Fighting cyber crime and protecting privacy in the cloud

Bigo, D.; Boulet, G.; Bowden, C.; Carrera, S.; Jeandesboz, J.; Scherrer, A.

Publication date
2012
Document Version
Final published version

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Fighting cyber crime and protecting privacy in the cloud

STUDY

EN

2012

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Fighting cyber crime and protecting privacy in the cloud

STUDY

Abstract

This study addresses the challenges raised by the growing reliance on cloud computing. It starts by investigating the issues at stake and explores how the EU is addressing the identified concerns. The study then examines the legal aspects in relation to the right to data protection, the issues of jurisdiction, responsibility and regulation of data transfers to third countries. These questions have been neglected in EU policies and strategies, despite very strong implications on EU data sovereignty and the protection of citizens' rights.

PE 462.509 EN

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs

AUTHORS

Prof. Didier Bigo (Centre d'Etudes sur les Conflits, C&C)
Mr Gertjan Boulet (under coordination of the Centre for European Policy Studies, CEPS)
Mr Caspar Bowden (under coordination of the Centre d'Etudes sur les Conflits, C&C)
Dr Sergio Carrera (Centre for European Policy Studies, CEPS)
Dr Julien Jeandesboz (Centre d'Etudes sur les Conflits, C&C)
Dr Amandine Scherrer (Centre d'Etudes sur les Conflits, C&C)

Under coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS) and the Centre d'Etudes sur les Conflits (C&C)

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C: Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: alessandro.davoli@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

European Parliament, Manuscript completed in October 2012.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS 5

LIST OF FIGURES 7

Executive Summary 8

General information 10

INTRODUCTION 12

1.1. Cloud computing technologies 13

1.2. Cloud computing, cybercrime and privacy: what are the challenges? 14

2. CIOUD COMPUTING, CYBERCRIME, PRIVACY: THE EU FRAMEWORK 15

2.1. What is at risk with the cloud? 17

2.2. Cloud computing and the EU legal, policy and operational framework 18

3. THE TRIANGULAR DIPLOMACY OF CLOUD COMPUTING AND THE IMPLICATIONS FOR THE INDIVIDUAL 27

3.1. The triangular diplomacy of cloud computing: states, companies and inter-state relations 27

3.2. The companies/ states/ inter-state relations 31

3.3. The states/ inter-state/ companies relations 32

3.4. The inter-state/ states/ companies relation 34

4. CLOUD COMPUTING AND CYBERCRIME: LEGAL CHALLENGES FOR DATA PROTECTION LAW 35

4.1. Definitional dilemma in the EU data protection legal framework 37

4.2. The challenge of jurisdiction 38

4.3. The challenge of responsibility: data controller, data processor and personal data 40

4.4. Data transfers/ processing to third countries 42

4.5. The challenge of regulation for EU Home affairs agencies 45

5. RECOMMENDATIONS 46

5.1. EU General Priorities 46

5.2. Extension of the scope of data protection and harmonization of legal concepts 47

5.3. Oversight of EU agencies in the field 48

5.4. US/ EU Relations 48
5.5. EU ownership over data 48

References 49

Annexes 54

LIST OF ABBREVIATIONS

AWFs	Analysis Work Files
CERTs	Computer Emergency Response Teams
CIIP	Critical Information Infrastructure Protection
CLP	Cloud Legal Project
DoS	Denial-of-Service
DPA	Data Protection Authority
DPD	Data Protection Directive
DPFD	Data Protection Framework Decision
EC3	European Cyber Crime Centre
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
ENU	Europol National Units
EPCIP	European Programme for Critical Infrastructure Protection
EU ISS	EU Internal Security Strategy
EWS	Amazon Web Services
FISAA	Foreign Intelligence Surveillance Amendment Act
HTCC	High Tech Crime Centre
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
iOCTA	Internet Facilitated Organised Crime Report
LEA	Law Enforcement Authorities
NASA	National Aeronautic Space Administration
NIS	Network and Information Security
OASIS	Organisation for the Advancement of Structured Information Standards
OCSIA	UK Office of Cyber Security and Information Assurance
PaaS	Plaftorm-as-a-Service
PGDPR	Proposal for a General Data Protection Regulation
PPCJDD	Proposal for a Police and Criminal Justice Data Protection Directive
SaaS	Software-as-a-Service

