shall apply as well in the data preservation request
- Information about possible destinations of the traces

#### c) Bad practice

- Art. 17 request in cases where only content data is concerned

### 3.2.4 Production order regarding content and traffic data (Art. 18.1a CoC)

#### a) Introduction

As mentioned above Art. 16 does only oblige the provider to save those data that were processed by the provider and not deleted at the time the provider receives the order.<sup>84</sup> The provision does not oblige the provider to transfer the relevant data to the authorities.

The transfer obligation is regulated in Art.18 Convention on Cybercrime. Art. 18 Convention on Cybercrime is not only applicable after a preservation order was issued. The provision is a general instrument that LEA's can make use of. If the LEA's are voluntarily transferring the requested data LEA's are not limited to seizing hardware but can apply the less intensive production order. The advantage of a separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application. With regard to the importance of immediate reaction it would for example be supportive to waive the requirement of an order by a judge and enable the prosecution or police to order the preservation.<sup>85</sup> This would enable these competent authorities to react

---

<sup>82</sup> Gercke, The Convention on Cybercrime, MMR 2004, 802.

<sup>83</sup> "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

<sup>84</sup> 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

<sup>85</sup> "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

faster. The protection of the rights of the suspect can be achieved by requiring an order for the disclosure of the data.<sup>86</sup>

b) Best practice

- Short time between the preservation request and the production order
- Clear indication of different competence with regard to preservation request and production order

c) Bad practice

- Instrument is not taken into consideration as an alternative solution to search and seizure

### 3.2.5 Submission of subscriber information (Art. 18.1b CoC)

a) Introduction

In addition to the obligation to submit computer data, Art. 18 CoC enables law enforcement agencies to order the submission of subscriber information. This investigation instrument is of great importance in IP-based investigations. If the law enforcement agencies are able to identify an IP-address that was used by the offender while carrying out the offence they will need to identify the person<sup>87</sup> who used the IP-address at the time of the offence. Based on Art. 18 Subsection 1 b) Convention on Cybercrime a provider is obliged to submit those subscriber information listed in Art. 18 Subsection 3 Convention on Cybercrime.

b) Best practice

- In addition to the IP-address as many other known identity related information (like e-mail address, computer system used, ...) should be provided on request

c) Bad practice

- Requests related to subscriber information in IP-based investigations without time related information (time and date of use, timezone).

---

<sup>86</sup> The drafters of the Convention on Cybercrime tried to approach the problems related to the need of immediate action from law enforcement agencies on the one hand side and the importance of ensuring safeguards on the other hand side in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime No. 174: „The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.“

<sup>87</sup> An IP-address does not necessarily immediately identify the offender. If law enforcement agencies know the IP-address an offender used to commit an offence this information does only enable them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café) further investigations are necessary to identify the offender.

### 3.3 Carrying out search and seizure procedures

Currently a number of innovative investigation instruments like the remote access to a suspects computer system are discussed. Despite this discussion and the availability of instruments like real-time collection of content data or the use of remote forensic software to identify and offender the search and seizure remains one of the most important investigation instruments.<sup>88</sup> As soon as the offender is identified and the law enforcement seized his IT equipment the computer forensic experts can analyse the equipment to collect the necessary evidence for the prosecution. The physical access to the hardware enables forensic experts to carry out highly efficient investigation techniques.<sup>89</sup>

#### 3.3.1 Search (Art. 19.1 and 19.2 CoC)

##### a) Introduction

Analysing various national law systems demonstrates that most national criminal procedural laws do contain provisions that enable the law enforcement agencies to search and seize tangible objects.<sup>90</sup> The reason why the drafter of the Convention on Cybercrime nevertheless included a provision dealing with search and seizure is the fact that national laws do often not cover data-related search and seizure procedures.<sup>91</sup> Some countries for example limit the application of seizure procedures to seizing physical objects.<sup>92</sup> Based on such provision the investigators would be able to seize an entire server but not seize only the relevant data by copying them.<sup>93</sup> Art. 19 Subparagraph 1 Conventions aims to establish an instrument that enables investigators to search computer systems as efficiently as they are able to perform traditional search procedures.<sup>94</sup>

Art. 19 Subparagraph 2 CoC addresses a growing problem within Cybercrime related investigations. During the search for information at the physical location of a computer system investigators frequently realise that the suspect did not store the relevant information (e.g. child pornography) on local hard drive but on an external server that he can access via Internet.<sup>95</sup> Using Internet servers to store data

---

<sup>88</sup> A detailed overview about the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et. seqq. For more information on Computer-related Search and Seizure see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et seqq.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 et seqq.

<sup>89</sup> Apart from the fact that direct access enables the law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspects computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6 – available at: <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf>.

<sup>90</sup> See Explanatory Report to the Convention on Cybercrime, No. 184.

<sup>91</sup> "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184.

<sup>92</sup> Explanatory Report No. 184.

<sup>93</sup> This can cause difficulties in those cases where the relevant information are stored on a server with the data of hundreds of other users that would not be available anymore when law enforcement agencies seize the server.

