Privacy Protection vs. Privacy Offences in the European Regulatory Context:

The Cases for Interception of Communications and the Retention of Traffic Data

Mrs. Anastasia S. Spiliopoulou
Lawyer, LL.M., Member of Athens Bar Association,
Dept. of Regulatory Issues, General Directorate of Regulatory Affairs,
Hellenic Telecommunications Organization S.A. (OTE)

Dr. Ioannis P. Chochliouros
Ph.D., M.Sc., Telecommunications Engineer,
Head of Research Programs Section, Labs & New Technologies Division,
Network Strategy & Architecture Dept., General Directorate for Technology,
Hellenic Telecommunications Organization S.A. (OTE)

Dr. Stergios P. Chochliouros
Independent Consultant, Researcher

Thematic Contents:

1. Introduction
2. Current European Responses for Increased Electronic Security
3. Privacy Protection vs. Privacy Offences in the European Framework
4. Interception of Communications
5. Retention of Traffic Data
6. Overview & Conclusion - Projection to the Future

Introductory Framework

- **Exponential growth of electronic communication networks and information systems in the recent years:** Both they constitute an **essential part of the daily lives** of the European citizens and **fundamental "tools"** to the success of the broader economy.
- **Networks and information systems are converging and becoming increasingly interconnected:** This option **creates potential opportunities** for all categories of "players" involved and **affects, very seriously, all sectors of human activity** (business, public services and private sphere).
- **Networks and information systems, through innovative ICTs, are having revolutionary and critical impact and are now becoming the "lifeblood" of societies and economies!!!**
- **The success of Information Society's development is important for growth, competitiveness and employment opportunities and has far-reaching economic, social and legal implications.**

Introductory Framework - 2

- **In the hands of persons acting with bad faith, malice, or grave negligence, ISTs may become "tools" for actions that endanger or "injure" the life, property or dignity of individuals or even damage the public interest.**

- **As cyberspace gets more and more complex (and its components more and more sophisticated), especially due to the fast evolution of (broadband) Internet-based platforms, new and unforeseen vulnerabilities may emerge!**

- **As the Internet becomes ubiquitous for all business and personal communications, the sensitivity and economic value of the content of information transmitted is increasing.**

  The economic damage caused by any disruptions is extremely severe!!!

Introductory Framework - 3

- **Due to the trans-national and borderless character of modern systems, it is possible to launch an "attack" from anywhere to every place in the world, at any time, while cross-border crime is more prevalent than before.**

- **Due to the ever-increasing amount of inter-connectivity in the modern (global) communications environment, various areas can be affected:** e-Communications network operators and service providers, e-Commerce companies, public sector organizations, industry sector, governments, individuals-citizens.

There are severe threats to the achievement of a safer information society supporting an area of freedom, security and justice *and therefore*, this requires a "proper" and immediate response!!!

Current European Responses for Increased e-Security

- **The secure functioning of networks-infrastructures, services-transactions and systems has become a key concern, especially for the smooth operation of the internal EU market and society…**

- **e-Security is a priority of the present European policies & applied measures, *towards the transition to a competitive, dynamic and knowledge-based economy.***

- **Users should be able:**
  - **to *rely on the availability of information services* and,**
  - **to *have the confidence that their communications* (and data) *are safe* from unauthorized access or any other modification.**

Security is an "enabler" for e-Businesses and a pre-requisite for users' privacy.

Current European Responses for Increased e-Security - 2

- **There is scope for significant action:**

in terms of preventing criminal activity by enhancing the security of infrastructures/services via modern technical means at certain areas *(e.g. by protecting IPRs and personal data, fighting harmful and illegal content on the Internet and promoting e-Commerce and the usage of e-Signatures)*

and by ensuring that law enforcement authorities (or any other appropriate legal authorities) have the appropriate means to act, *especially through an interactive cooperation between all relevant parties involved.*

Privacy Protection vs. Privacy Offences in the EU

General Remarks:

- **European Authorities underline the primary importance of the information society for democracy and the respect for human rights and fundamental freedoms *(e.g. the European Treaty, the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Constitutions of Member States).***

- **The rights of privacy and data protection constitute substantial issues of the contemporary European policy *(e.g. Directives 95/46/EC, 2002/58/EC).***

Privacy Protection vs. Privacy Offences in the EU - 2

The *Directive on privacy of e-communications* (2002/58/EC) required:

- Development/establishment of **appropriate technical & organisational measures to safeguard security** of services offered by market players, and;
- **Assurance of confidentiality** of the communications & (related traffic data).

The Directive comprises basic obligations.