SHA	Safe Harbour Agreement
SLA	Service Level Agreement
WP29	Article 29 Data Protection Working Party

LIST OF FIGURES

FIGURE 1: The relation between NIS, cybercrime and data protection seen by DG INFSO **22**

FIGURE 2: The triangular diplomacy of cloud computing from the point of view of the global regulation of the Internet **29**

FIGURE 3: The triangular diplomacy of cloud computing from the point of view of the individual **30**

EXECUTIVE SUMMARY

Background

While cloud computing is not a new technology *per se* and has been developed and marketed primarily for profit-driven purposes, the growing reliance on its infrastructures and services poses a series of challenges for EU strategies and policies. This study addresses these challenges, examining the current EU framework in the field and highlighting the legal aspects in relation to the right to data protection, the issue of jurisdiction, responsibility and the regulation of data transfers to third countries.

Aim

The study starts by investigating the issues at stake when dealing with cloud computing (Sections 1 and 2). It suggests that the main concern arising for private citizens, companies and public administration using cloud technologies is **not so much the possible increase in "cyber" fraud or crime than the loss of control over one's data**. From a risk-assessment perspective, the higher risk is indeed to be found in the management of the data contained in data centres, whether this management is of a criminal nature or not.

Currently, the EU framework on cloud computing in relation to cybercrime lacks a clear sense of direction, priorities and practical coordination (Section 2.2). The various components of the EU's cybercrime policy framework fall under the responsibility of different services and involve different groups of experts and 'stakeholders'. The Commission's decision to locate the European cybercrime centre (EC3) within EUROPOL raises further questions over the respective roles of the European Network and Information Security Agency (ENISA) and EUROPOL. Moreover, the way in which the Commission envisages the role of EC3 perpetuates the habit of providing a list of activities, blurring priorities and a sense of direction, as well as a reliable assessment of the resources that are required to meet the stated goals. However, the main concern remains the lack of a concept of 'cybercrime' within the EU. This has direct implications for the functioning of the proposed EC3 as part of EUROPOL and creates a wider degree of uncertainty for the individual as regards lower data protection standards for 'cybercrime' and whether this differs from other crimes such as 'computer crime' and/or other 'serious crimes'. In the field of cybercrime, the study thus strongly underlines that **the challenge of privacy in a cloud context is underestimated, if not ignored** (Section 3). In most European *fora* dealing with cybercrime, Data Protection laws appear to be marginalised in the agenda and inadequately addressed. The data subject and its protection are therefore key to ensure that the rule of law, democratic principles and human rights are guaranteed by EU law and regulations.

This study therefore examines in depth what is at stake from the perspective of data protection and privacy (Sections 3 and 4). The set of relations currently defining cloud computing technologies encompasses negotiations and tensions between public authorities, private entities and public and private authorities. In this set of relationships, data protection and privacy are often objects of negotiation to the detriment of individual rights. Where cloud computing is possibly most disruptive is where it **breaks away from the forty-year-old legal model for international data transfers**, jeopardising the rights of the EU citizens:

- Consumers' rights are subsumed into a complex mesh of contracts among private entities. Therefore, from a legal perspective, the challenge of jurisdiction is central. The legal determination of both the responsibilities and legal liabilities of data controllers and processors and the rights of the individual as 'data subject' are paramount.
- Lack of legal certainty surrounding the concept of cybercrime and legal frameworks of cloud-based investigations, as well as inadequate tools to safeguard privacy and data protection increase the potential for misuses and abuses by law enforcement actors and agencies. European citizens' data are not sufficiently protected in this regard. This aspect is enhanced by exceptional measures taken in the name of security and the fight against terrorism. The US context is here particularly illuminating, both in the case of the Patriot Act and in the case of the US Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008. In this case, the question of the legal framework of data transfers/processing to third countries is critical.

These elements, examined throughout this study, have been neglected in EU policies and strategies, despite their very strong implications for EU data sovereignty and the protection of citizens' rights.