<sup>94</sup> "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

<sup>95</sup> The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning

becomes more and more popular.<sup>96</sup> To ensure that investigations can be carried out efficiently it is important to maintain a certain flexibility of investigations. If the investigators discover that the relevant information is stored in another computer system they should be able to extend the search to this system.<sup>97</sup>

b) Best practice

- Precise indication what information is relevant for the investigation
- Evaluation if a production order is sufficient for the investigation of the offence
- Seeking the assistance of ISP to locate information

c) Bad practice

- Intensive and long lasting investigations where ISP were willing to actively support the search for illegal content
- Forcing LEA to carry out physical search procedures because production orders are constantly ignored or refused

### 3.3.2 Seizure (Art. 19.3 CoC)

a) Introduction

As pointed out previously the physical examination of storage devices can be necessary within Cybercrime investigations. Art. 19 Subparagraph 3 Convention on Cybercrime enables the LEA's to seize computer hardware.<sup>98</sup> Very often – especially if the relevant data is stored on a computer system that is used by other users – the physical seize of the hardware can have great impact on people not involved in the investigation. Therefore the instruments provided by the Convention on Cybercrime are not limited to the physical seizure of the hardware. They include the act of copying the relevant data instead of seizing the hardware.<sup>99</sup> If the LEAs decide not to seize the hardware but only to copy the relevant data there are a number of side-measures that are necessary to maintain an equal efficiency compare to the seizure of the computer system itself. The most important aspect is maintaining the integrity of the copied data.<sup>100</sup> If the investigators do not have the permission to take the

---

problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543<sup>rd</sup> meeting of the Ministers Deputies. The text of the Recommendation is available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/combating\\_economic\\_crime/1\\_standard\\_settings/Rec\\_1995\\_13.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf)

<sup>96</sup> One of the advantages of storing the information on Internet servers is the fact that the information can be accessed from any place with Internet connection.

<sup>97</sup> In this context it is important to keep in mind the principle of National Sovereignty. If the information are stored on a computer system outside the territory an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be "in its territory" - Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue see as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12 – available at: <http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf>.

<sup>98</sup> For guidelines how to carry out the seizure of computer equipment see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory – available at: <http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm>; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice – available at: <http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf>.

<sup>99</sup> Regarding the classification of the act of copying the data see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 et seqq.

<sup>100</sup> "Since the measures relate to stored intangible data, additional measures are required by competent authorities to

necessary measure to ensure the integrity of the copied data these copied data may not be accepted as evidence in criminal proceedings.<sup>101</sup>

After the investigators copied the data and took measures to maintain the integrity the will need to decide how to treat the original data. Due to the fact that the investigators will not remove the hardware during the seizure process the information would in general remain there. Especially in investigations related to illegal content (e.g. child pornography) the investigators will not be able the leave the data on the server. Therefore they need an instrument that allows them to remove the data or at least ensure that they cannot be accessed anymore.<sup>102</sup> The Convention on Cybercrime addresses the above mentioned issues in Art. 19 Subparagraph 3.

b) Best practice

- Precise definition of the required information

c) Bad practice

- Copying data is not taken into consideration as an alternative instrument

### 3.3.2 Providing information (Art. 19.4 CoC)

a) Introduction

If the relevant information are stored on computer server that is part of a large IT the investigators might face difficulties in identifying the exact location of the data. It is very likely that even small and medium size hosting providers have hundreds of servers and thousands of hard disks. Very often the investigators will not be able to identify the exact location with the help of the system administrator that is responsible for the server infrastructure.<sup>103</sup> But even if they are able to identify the hard drive protection measures might stop them from searching for the relevant data. The drafters of the Convention decided to address the issue by implementing a coercive measure to facilitate the search and seizure of computer data. Art. 19 subparagraph 4 enables the investigators to compel a system administrator to assist the law enforcement agencies.

b) Best practice

- Active cooperation between ISP and LEA within search investigation
- Respecting the right of the suspect not to actively support the search for evidence

c) Bad practice

- Misleading information about the storage place or the ability to get access to the information

---

secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data". Explanatory Report to the Convention on Cybercrime, No. 197.

<sup>101</sup> This principle applies with regard to the seizure of hardware as well. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

<sup>102</sup> One possibility to prevent access to the information without deleting them is the use encryption technology.

<sup>103</sup> "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

### 3.4 Interception and collection of data

In many countries telephone surveillance is an instrument that is used in capital crime investigations.<sup>104</sup> Today the exchange of data replaces the classic phone conversations. The exchange of data is not limited to e-mails and file-transfer. An increasing number of voice communications are performed by using technology based on the Internet protocols (Voice-over-IP).<sup>105</sup> Seen from a technical point of view a voice-over-IP phone call is much more comparable to the exchange of e-mails than to a classic phone call using the telephone wire and the interception goes along with unique difficulties.<sup>106</sup> The Convention on Cybercrime therefore provides a set of provisions that enable the LEAs to lawfully collect traffic data or intercept data communication.

#### 3.4.1 Collection of traffic data (Art.20 CoC)

##### a) Introduction

Traffic data play an important role in Cybercrime investigation.<sup>107</sup> While having access to content data enables the law enforcement agencies to analyse the nature of messages of files exchanged traffic data can be necessary to identify an offender. In child pornography cases traffic data can for example enable the investigators to identify a webpage where the offender is uploading child pornography images. By monitoring the traffic data generated during the use of Internet services law enforcement agencies are able to identify the IP-address of the server and can then try to determine it's physical location. With Art. 20 the Convention on Cybercrime provides the legal basis for the real time collection of traffic data. The provision is neither drafted with preference to a specific technology nor is it intending to set standards that go along with the need for high financial investments for the industry involved.<sup>108</sup>

---

<sup>104</sup> Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel see: Legal Opinion on Intercept Communication, 2006 – available at: <http://www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf>.