It has been **adapted to the national legislations** to conform to developments in the markets and technologies for modern communications, in a way **to provide an "equal level" of protection** of personal data and privacy for all related users, **regardless of the technologies used.**

Privacy Protection vs. Privacy Offences in the EU - 3

The *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (95/46/EC) required:

"The protection of the primary rights (and freedoms) of natural persons, and specifically their right to privacy with respect to the processing of personal data, in order to ensure free data flow".

The Directive obliged European States to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access *(in particular where the processing involved the transmission of data over a network and against all other unlawful forms of processing).*

The Directive has broadly achieved its aim of ensuring strong protection for privacy, while making it easier for personal data to be moved around the EU.

Privacy Protection vs. Privacy Offences in the EU - 4

The current state & trends of the EU environment:

- Various EU countries have introduced criminal law addressing privacy offences, illegal collection, storage, modification, disclosure or dissemination of personal data.
- Several provisions oblige Member States to adopt appropriate measures to ensure imposition of sanctions in case of infringements.
- There is a need for substantive and procedural law instruments, *approximated at European level,*
  - to protect potential victims of electronic- or computer-related crime and
  - to bring the perpetrators to justice, imposing (common) incriminations and sanctions, and
  - to ensure the greatest possible police and judicial cooperation.

Privacy Protection vs. Privacy Offences in the EU - 5

The current state & trends of the EU environment:

- **Multiple forms of criminal or terrorist activities could be prevented *(or, in the worst case, properly investigated)* via the appropriate and coordinated control and/or surveillance of the electronic means, *used for such illegal purposes.***
- **Law enforcement agencies must possess the powers to investigate offences and to respond drastically, whenever they detect unlawful activities, to preserve security of the State and of individuals.**
- **However, it must be guaranteed that personal communications, privacy and data protection, access to and dissemination of information remain fundamental rights in modern democracies.**

Privacy Protection vs. Privacy Offences in the EU - 6

The availability and use of effective prevention measures are desirable, to reduce the legitimate need to apply law enforcement and public security measures.

Any legislative measures that might be necessary to tackle electronically-related crime, **need to strike the "right balance" between law enforcement & public security requirements.**

Interception of Communications

General Issues:

In the EU, the confidentiality of communications *(and related traffic data)* is fully guaranteed, in accordance with international instruments relating to human rights (ECHR & National Constitutions of the Member States)

- **The introduction of advanced digital technologies in telecommunications networks, gives rise to specific requirements, concerning the protection of personal data and end-user's privacy.**
- **Any (legal, regulatory, or technical) adopted measures concerning privacy issues and the legitimate interest of legal persons, must be properly harmonised, to avoid obstacles to the proper development and the functioning of the internal market…**

Interception of Communications - 2

The "approach" promoted by the European legislation:

- **Interceptions are illegal unless they are authorised by law**, when necessary, *in specific cases*, for limited purposes.
- National authorities need to ensure confidentiality of communications, **through suitable legislation in force**.

Interferences by appropriately authorized (public) bodies:

Communications interferences by public authorities are permitted

- if they are in accordance with the law, and
- if they are necessary in a democratic society

in the interests of national security, public safety or the economic well-being of the country,

- for the **prevention of disorder or crime**,
- for the **protection of health or morals**, or
- for the **protection of the rights and freedoms of citizens**.

Interception of Communications - 3

Basic Principles:

Authorities need to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by persons other than users, *without the consent of the user concerned* (regardless of whether the latter is a natural or a legal person), except when "legally authorised" to act so.

Diverse measures can be applied, *if "necessary",*

- **for the protection of public security, defence, State security (including the economic well-being and financial interests of the State when relating to national security matters) and**
- **for the enforcement of criminal law (prevention, investigation, detection and prosecution of criminal offences).**

Interception of Communications - 4

State (or governmental) Response:

The legally authorized interception of communications can be an **important tool for the protection of national interests**, in particular for national security and for the investigation of criminal activities.

All corresponding **measures have to be in line with Community Law**, and "fully proportionate" to the specific aims they intend to fulfil.

Interception can be undertaken in a number of ways, **through the physical access of a network** (e.g. network management and concentration points, such as routers, gateways, switches and network operation servers), under the supervision of the proper authorities.

Interception of Communications - 5

Market Response:

- ✓ **Interception may only be effected if proper technical provisions have been made applicable, according to common principles/rules, in the entire EU environment.**

- ✓ **Questions on regulations, technical feasibility, allocation of costs and commercial impact, *all have to be always clarified*, especially when need to be implemented by certain market players.**

- ✓ **Wherever new technical interception requirements are to be applied, these shall be co-ordinated (internationally),**
- to prevent distortion of the single internal market,
- to minimise the costs for industry and
- to respect privacy and data protection requirements.