GENERAL INFORMATION

KEY FINDINGS

- The main concern arising from the growing reliance on cloud computing is less the possible increase in cyber fraud or crime than the loss of control over individual identity and data.
- To a large extent, cloud computing is not a genuinely new technology, it contributes to the growth of cross-border transfers of data and as such poses a set of original challenges to EU policies, including with regard cybercrime and privacy.
- These challenges comprise, first and foremost, the establishment of clear priorities in the current set of measures implemented by EU agencies, bodies and institutions in relation to "cyber" security matters. Who is most at risk in the context of cloud computing, and how these risks come about, are core questions in this regard.
- Cloud computing raises a number of specific legal challenges in relation to the right to data protection, including the development of a legal definition of cybercrime, the issue of jurisdiction and responsibility, the regulation of data transfers to third countries, and of the work of EU agencies.
- Risks associated with cloud computing are an exacerbation of traditional information security concerns. The risk faced by individuals using cloud services is the most central.
- There is considerable disagreement over the risks that can actually be attributed to cybercrime. Some experts consider that companies are most at risk and face the steepest costs, while others argue convincingly that average citizens are the most concerned.
- The various components of the EU's cybercrime policy framework currently fall under the responsibility of different services and involve different groups of experts and 'stakeholders'. This contributes to unclear priorities and possible misallocation of resources.
- The Commission's decision to locate the European cybercrime centre (EC3) within EUROPOL raises the question of the respective roles of ENISA and EUROPOL.
- The way in which the Commission envisages the role of EC3 perpetuates the habit of providing a list of activities, blurring priorities and a sense of direction, and lacking a reliable assessment of the resources that are required to meet agreed goals.
- The set of relations currently defining cloud computing technologies encompasses negotiations and tensions between public authorities, private entities and public and private authorities. In this set of relationships, data protection and privacy are often objects of negotiations to the detriments of the individuals' rights.
- If one places the individuals and her/his rights at the centre of the discussion, the cybercrime dimension is but one of the pending issues. Where cloud computing is possibly the most disruptive is in the fact that cloud computing breaks away from the forty-year-old legal model for international data transfers.
- In the field of cybercrime, the challenge of privacy in a cloud context is underestimated, if not ignored. In most European *fora* dealing with cybercrime, Data

Protection laws appear to be very marginal in the agenda and inadequately addressed to meet the challenges.

- The question of privacy and data protection is furthermore challenged by exceptional measures taken in the name of security and the fight against terrorism. The US context is here particularly highlighting, both in the case of the Patriot Act and in the case of the Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008. These elements have been totally neglected, despite very strong implications on EU data sovereignty and the protection of its citizens' rights.

- Conceptual uncertainties emerge in relation to the wide room of discretion by the Member States at times of establishing jurisdiction i.e. the applicable implementing law of the Member State under the Data Protection Directive (DPD). This most directly causes uncertainty for any affected individual who might face conflict of laws resulting from the multiple national implementing legislations. A targeting/directing test would establish jurisdiction in relation to data connected to the EU, but would not rule out conflict of laws nor preclude secret surveillance by third countries. Yet, these initiatives should be seen as valuable tool to ensure that US companies are "in principle" covered by EU Data Protection Law

- An'accountability approach' would imply the vesting of obligations and liabilities upon every actor with considerable power, i.e. knowledge and control of the personal data. This explains why anonymous data, i.e. data to which there is a minimized risk of unauthorized access, are no 'personal data' in the DPD. Standard setting on the EU level as regards what constitutes personal data would contribute to a harmonized approach to the "who" question (see Annex 2), i.e. who is the cloud user data (joint) controller, data processor, data subject. This "who" question is important in light of the question of jurisdiction and the resulting or potential responsibilities, liabilities and obligations towards the individual.

- Definitional uncertainties also emerge in relation to self-regulatory data protection regimes 'quite separate from the wider EU level framework on data protection', when assessing data transfers to third countries. The notion of 'adequacy' as regards data transfers to third countries is defined on several levels (Member States, European Commission and EUROPOL), and this further expands the vulnerability of the data subject as regards what actually are 'adequate data protection standards', and the capacity to control her/his data as a fundamental right. This is exacerbated by the lack of a concept of cybercrime within the EU, which creates even more legal uncertainty for the individual as regards the justification of lower data protection standards for cybercrime.

INTRODUCTION

KEY FINDINGS

- The main concern arising from the growing reliance on cloud computing is less the possible increase in cyber fraud or crime than the loss of control over individual identity and data.
- To a large extent, cloud computing is not a genuinely new technology, it contributes to the growth of cross-border transfers of data and as such poses a set of original challenges to EU policies, including with regard cybercrime and privacy.
- These challenges comprise, first and foremost, the establishment of clear priorities in the current set of measures implemented by EU agencies, bodies and institutions in relation to "cyber" security matters. Who is most at risk in the context of cloud computing, and how these risks come about, are core questions in this regard.
- Cloud computing raises a number of specific legal challenges in relation to the right to data protection, including the development of a legal definition of cybercrime, the issue of jurisdiction and responsibility, the regulation of data transfers to third countries, and of the work of EU agencies.