<sup>105</sup> Regarding the interception of VoIP to assist law enforcement agencies see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP – available at <http://www.itaa.org/news/docs/CALEAVOIPreport.pdf>; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006 - available at: [http://scissec.scis.ecu.edu.au/wordpress/conference\\_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf](http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf).

<sup>106</sup> Regarding the interception of VoIP to assist law enforcement agencies see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP – available at <http://www.itaa.org/news/docs/CALEAVOIPreport.pdf>; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006 - available at: [http://scissec.scis.ecu.edu.au/wordpress/conference\\_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf](http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf).

<sup>107</sup> "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in Cybercrime investigations see as well: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 et. seq.

<sup>108</sup> "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

b) Best practice

- Clear distinction between traffic data and content data in the order

c) Bad practice

- No clear indication if the order is related to data that was generated in the past or data the is currently processed
- No clear indication that the collection shall be stopped

### 3.4.2 Interception of content data (Art.21 CoC)

a) Introduction

The possibility to intercept data exchange processes can be important in those cases where the law enforcement agencies do already know the communication partner but have no information about the type of information exchanged. Art. 21 is giving them the possibility to record data communication and analyse the content.<sup>109</sup> This includes files downloaded from websites or file-sharing systems, e-mails send or received by the offender and chat conversations.

b) Best practice

- Clear distinction between traffic data and content data in the order

c) Bad practice

- No clear indication if the order is related to data that was generated in the past or data the is currently processed
- No clear indication that the collection shall be stopped

---

<sup>109</sup> One possibility to prevent law enforcement agencies to analyse the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures see: *Singh*; *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, 2006; *D'Agapeyev*, *Codes and Ciphers – A History of Cryptography*, 2006; *An Overview of the History of Cryptology* – available at: <http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf>.

### 3.5 Additional instruments

#### a) Introduction

The Convention on Cybercrime provides a collection of the most relevant provisions with regard to Cybercrime investigations. Among them are:

- Data Retention Obligations

Other issues should be mentioned:

- Development of remote forensic software. There are reports about the use of remote forensic software by US investigators.<sup>110</sup> In a topic case a software tool was secretly installed on the suspects computer to prove his participation in a criminal offence.<sup>111</sup> Currently the question if such instruments are necessary but also if they are legitimate and proportionate as regards the right to respect for private life is intensively discussed.<sup>112</sup>
- Obligation to go through an identification process prior to the use of Internet services. An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144.<sup>113</sup>. The question if such obligation is proportionate as regards fundamental rights is still debated.

---

<sup>110</sup> See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 et. seqq – available at: <http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf>; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3 – available at: [http://assets.opencrs.com/rpts/RL32706\\_20070926.pdf](http://assets.opencrs.com/rpts/RL32706_20070926.pdf); Green, FBI Magic Lantern reality check, The Register, 03.12.2001 – available at: [http://www.theregister.co.uk/2001/12/03/fbi\\_magic\\_lantern\\_reality\\_check/](http://www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/); *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001 – available at: [http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127\\_5011.htm](http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm); *Sullivan*, FBI software cracks encryption wall, 2001 – available at: <http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm>; Abreu, FBI confirms "Magic Lantern" project exists, 2001 – available at: [http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic\\_Lantern.pdf](http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf).

<sup>111</sup> *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007 – available at: <http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0>; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007 – available at: <http://www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950>; *Poulsen*, FBI's Secret Spyware Tracks Down Teen Who Makes Bomb Threats, Wired, 18.07.2007 – available at: [http://www.wired.com/politics/law/news/2007/07/fbi\\_spyware](http://www.wired.com/politics/law/news/2007/07/fbi_spyware); *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008 – available at: [http://www.theregister.co.uk/2008/02/08/fbi\\_spyware\\_ploy\\_app/](http://www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/); *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007 – available at: [http://news.zdnet.com/2100-1009\\_22-6197405.html](http://news.zdnet.com/2100-1009_22-6197405.html); *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007 – available at: <http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf>;

<sup>112</sup> Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459>; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News – available at: [http://www.news.com/8301-10784\\_3-9769886-7.html](http://www.news.com/8301-10784_3-9769886-7.html).

<sup>113</sup> Decree-Law 27 July 2005, no. 144. - Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article Privacy and data retention policies in selected countries available at <http://www.icregulationtoolkit.org/en/PracticeNote.aspx?id=2026>.

- Obligation of ISP to install filter technology<sup>114</sup>

It is appropriate to note the recommendation of the Council of Europe's Committee of Ministers adopted on 26 March 2008<sup>115</sup> which sets out requirements for States and Industry when an active Internet filter is put in place. It supports "voluntary and responsible use of Internet filters" and it recommends that States should not get involved in national filtering unless it "concerns specific and clearly identifiable content" that has been declared illegal by a "competent national authority" and that also satisfies the conditions set out in the Convention on the Protection of Human Rights and Fundamental Freedoms.

The authors of this study discussed if these new approaches should be included in this study. Currently the need for such instruments and related advantages and disadvantages are intensively debated. Based on the result and the discussion with both, LEA and ISP the authors decided to exclude these approaches from the development of recommendations. The ongoing discussion process should be monitored to decide if amendments to the recommendations should be taken into consideration in the future.