Retention of Traffic Data

General Remarks:

- ✓ Data relating to subscribers processed to establish electronic communications contain information on the private life of natural persons and concern the right to respect for their correspondence, or concern the legitimate interests of legal persons.

- ✓ Electronic communications generate "traffic data" and/or "location data" which include details about the location of the caller, the number called, the time and duration of the call.

- ✓ The processing of traffic data has to be restricted to specific authorised persons, for a limited time and for specific purposes, like:
  - billing or traffic management; revenue collection; interconnection payments;
  - customer enquiries; fraud detection;
  - marketing of e-Communications services, or;
  - provision of value added services.

Retention of Traffic Data - 2

Action Principles:

- ✓ Traffic data need to be erased (or made anonymous) when no longer needed for the purpose of the certain transmission.
- ✓ Location data generated by mobile phones can only be further used or passed on by network operators with explicit user consent!
  (Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes)
- ✓ An exemption is also predicted for the cases of emergency calls, to offer access to calling line identification and location data without the prior user consent.

The availability of traffic data is important for purposes related to law enforcement and security (in particular against terrorism and organised crime, also including drug and people traffickers).

Traffic data can help investigations by providing a “link” between people, times and places which may lead to the identification of witnesses, forensic opportunities or even the criminal’s financial assets…

Retention of Traffic Data - 3

Thematic Field:

Traffic data may include any **"translation" of the naming, numbering or addressing information** provided by the sender of a communication or the user of a connection to perform the communication, over the network upon which it is transmitted.

In addition, traffic data may, *inter alia*, consist of

- data referring to the routing, duration, time or volume of a communication,
- the protocol used,
- the location of the terminal equipment of the sender or recipient,
- the network on which the communication originates (or terminates),
- the beginning, end or duration of a connection.

They may also consist of the **format** in which the communication is conveyed by the underlying network(s).

Retention of Traffic Data - 4

Actual challenge:

Differences in legal, regulatory and technical provisions concerning the retention of certain categories of data, as well as cost compensation schemes, present obstacles to the internal EU market for electronic communications, as service providers are faced with different requirements regarding the types of data to be retained, together with the conditions and the duration of retention.

The response:

Validation of the newly proposed Directive 2006/24/EC aiming to:

(i) Establish, clearly, the purpose for which the data which are retained can be used;

(ii) Limit the categories of data to be retained, and;

(iii) Limit the period of retention, *to the appropriate extent*.

The content of the communications is however excluded!

Retention of Traffic Data - 5

The Basic Context:

The following data categories are retained, necessary to:

- ✓ Trace and identify the **source** and/or the **destination** of a communication, concerning both **fixed network telephony and/or mobile telephony** and **Internet access, Internet e-mail and Internet telephony**;
- ✓ Identify the **date**, the **time**, the duration and the **type** of a communication;
- ✓ Identify the **communication device/equipment**, and;
- ✓ Identify the **location** of mobile communication equipment.

The categories of information to be retained reflect an appropriate "balance" between:

- ❖ the **expected benefits** for the prevention, investigation, detection, and prosecution of serious offences involved, and
- ❖ the **level of invasion of privacy** they will cause.

Retention of Traffic Data - 6

Periods for retention:

The approach suggests that:

"Retention periods of not less than six months and not more than two years from the date of the communication are appropriate".

For example,

- **1 year for mobile and fixed telephony traffic data and**
- **six months for traffic data related to Internet usage**

can sufficiently cover the main needs of law enforcement,
whilst limiting the associated costs for industry and the intrusion into the private life of citizens.

- **Data shall be destroyed at the end of the period for retention except those which have been accessed and preserved.**
- **Care should be provided for proper storage requirements and for immediate transmission to the competent authorities, without undue delays.**

Overview and Conclusion

Europe has entered a new phase in its history, marked by the transition to a competitive, dynamic and knowledge-based economy.

In the global environment, electronic security is a (complex) but very rapidly evolving concept, and faces many challenges, in numerous areas.

Possible measures affect a wide range of existing and emerging policies, citizens' concerns (including the protection against criminal and terrorist threats), and the adaptation of governance structures, to effectively deal with these matters.

Overview and Conclusion - 2

The future perspective:

The **implementation of appropriate measures** (following in particular from the *Data Protection Directives)* **contributes to enhancing security of the networks (and of data processing),** which now constitute a **major area of concern,** for:

- ⇨ the **growth of the digital economy** and
- ⇨ the **fight against terrorism and organised crime**.

It is a high priority for the EU to increase the security level of its electronic communications systems,

- ⇨ **via the establishment of suitable measures,**
- ⇨ **occasionally permitting both telecommunications lawful interception and retention of traffic data, *when necessary*, for specific purposes.**

MANY

THANKS

FOR

YOUR ATTENTION…