This study argues that the main concern arising from the growing reliance on cloud computing by private citizens, companies and public administration is less the possible increase in "cyber" fraud or crime than the loss of control over individual identity and data. As we will detail further below (1.1.), cloud computing does make cross-border transfers of data ubiquitous and instantaneous in our "information societies". As such, cloud computing has drawn the attention on the need for a global regulation of the Internet, but this focus on regulation has rendered the individual and his rights invisible. The discussion has concentrated on issues of traceability of IP addresses in a cloud computing context, on threats to national security associated with cyber attacks on critical infrastructures, and on dramatic forms of cyber criminality such as child pornography. The citizen is taken into account, but as the victim of crimes such as identity theft or botnet attacks, not as a bearer of rights, including the right to data protection and to privacy.

This note aims at reverting this trend and examines the consequences of putting the individual at the centre of the system of triangular diplomacy at play over the question of cloud computing, between national authorities of the country where s/he resides, the companies providing cloud computing infrastructures, platforms and services, and the international stage where other national governments and transnational bodies such as the EU define the stakes involved in the global regulation of an Internet redefined by cloud computing innovations.

Assessing these innovations is important in order to avoid both sceptical and catastrophic framings of cloud computing. For the sceptics, cloud computing has brought no particular change. For the catastrophists, cloud computing is a radically new phenomenon that calls for more control over the Internet, viewed as a "Far West" with outlaw, but without a proper sheriff. As this note will argue, the terminology of "the cloud" in itself comes from advertisement, and reflects an effort at "branding" distributed parallel computation services. But "the cloud" does not float in the air and is not purely virtual. It involves an

infrastructure of data centres that is thoroughly territorialised, within which data moves at high speed and can neither be traced nor localised easily. Cloud computing thus creates a series of challenges tied to the means of countering attacks, to the difficulties for law enforcement agencies to trace the activities of criminals, ad to the quasi-impossibility for EU citizens to know exactly what has been done with their personal data when it is processed by companies either using or providing cloud services. Existing legal protections, such as Safe Harbour for US-based companies, are limited. They rest on the good will of third parties and are not tied to real enforcement powers. This also holds true when the data (whether personal or anonymised) of EU citizens is used for the purpose of preventing illegal acts.

1.1. Cloud computing technologies

Cloud computing can be defined in general terms as the distributed processing of data on remotely located computers accessed through the Internet[1]. To some extent, cloud computing is not really a new technology, but a new business model for companies such as Amazon, Google or Microsoft to commoditise the extraneous capacities of their data centres. The more advanced forms depend on new software techniques that allow simultaneous processing of data, distributed automatically over massively parallel hardware.

Cloud computing is geographically distributed across data centres. A data centre is a warehouse-sized building equipped with backup power supplies and air conditioning, housing racks containing tens of thousands of identical circuit boards (called “blades” - each containing a complete powerful computer) and disk drives. The blades and disks are all connected to high speed networking cables, and the programs to be run are orchestrated by an underlying “fabric” of software managing the available resources. While some of these data centres can be located[2], a consolidated map of all of them is currently not available.

There is arguably not a single cloud but several. The cloud can firstly be understood in terms of the services provided through it. Most studies distinguish between at least three technical varieties of cloud computing in this regard:

1. Infrastructure-as-a-Service (IaaS): the provision of computing and storage resources for remote control over the Internet. These resources usually are “virtual” machines, simulations of machines in software which share the resources of many physical machines efficiently.
2. Software-as-a-Service (SaaS): the provision of software applications (e.g. for word processing or spreadsheets), running on server computers in a datacentre, to remote users through their local computer acting as a terminal.
3. Platform-as-a-Service (PaaS): a Cloud operating system designed to distribute the dynamically varying demand for resources automatically over hundreds or thousands of machines, without needing to alter the code of programs written for that platform.

[1] See, *inter alia*, European Commission (2012(e)), *Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final.

[2] See e.g.: http://www.google.com/about/datacenters/inside/locations/ or http://www.zdnet.com/blog/microsoft/where-in-the-world-are-microsofts-datacenters/5700.