---

<sup>114</sup> Regarding filter obligations/approaches see: *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide – available at: <http://cyber.law.harvard.edu/filtering/>; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq – available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=487965](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965); Regarding the discussion about filtering in different countries see: *Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007 – available at: <http://www.edri.org/edriagram/number5.14/belgium-isp>; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7 – available at: [http://www.olswang.com/updates/ecom\\_nov07/ecom\\_nov07.pdf](http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf); *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch – available at: <http://www.ip-watch.org/weblog/index.php?p=842>; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17 – available at: <http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf>; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement – available at: [http://www.eff.org/files/filenode/effeurope/ifpi\\_filtering\\_memo.pdf](http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf); Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002 – available at: <http://pcmplp.socleg.ox.ac.uk/selfregulation/iapocoda/0211xx-isp-a-study.pdf>.

<sup>115</sup>

[https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2008\)6&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864)

### **3.6 Exchange of knowledge and expertise**

#### **3.6.1 Advice, expertise, knowledge (general)**

##### a) Introduction

Law enforcement and Internet industry obviously do have different interests and goals which nevertheless overlap in certain areas: security of systems, protection of customers/citizens or preservation of assets. An understanding of each other is a prerequisite to set up a bond of trust which enables constructive and fruitful cooperation. Law enforcement presentations at industry meetings for awareness raising and vice-versa as well as industry presentations at law enforcement meetings about the technical possibilities and/or procedural can lay the foundations for that objective.

##### b) Best practice

- a) (LEA) Presentations at industry meetings for awareness raising
- b) (Industry) Presentations at LEA meetings about technical possibilities or procedural

#### **3.6.2 Training**

##### a) Introduction

- Specific training modules

Many police forces in Europe certainly have access to central training facilities and/or a national training programme for law enforcement. They may already have drawn up training courses on IT crime. For example, Germany had set up a national training concept for IT crime consisting of a number of modules which can be combined in order to fit the needs of specific training for certain ranges of operation (e.g. first responders at one end of the scale of expertise required or forensic specialists at the other). The inclusion of a training module or, at least some lessons on "Cooperation with Internet industry" would be an ideal way to make officers sensitive to that scope.

- Joint training programmes

The establishment of joint training programmes for Internet industry and law enforcement would be a good way to learn from each other and understand the general set-up and problems of the counterpart. If specific joint training programmes deem to be not feasible mutual presentations or lessons at each others training programmes could be an appropriate alternative.

##### b) Best practice

- a) Integration of modules on LEA-industry cooperation in LEA training programmes. (Germany had set up a national training concept for IT crime – which, in fact, does not yet include such a module.)

- b) Joint training programmes for industry and LEA to learn from each other and to understand the opposite side

### **3.6.3 Consultancy**

#### a) Introduction

- Joint working parties

The setting up of joint working parties to build up confidence, improve information exchange on national level and explore legal and technical possibilities to assist law enforcement is a good occasion to get the concerned parties together to talk to each other. The German Federal Criminal Police, for example made a step towards this direction and established a working party on botnets in which stakeholders meet occasionally to improve the information exchange on national level, explore legal and technical possibilities to detect and investigate botnet activities.

- b) Points of Contact

The setting up of a national industry Point of Contact would be an excellent instrument to facilitate information exchange between Internet industry and law enforcement. Depending on the structure of law enforcement in the different member countries (centralised or decentralised) similar Points of Contact should be set up on national or regional level respectively.

- c) Central database / Secure website

Law enforcement needs to know to whom they have to address their requests for disclosure of data. Especially in urgent cases (eg. ongoing hacking) immediate contacts – even by phone – might be necessary. In case there is no national industry Point of Contact established or available, a central database on industry/ISP contacts would be an alternative.

This database or contact list could be embedded into a secure website for industry and law enforcement. Such a website would be ideal as repository for useful information (eg. announcements, calendar of events, court decisions, latest developments, legislation, statistics, training material) needed to facilitate cooperation and to understand each other.

### **3.6.4 Software, hardware, etc**

#### a) Introduction

Some Internet Service Providers Providers which also have software development services/capabilities, either develop specialised software for Law Enforcement Authorities and/or provide licenses for Law Enforcement to use their software in crime investigations.

## 4 Issues which arise

### 4.1 General issues

- Request coordination

It is important that requests are coordinated to ensure that all requests to/from law enforcement and to/from internet industry are coordinated through a structured channel on both sides which validates all requests for completeness and accuracy.

- Resourcing, prioritising and cataloguing requests and responses

It is important that units which process requests are resourced sufficiently for the workload involved. In addition where the number of requests incurs significant variations over a period of time it is critical that requests are prioritised on both sides to ensure the most urgent requests are processed efficiently. All the requests and responses should be catalogued and recorded to provide early identification of problems and issues.

- Bypassing processes/protocols

There are concerns that previously agreed processes and contact procedures are occasionally bypassed in order to expedite a data request. This creates problems for some organisations which can cause incorrect data to be released or data to be released without proper authorisation thereby possibly contaminating the chain of evidence and creating procedural problems in each organisation.

- Expedited Preservation Issues

Expedited preservation is a challenging area and speed is critical to success. Even though ALL requests for data should be signed and in e-document or printed format, some requests might be delivered by more efficient methods (facsimile, scanned document, etc) but extreme care should be taken in relation to instructions given/ received by phone and this should only happen by exception from a known point of contact to a known point of contact.