Each of these forms of cloud computing allow customers to be billed only for the resources they use, and more resources can be allocated "elastically" up to the aggregate capacity of the available data centres. Services such as Google Search or Facebook social networking are not examples of cloud computing as such, but are applications built on a foundation of PaaS architecture. Office365 is an example of SaaS. Services offering the hosting of virtual machines running the user's choice of operating system are an example of IaaS. A further distinction can be made between public clouds which involve the provision of IaaS/SaaS/PaaS to many customers sharing the processing power of a machine in a data centre, contrasted, and private clouds which are used only by a single customer (or a restricted group) usually for security reasons.

Although the application software must be written from scratch in special languages, only PaaS is capable of the true "elastic" scaling of demand from one machine to many thousands. By contrast, IaaS is arguably not "real" cloud computing at all, in that the only difference from traditional means of leasing computing power at a distance is that the machines are virtual. So far, major commercial PaaS platforms are offered only by US companies. Most cloud providers in the EU are actually reselling services controlled and designed in the US, and their privacy policies state that data will be exported to the US.

1.2. Cloud computing, cybercrime and privacy: what are the challenges?

If to some degree cloud computing is not a genuinely new technology, it does nonetheless hold the potential for presenting original challenges to EU policies in the field of information society as well as justice and home affairs. The growing reliance on cloud computing contributes to the growth of trans-border flows of data, not only within the EU, but also with third countries and particularly the United States. Cloud computing is usually envisaged as a challenge to the global regulation of the Internet. In the field of security, these concerns involve the questions of (information) infrastructure protection on the one hand, of the fight against crime on the other, as well as defence considerations linked with possibilities of cyber-spying and cyber-sabotage. These are certainly important stakes, but they fall mostly under the responsibility of Member States. Given that this study focuses on the EU, we will in the following pages concentrate on the issues related to the protection of EU citizens against crime, and to the guarantee of his fundamental freedoms and rights in the context of an increasingly cloud-intensive Internet.

The 'challenge of challenges', so to speak, is therefore to clarify what it is that EU bodies should be predominantly concerned with in the first place. This is a particularly timely discussion, given the recent creation of a European Cybercrime Centre (EC3) within the European Police Office EUROPOL, and the forthcoming adoption of an EU Cybersecurity strategy by the European Commission (foreseen December 2012 at the time of writing). Should the focus be on combating online criminality (i.e. cybercrime) in order to protect the data of EU citizens from fraudsters using 'the cloud' as an asset or a target? Is the main concern tied to the loss of sovereignty resulting from cyber-sabotage and cyber-spying and tensions among states? Or should the emphasis be placed on providing legal certainty in jurisdiction-spanning transfers of data involving a multiplicity of data controllers and processors? Ultimately, this raises the question of who is most affected by online developments among companies, states and individuals. As discussed in the study, it is certainly the case that the most pressing challenge, which is still not examined and recognised as such, lies with the provision of legal certainty to EU citizens regarding their right to data protection and their right to privacy.

The question of priorities associated with the challenge of privacy is thus central, and is the main issue discussed in this study. More specifically:

- Section 2 provides an overview of the **current knowledge on risks arising from the growing reliance on cloud computing**, continuing with a brief survey of the EU policy and operational framework in this regard.
- Section 3 builds on the conclusions of this overview to suggest that the main concern might not lie specifically or exclusively in dealing with fraudsters. **Cloud computing brings into focus the triangular diplomacy at play between states, companies and the inter-state system in the global regulation of the Internet**. The unfolding of this triangular diplomacy puts into question the degree to which the protection of individuals is central in current discussions of cloud computing. In this regard, it appears that the provision of the best legal and technical guarantees to EU citizens regarding their data is the most central and pressing challenge.
- Section 4 develops a legal perspective on this discussion. Cloud computing and cybercrime pose legal challenges to fundamental legal concepts in the fragmented EU legislative framework. Firstly, definitional uncertainties relate to the Member States' discretion to establish jurisdiction, and this creates legal uncertainty for the individual as regards the applicable law. Secondly, definitional uncertainties relate to the multiple definitions of adequacy as regards data transfers to third countries, and this creates legal uncertainty for the individual as regards the definition of 'adequate data protection standards'. This is exacerbated by the lack of a concept of cybercrime within the EU, which creates even more legal uncertainty for the individual as regards the justification of lower data protection standards for cybercrime.
- Section 5, finally, outlines several key recommendations for current and upcoming EU activities with regard cloud computing.