In ALL cases preservation orders must be confirmed in writing with 48 hours and must indicate a time-out when the data should be purged. Disclosure of the data should be covered by standard legal instruments in each jurisdiction. Some working group participants described experiences where expedited data which was stored was never disclosed because a disclosure order was never received.

- Insufficient resourcing

There is concern that the process of issuing requests and creating responses are insufficiently resourced on both sides. This is complicated by the fact that the number of requests being processed by both sides has grown exponentially in some countries. Several countries indicated that the volume of requests was now causing concern for some organisations and that there seemed to be no recognition of the internal

costs (time, financial, technical, legal, etc) incurred in responding to some non-proportionate requests.

It was also queried whether both sides are adequately resourcing a 24/7 response. This is complicated by the fact that there is currently very little prioritization of requests and that a 24/7 response is sometimes misused for non-urgent requests. Greater communication, knowledge exchange and inter-agency coordination would alleviate a number of these concerns. There is no point in having a 24/7 response if the person(s) managing such requests/ responses is (are) insufficiently trained or empowered to achieve immediate access to skilled legal, technical and managerial personnel to respond adequately. For example, an expedited preservation of data request to a 24/7 contact of data which is hosted within an organisation but in a different legal jurisdiction requires clear powers and procedures to implement.

- **Costs**

The purpose of this study is not to increase the burden (financial or otherwise) on either the Internet industry or Law Enforcement but to streamline procedures based on best practice gained from many shared experiences.

- The economic and organizational impact on normal business activities is a significant concern for Internet industry. The issue of cost impact/apportionment for requests/responses by the public authorities is of major importance to both sides. Therefore both sides should be mindful of the costs involved in creating and responding to requests. Procedures should be developed with consideration of the financial impact of these activities and issues of cost reimbursement or fair compensation to relevant parties should be considered.
- The recommendations need to be cognisant of the financial impact associated with processing requests and the impact on the normal business activities of the Internet Service Provider and on the investigations of law enforcement.
- The compilation of high demands on the resourcing by the ISPs could put at risk the subsistence of small Internet companies and the multiplicity of the different levels of competition in the new media world.

It is clear that cost reimbursement would have a positive effect on the quality of the cooperation. However, creating a cost algorithm which unreasonable impacts on law enforcement and therefore on crime investigations could also have a negative impact on successful prosecutions.

## **4.2 Bad practices**

### **4.2.1 Industry specific issues**

- receive one request with many accounts being queried
- receive multiple requests which are clearly fishing expeditions and these also take a long time to process

- receive requests for the content of communications without appropriate legal procedures being followed
- receive many simultaneous requests with no categorisation or prioritisation
- receives requests which are incomplete, unclear and with insufficient detail
- receives requests which are sent to the wrong industry player or the organisation which does not own the data requested
- requests and responses are sent and received by the wrong persons and/or departments

#### **4.2.2 Law enforcement specific issues**

- receive rejections to requests with no clear reason given
- receive responses which are inadequate, incomplete, inaccurate or unclear
- timely urgent requests in serious cases (lack of time for getting a court order – court order to be presented **after** disclosure of data)

#### **4.2.3 Other issues**

- Law Enforcement and Industry receive preservation requests which are not followed up with disclosure requests causing substantial workload for no purpose.

### **4.3 Conclusion**

Within the discussion there was a consensus that it is important to encourage good practice *and* to discourage bad practice.

It is important that requests and responses are properly validated internally before being exchanged externally.

It is important to track and audit the system in use so that relevant usage statistics can be recorded to identify issues and strengths in the system, to identify problem organisations and, if appropriate, for potential public reporting purposes.

## 5 Guidelines<sup>116</sup>

### **Guidelines for the cooperation between law enforcement and internet service providers against cybercrime**

#### **Introduction**

1. Building an information society requires the strengthening of trust in information and communications technologies (ICT's), the protection of personal data and privacy, and the promotion of a global culture of cyber-security in a context where societies worldwide are increasingly dependent on ICT and thus vulnerable to cybercrime;

2. The First and Second World Summit on the Information Society (Geneva 2003, Tunis 2005) – among other things – committed to build an inclusive information society where everyone can create, access, utilize and share information and knowledge, achieve their potential and improve their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights, and which calls for new forms of partnerships and cooperation among governments, the private sector, civil society and international organisations;

3. Internet service providers (ISP) and law enforcement authorities (LEA) play a crucial role in the realization of this vision;

4. National legislation in line with the Convention on Cybercrime of the Council of Europe (the "Budapest Convention") helps countries create a sound legal basis for public-private cooperation, investigative powers as well as international cooperation;

5. The guidelines are not intending to substitute existing legal instrument but assume adequate legal instruments exist that provide a well balanced system of investigation instruments as well as related safeguards and a protection of fundamental human rights such as freedom of expression, the respect for private life, home and correspondence and the right to data protection. It is therefore recommended that states adopt regulations in their national law in order to fully implement the procedural provisions of the Convention on Cybercrime, and to define investigative authorities and obligations of law enforcement while putting in place conditions and safeguards as foreseen in Article 15 of the Convention. This will

- ensure efficient work of law enforcement authorities
- protect the ability of Internet service providers to provide services
- ensure that national regulations are in line with global standards
- promote global standards instead of isolated national solutions
- help ensure due process and the rule of law, including principles of legality, proportionality and necessity;

6. For the purposes of these guidelines we use the definition of service provider included in the Convention on Cybercrime in Article 1 which defines "service provider" in a broad manner as meaning:

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

---

<sup>116</sup> These guidelines were discussed and adopted by the conference "cooperation against cybercrime", Strasbourg, 1-2 April 2008.