2. CLOUD COMPUTING, CYBERCRIME, PRIVACY: THE EU FRAMEWORK

KEY FINDINGS

- Risks associated with cloud computing are an exacerbation of traditional information security concerns. The risk faced by individuals using cloud services is the most central.
- There is considerable disagreement over the risks that can actually be attributed to cybercrime. Some experts consider that companies are most at risk and face the steepest costs, while others argue convincingly that average citizens are the most concerned.
- The various components of the EU's cybercrime policy framework currently fall under the responsibility of different services and involve different groups of experts and 'stakeholders'. This contributes to unclear priorities and possible misallocation of resources.

- The Commission's decision to locate the EC3 within EUROPOL raises the question of the respective roles of ENISA and EUROPOL.
- The way in which the Commission envisages the role of EC3 perpetuates the habit of providing a list of activities, blurring priorities and a sense of direction, and lacking a reliable assessment of the resources that are required to meet agreed goals.

> "*The advanced methods discovered in Operation High Roller show fraudsters moving toward cloud-based servers with multi-faceted automation in a global fraud campaign*"
>
> (David Marcus, director of security research for McAfee Labs - June 2012).

In a white paper published in June 2012[3], McAfee and Guardian Analytics described what supposedly exemplified cybercrime moving to the cloud. "Operation High Roller" designates a series of highly sophisticated campaigns designed to take money out of bank accounts in Europe, the U.S. and South America through automated transfers. If the first stage of the fraud can be seen as "traditional" (phishing e-mail, use of a Trojan - in this case Zeus or SpyEye), the final stage was allegedly more innovative, the fraudsters operating malware from a server in the cloud. The McAfee/Guardian Analytics white paper concluded by stressing new opportunities for criminals arising from "the cloud".

The latest Europol Report dedicated to cybercrime (iOCTA - 2011) echoes these concerns. It states that the process of outsourcing data storage to third parties (as a cost-saving option and a way of remote access to data from any location) "*poses both a threat to users and a challenge to law enforcement. Data stored in the Cloud is not only accessible to all authorized users, but also vulnerable to external attacks*"[4].

The fraud described in Operation High Roller indeed shows how the cloud can be used for illicit purposes. It also emphasizes the high level of sophistication of the individuals who planned it.

The 2002 Proposal for a Council Framework Decision on attacks against information systems, in its §28 distinguishes between 'criminal attack (threat) to computer infrastructure' and 'computer-assisted crime (threat)':

> First, threats to computer infrastructures, which concern operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computer and networks themselves. Secondly, computer-assisted threats, which concern malicious activities, such as fraud, money laundering, child pornography, infringement to intellectual property rights and drug trafficking, which are facilitated by the use of a computer.

However, while the cloud certainly offers new possibilities for criminals and can be a facilitator for a wide range of criminal activities, to single out cloud computing as a new type of cybercrime is problematic, and this section emphasises the following:

- First, **cloud technologies are a means to commit crime**, much like other computer-related technologies (i.e. viruses, phishing, botnets, malware, etc.).

[3] Marcus, D. and Sherstobitoff, R. (2012), *Dissecting Operation High Roller*, White Paper, June 2012.
[4] EUROPOL (2011), Threat Assessment Report (Abridged), *Internet Facilitated organised Crime – iOCTA,* January 2011, p.10.

- Second, if cloud technologies can be seen as a key challenge for all online data storage users, **major risks are not necessarily coming from fraudsters**.

2.1. What is at risk with the cloud?

Among the various reports tabled by EU institutions as well as other public or private bodies in recent years on cloud computing, cybercrime is not particularly singled out as a specific concern. Out of the ten 'top security risks' listed by the European network and information security agency ENISA in a recent report on the cloud[5], only two, possibly three can be potentially related to criminal activities. This includes the possibility of attacks launched on isolation mechanisms (since cloud computing is based on multi-tenancy and shared resources, isolation of tenant 'spaces' is central), the compromising of management interfaces which would give attackers access to a potentially greater set of resources than in traditional, networked computing, and the possibility of a so-called 'malicious insider' within a cloud service provider. **These risks are arguably an exacerbation of traditional information security concerns rather than something brought about exclusively by cloud computing**. The same can be said about the above mentioned Operation High Roller, where the fraud was based on a denial-of-service attack - DoS attack, *i.e.* an attempt to make a machine or network resource unavailable to its intended users that has nothing specific to the cloud.