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

7. In order to enhance cybersecurity, minimise use of services for illegal purposes and build trust in ICT, it is essential that Internet service providers and law enforcement authorities cooperate with each other in an efficient manner with due consideration to their respective roles, the cost of such cooperation and the rights of citizens;

8. The purpose of the present guidelines is to help law enforcement authorities and Internet service providers structure their interactions in relation to cybercrime issues. They are based on existing good practices and should be applicable in any country around the world in accordance with national legislation and respect for the freedom of expression, privacy, the protection of personal data and other fundamental rights of citizens;

9. It is therefore recommended that States, law enforcement authorities and Internet service providers undertake the following measures at a national level:

### **Common guidelines**

10. Law enforcement authorities and Internet service providers should be encouraged to engage in information exchange to strengthen their capacity to identify and combat emerging types of cybercrime. Law enforcement authorities should be encouraged to inform service providers about cybercrime trends;

11. Law enforcement and Internet service providers should promote a culture of cooperation – rather than confrontation - including the sharing of good practices. Regular meetings in order to exchange experience and resolve problems are encouraged;

12. Law enforcement and service providers should be encouraged to develop written procedures for cooperation with each other. Where possible, both parties should be encouraged to provide structured feedback on the operation of these procedures to each other;

13. Formal partnerships between law enforcement and service providers should be considered in order to establish longer-term relationships with proper guarantees for both sides that the partnership will not infringe any legal rights on the side of the industry or interfere with any legal powers on the side of law enforcement;

14. Both law enforcement authorities and Internet service providers should protect the fundamental rights of citizens according to United Nations and other applicable European and international standards such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as domestic law. This places reasonable limits to the level of cooperation possible;

15. Law enforcement authorities and Internet service providers are encouraged to cooperate with each other in view of enforcing privacy and data protection standards at the domestic level but also with regard to cross-border data flows. The work of the Council of Europe and the OECD provides guidance in this respect;

16. Both sides should be mindful of the costs involved in creating and responding to requests. Procedures should be developed with consideration of the financial impact of these

activities and issues of cost reimbursement or fair compensation to relevant parties should be considered.

### **Measures to be taken by law enforcement**

17. Broad and strategic cooperation – Law enforcement should be encouraged to assist service providers by engaging in a broad and strategic cooperation with industry that would include conducting regular technical and legal training seminars, as well as providing feedback on investigations conducted based on complaints filed by service providers or on the intelligence gathered based on known criminal activity reported by the service providers;

18. Procedures for legally binding requests – Law enforcement should be encouraged to prepare written procedures, which include appropriate due diligence measures, for the issuing and processing of legally binding requests, and ensure that requests are carried out pursuant to the agreed procedures;

19. Training – Law enforcement should be encouraged to provide training to a designated set of their personnel on how to implement these procedures, including the manner in which records may be obtained from service providers and how to process information received, but also on internet technologies and their impact in general as well on how to respect due process and the fundamental rights of individuals;

20. Technical resources – Law enforcement personnel responsible for cooperation with service providers should equip themselves with the necessary technical resources, including internet access, an agency-issued email address that makes the affiliated agency apparent in the address, and other technical resources to permit them to receive information securely from a service provider electronically;

21. Designated personnel and contact points – Interaction between law enforcement and service providers should be limited to trained personnel. Law enforcement should be encouraged to designate contact points for their cooperation with service providers;

22. Authority for requests – Law enforcement authorities should be encouraged to define clearly in their written procedures which law enforcement personnel can authorise what type of measures and requests to Internet service providers and how these requests can be validated/authenticated by Internet service providers;

23. Law enforcement should be encouraged to make information available to Internet service providers on their procedures and, where possible, which personnel or which nominated job positions are responsible for cooperation with Internet service providers;

24. Verification of source of request – The source of a request from law enforcement should be verifiable by service providers:

- All correspondence should include the contact name, telephone number and e-mail address of the law enforcement agent(s) seeking the records so that the service provider can contact the requesting individual if issues arise
- service providers should not be asked to correspond with an agent through the agent's personal e-mail address, but rather through an appropriate agency-provided e-mail account
- all letters should be on department letterhead, and all correspondence should include the agency's main switchboard number and website address so that service providers can take steps to verify the authenticity of requests if deemed appropriate;

25. Requests – Requests from law enforcement to service providers should be made in writing (or other legally acceptable electronic method) and leave a documentary trail. In extremely urgent cases when oral requests are acceptable, they must be immediately followed up by written (or other legally acceptable electronic method) documentation;

26. Standard request format – At the national level, and if possible internationally, law enforcement should be encouraged to standardise and structure the format used for sending requests and for responding to requests. As a minimum requests should contain the following information:

- Registration number
- Reference to legal basis
- The specific data requested
- Information to verify the source of the request;

27. Specificity and accuracy of requests – Law enforcement should be encouraged to ensure that requests sent are specific, complete and clear, and provide a sufficient level of detail to allow service providers to identify relevant data. They should be encouraged to ensure that requests are sent to the service provider that has the records. Requests for multiple and unspecified data should be avoided;

28. Law enforcement should be encouraged to provide as many facts about the investigation as possible without prejudicing the investigation or any fundamental rights in order to enable service providers to identify relevant data;