By contrast, the central point emphasised in the ENISA report is the **risk faced by customers if the cloud provider makes improper use and/or mismanages the data** contained in its data centres. One of the main challenges raised by cloud computing are those of privacy and trust and not only security, even though the quality of the protection measures put in place is of course central. Cloud-computing infrastructure is indeed today almost exclusively owned by private companies, and represents a significant and growing part of the Internet. Thus, the economic aspects and commercial interests should not be underestimated. The cloud services provided by well-known US based company Amazon (under the label Amazon Web Services, EWS), for instance, is presumed to account for 1% of all Internet consumer traffic[6]. This trend appears to be reinforced as the current economic and financial crisis brings budgetary control into the spotlight, leading public authorities to opt for outsourcing cloud computing to private entities, sometimes to the detriment of other initiatives. A good example is the June 2012 decision by US space agency NASA to shift part of its infrastructure to the aforementioned Amazon EWS to the detriment of its efforts in the development of open-source cloud platform OpenStack, an initiative it had founded with company Rackspace Hosting[7].

The question, in this regard, is whether the focus on cloud computing from the perspective of cybercrime is appropriate and in tune with the challenges raised by cloud computing. As detailed in the following subsection, this is all the more stringent as the current EU policy framework dealing with cybercrime is piecemeal, a situation that follows in part from the development of two distinct perspectives, one pertaining to network and information security and the other to law-enforcement.

[5] European Network and Information Security Agency (ENISA) (2009(a)), *Cloud computing: benefits, risks and recommendations for information security*, Heraklion, November 2009.

[6] Based on estimates by US-based start-up Deepfield, see: Labovitz, C. (2012), 'How Big is Amazon's Cloud?', 18.3.2012, available from: http://www.deepfield.net/2012/04/how-big-is-amazons-cloud/, retrieved 20.8.2012.

[7] See the announcement by NASA Chief Information Officer Linda Cureton, 'IT Reform at the National Aeronautics and Space Administration', 8.6.2012, available from http://blogs.nasa.gov/cm/blog/NASA-CIO-Blog/posts/post_1339205656611.html, retrieved 20.8.2012.

2.2. Cloud computing and the EU legal, policy and operational framework

2.2.1. The problem with measuring cybercrime

The 2007 EU Commission's communication dedicated to computer-related crimes gives this definition of cybercrime: "criminal acts committed using electronic communications networks and information systems or against such networks and systems":

> In practice, the term cyber crime is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of illegal content over electronic media (i.e. child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking[8].

As underlined by many scholars and experts, this definition of cybercrime is highly problematic from a legal point of view. The lack of a concept of 'cybercrime' within the EU has direct implications for the functioning of the proposed European Cybercrime Centre (EC3) as part of EUROPOL[9], and creates a larger degree of uncertainty for the individual as regards lower data protection standards for 'cybercrime' and whether this differs from other crimes such as 'computer crime' and/or other 'serious crimes'. Furthermore, the scope of this definition, as well as the three types of crime presented (internet facilitating various types of crimes, illegal use of online data, crimes specific to electronic networks) means that a significant proportion of criminal activities fall, in one way or another, under the heading of cybercrime.

As a consequence, **attempts to measure the cost of cybercrime should be considered with caution**, all the more since available figures tend to be hotly disputed, as the recent controversy over the Detica study in the United Kingdom illustrates. In February 2011, the UK Cabinet Office commissioned Detica, a private company working in the area of information intelligence with governments and commercial customers, to work jointly with the UK Office of Cyber Security and Information Assurance (OCSIA)[10] to assess the costs of cybercrime to the British economy. The Detica study focused on three phenomena:

1. identity theft and online scams affecting UK citizens;
2. IP theft, industrial espionage and extortion targeted at UK businesses;
3. Fiscal fraud committed against the Government.

It calculated the magnitude of the costs of cyber crime using three-point estimates (worst-case, most-likely case and best-case scenarios), focusing in particular on IP theft and industrial espionage and its effect on the different industry sectors. According to the study's most-likely scenario, the cost of cybercrime to the UK amounted to £27bn per annum. A

[8] European Commission (2007), *Communication to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime*, SEC(2007) 641, SEC(2007) 642, COM/2007/0267 final, Brussels, 22.5.2007.