29. Law enforcement should be encouraged to provide explanations and assistance to service providers regarding non-case-related investigation techniques in order for them to understand how their cooperation will result in more efficient investigations against crime and better protection for citizens;

30. Prioritisation – Law enforcement should be encouraged to prioritise requests, especially those related to large volumes of data, to enable service providers to address the most important ones first. Prioritization is best done in a consistent manner across national law enforcement authorities and if possible internationally;

31. Appropriateness of requests – Law enforcement should be encouraged to be mindful of the cost that requests entail for service providers and give service providers sufficient response time. They should be mindful that service providers may also need to respond to requests from other law enforcement authorities, and should be encouraged to carefully monitor volumes submitted;

32. Confidentiality of data – Law enforcement should ensure the confidentiality of data received;

33. Avoid unnecessary cost and disruption of business operations – Law enforcement should be encouraged to avoid unnecessary cost and disruption of business operations of the service providers and other types of business;

34. Law enforcement should be encouraged to restrict the use of emergency contact points service to extremely urgent cases only to ensure this service is not abused;

35. Law enforcement should be encouraged to ensure that preservation orders and other provisional measures are followed up in a timely manner by disclosure orders, or the Internet service provider is informed in a timely manner that preserved data is no longer required;

36. International requests – For requests addressed to non-domestic Internet service providers, domestic law enforcement authorities should be encouraged not to direct requests directly to non-domestic Internet service providers but make use of procedures as described in international treaties, such as the Convention on Cybercrime and the network of 24/7 law enforcement points-of-contact for urgent measures, including preservation orders/requests;

37. Requests for international mutual legal assistance – Law enforcement and criminal justice authorities should be encouraged to take the necessary steps to ensure that requests for provisional measures are followed by international procedures for mutual legal assistance, or the Internet service provider is informed in a timely manner that preserved data is no longer required;

38. Coordination among law enforcement agencies – law enforcement authorities should be encouraged to coordinate their cooperation with Internet service providers and share good practices among each other nationally and internationally. Internationally they should make use of relevant international representative bodies for that purpose;

39. Criminal compliance programmes – Law enforcement should be encouraged to organise their interactions outlined above with service providers in the form of a comprehensive criminal compliance programme, and provide a description of such programme to service providers, including:

- The information necessary to contact the law enforcement designated criminal compliance personnel, as well as the hours during which such personnel are available
- The information necessary for service provider to be able to provide documents to the criminal compliance personnel
- Other particulars specific to the law enforcement criminal compliance personnel (such as the extent that a law enforcement co-operates with multiple countries, documents to be translated into a particular language etc.);

40. Audit of the compliance system – Law enforcement authorities should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;

#### **Measures to be taken by service providers**

41. Cooperation to minimize use of services for illegal purposes– Subject to applicable rights and freedoms, such as freedom of expression, privacy and other national or international laws, as well as user agreements, service providers should be encouraged to cooperate with law enforcement to help minimize the extent to which services are used for criminal activity as defined by law;

42. Service providers should be encouraged to report criminal incidents affecting the Internet service provider of which he is aware of to law enforcement. This does not oblige service providers to actively search for facts or circumstances indicating illegal activities;

43. Service providers should be encouraged to assist law enforcement with education, training and other support on their services and operations.

44. Follow up to requests from law enforcement authorities – Service providers should be encouraged to undertake all reasonable efforts to assist law enforcement in executing the request;

45. Procedures for responding to requests – Service providers should be encouraged to prepare written procedures, which include appropriate due diligence measures, for the processing of requests, and ensure that requests are followed up to pursuant to the agreed procedures;

46. Training - Service providers should be encouraged to make sure that sufficient training is provided to their personnel responsible for implementing these procedures;

47. Designated personnel and contact points – Service providers should be encouraged to designate trained personnel as contact points for cooperation with law enforcement;

48. Emergency assistance – Service providers should be encouraged to establish a means by which law enforcement may reach their criminal compliance personnel outside of normal business hours to address emergency situations. Service providers should be encouraged to provide law enforcement with relevant information for emergency assistance;

49. Resources – Service providers should be encouraged to provide contact points or personnel responsible for cooperation with law enforcement with the resources necessary to enable them to comply with requests from law enforcement;

50. Criminal compliance programmes – Service providers should be encouraged to organise their cooperation with law enforcement in the form of comprehensive criminal compliance programmes, and provide a description of such programmes to law enforcement, including:

- The information necessary to contact the providers’ designated criminal compliance personnel, as well as the hours during which such personnel are available
- The information necessary for law enforcement to be able to provide documents to the criminal compliance personnel
- Other particulars specific to the providers’ criminal compliance personnel (such as the extent that a service provider operates in multiple countries, documents to be translated into a particular language etc.);
- In order to allow law enforcement to make specific and appropriate requests, service providers should be encouraged to provide information on the type of services offered to users, including web links to the services and additional information as well as contact details for further information;
- Where possible, the Internet service provider should be encouraged to provide a list, on request, of which types of data could be made available for each service to law enforcement on receipt of a valid disclosure request from law enforcement accepting that not all this data will be available for every criminal investigation;

51. Verification of source of requests – Service providers should be encouraged to take steps to verify the authenticity of requests received from law enforcement to the extent possible and necessary to ensure that customer records are not disclosed to unauthorized persons;

52. Response – Service providers should be encouraged to respond to requests from law enforcement in writing (or other legally acceptable electronic method) and ensure that a

documentary trail is available in relation to requests and responses accepting that this trail might not include any personal data;

53. Standard response format – Taking into account the format for requests used by law enforcement, service providers should be encouraged to standardise the format for sending information to law enforcement;

54. Service providers should be encouraged to process requests in a timely manner, in line with the written procedures they have defined and provide guidelines to law enforcement on the average delays incurred to respond to requests;

55. Validation of information sent – Service providers should be encouraged to ensure that information transmitted to law enforcement is complete, accurate and protected;

56. Confidentiality of requests – Service providers should ensure the confidentiality of requests received;

57. Explanation for information not provided – Service providers should be encouraged to provide explanations to the law enforcement authority sending a request if requests are rejected or information cannot be provided;

58. Audit of the compliance system – Service providers should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;

59. Coordination among service providers – being mindful of anti-trust/competition regulations service providers should be encouraged to coordinate their cooperation with law enforcement and share good practices among each other, and make use of service provider associations for that purpose.

## **6 Conclusion**

Existing industry engagement activities with Law enforcement such as education, training, processes and impact assessment are very useful activities and should continue.

The benefit of representative organisations in areas of large numbers of Internet Industry players and law enforcement agencies/departments is significant to ensure consistent and transparent approaches to best practices.

The benefit of a single point of contact and a 24/7 contact but that resourcing these points-of-contact is essential for it to be a success.

Working together creates a more accurate picture of the scale and impact of criminal use of the Internet and its impact on the workload of Law Enforcement and Internet Industry. In addition, this would encourage greater appreciation (internally and externally) of the work of the ISP teams who handle requests from law enforcement. It is expected that if requests are managed by ISPs through constant dialog with LEA on the quality of the processes, ISPs will be in a better position to anticipate the increasing and changing demands of LEA and will be at the same time protect themselves from inappropriate/excessive requests.

Sharing of good practice is essential for everyone to learn from each other and should continue.

The guidelines as adopted in Strasbourg on 1-2 April 2008 will be most helpful in this respect. They are a non-binding tool that can now be disseminated and used to help law enforcement and service providers in any country around the world to organise their cooperation against cybercrime while respecting each others' roles and responsibilities as well as the rights of internet users.

## **Appendices**

- Appendix 1 Working group members
- Appendix 2 Relevant Legal Instruments
- Appendix 3 Extract – procedural provisions of the Convention on Cybercrime

## Appendix 1 – Working Group Members

Country	Organisation	Name
Belgium	ebay	A. Spasova
Belgium	ebay	A. Barbagallo
Belgium	ebay	C. Breure
Belgium	EuroISPA	R. Nash
France	AFA	D. Kownator
France	AFA	E. DeMarco
France	CoE	A. Seger
France	DCPJ/OCLCTIC	C. Aghroum
France	Microsoft	V. Lestoquoy
France	Microsoft	J-C LeToquin
Germany	BKA Wiesbaden	W. Schrieber
Germany	CoE	M. Gercke
Germany	ECO	H. Lesch
Germany	ECO	I. Ivanov
Ireland	CoE/Aconite	C. Callanan (Chair/Rapporteur)
Ireland	EuroISPA	P. Durrant
United Kingdom	BT	C. Persson
United States	Microsoft	T. Daemen

## Appendix 2 - Relevant Legal Instruments

### *Definitions of service providers*

---

#### **Convention on Cybercrime (Council of Europe)**

##### **Article 1 – 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;

---

#### **Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)**

##### **Article 2**

##### **Definitions**

For the purpose of this Directive, the following terms shall bear the following meanings:

- (a) "information society services": services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;
- (b) "service provider": any natural or legal person providing an information society service;
- (c) "established service provider": a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;

Section 4: Liability of intermediary service providers

##### **Article 12**

##### **"Mere conduit"**

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission;
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this

takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

### **Article 13**

#### **"Caching"**

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

- (a) the provider does not modify the information;
- (b) the provider complies with conditions on access to the information;
- (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

### **Article 14**

#### **Hosting**

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

### **Article 15**

#### **No general obligation to monitor**

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

---

**Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations**

For the purposes of this Directive, the following meanings shall apply:

- 1). "product": any industrially manufactured product and any agricultural product, including fish products;
- 2). "service": any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:

- "at a distance": means that the service is provided without the parties being simultaneously present,
- "by electronic means": means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- "at the individual request of a recipient of services": means that the service is provided through the transmission of data on individual request.

## **Appendix 3 - Extract procedural provisions of the Convention on Cybercrime**

### **Article 16 – Expedited preservation of stored computer data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

### **Article 17 – Expedited preservation and partial disclosure of traffic data**

- 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
  - a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
  - b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

#### *Title 3 – Production order*

### **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.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
- a the type of communication service used, the technical provisions taken thereto and the period of service;
  - b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
  - c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

*Title 4 – Search and seizure of stored computer data*

**Article 19 – Search and seizure of stored computer data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
- a a computer system or part of it and computer data stored therein; and
  - b a computer-data storage medium in which computer data may be stored
- in its territory.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;

- b make and retain a copy of those computer data;
  - c maintain the integrity of the relevant stored computer data;
  - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

*Title 5 – Real-time collection of computer data*

**Article 20 – Real-time collection of traffic data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary 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,
- traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

**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.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.