[9] European Commission (2012(d)), *Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final, Brussels, 28.03.2012, p. 7.

[10] The OCSIA supports the UK Minister for the Cabinet Office and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK.

significant proportion of this cost comes from the theft of IP from UK businesses, which they estimate at £9.2bn per annum.

These figures have been met with skepticism, to the extent that an alternative study was subsequently commissioned, this time by the UK ministry of Defence. Undertaken by four independent researchers, the second study built on a report initially commissioned in 2008 by ENISA on `Security Economics and the Single Market'[11]. The report submitted to ENISA analysed the statistics available at the time, their shortcomings, and the ways in which they could lead to incorrect policy decisions. One of the element emphasized in this study was the lack of hard data about information security failures, as many of the available statistics are not only poor but are collected by parties such as security vendors or law enforcement agencies that have a vested interest in under- or over-reporting.

The report commissioned by the UK ministry of Defence, entitled 'Measuring the Cost of Cybercrime'[12], further identified which figures are actually known, what can reasonably be estimated and what can only be guessed. According to the data gathered and analysed, it came to the following conclusions[13]:

1. Traditional frauds such as tax and welfare fraud cost citizens a few hundred pounds/euros/dollars a year. With such crimes, the costs of defence – i.e. the monetary equivalent of prevention - are much less than the amounts stolen.
2. Transitional frauds such as payment card fraud cost citizens a few tens of pounds/euros/dollars a year. Online payment card fraud, for example, typically runs at 30 basis points, or 0.3% of the turnover of e-commerce firms. Defence costs are broadly comparable with actual losses, but the indirect costs of business foregone because of the fear of fraud, both by consumers and by merchants, are several times higher.
3. The new cyber-frauds such as fake antivirus net their perpetrators relatively small sums, with common scams pulling in tens of cents/pence per year per head. In total, the earnings of cyber-fraudsters might amount to a couple of dollars per citizen per year. But the indirect costs and defence costs are very substantial, at least ten times that. The cleanup costs faced by users (whether personal or corporate) are the largest single component; owners of infected PCs can spend hundreds of dollars, while the average cost to each of us as citizens runs in the low tens of dollars per year. The costs of antivirus (to both individuals and businesses) and the cost of patching (mostly to businesses) are also significant at a few dollars a year each.

The report concludes that **despite the fact that cybercrimes are global and have strong externalities, the figures suggest that less funding should be allocated to measures anticipating cybercrime (on antivirus, firewalls, etc.) and more to reactive measures**: that is to "*the prosaic business of hunting down cyber-criminals and throwing them in jail*". Another element usefully recalled in the report is the mere fact that **the misallocation of resources associated with cybercrime results more from economic and political factors than from behavioral ones** and that *"previous studies of cybercrime have tended to study quite different things and were often written by organisations (such as vendors, police agencies or music industry lawyers) with an obvious `agenda'"*[14].

[11] Anderson, R., Bohme, R., Clayton, R., Moore, T. (2008), *Security Economics and the Single Market*, 2008.
[12] Anderson, R., Barton, C., Bohme, R. e*t al* (2012), *Measuring the Cost of Cybercrime*, Workshop on the Economics of Information Security, June 2012.
[13] Ibid, Conclusions of the study, p.25
[14] Ibid, p.2

This element in particular contrasts with the conclusions of the Detica report, which presents business as facing the steepest costs and encourages more governmental funding in the area of prevention and improvement of cyber security. One should keep in mind that Detica is part of BAE Systems, a global defence and security company, with activities in the field of cybersecurity, risk management and compliance. As underlined in the UK ministry of Defence report, the long-term winners of the fight against cybercrime as it is now steered may well be firms such as BAE Systems, but also Google and Microsoft as people are driven to webmail services with good spam protection. One could argue here that **the need to fight cybercrime in a proactive manner is an argument deployed by industry, largely for commercial purposes**.

This is all the more important as the reports of EU bodies draw significantly on the expertise provided by private companies. EUROPOL's 2011 iOCTA report states for instance that "whilst the value of the cybercriminal economy as a whole is not yet known, one recent estimate of global corporate losses stands at approximately $1 trillion per year" (p.5). This figure is derived from a report by antivirus software provider McAfee on "Unsecured Economies: Protecting Vital Information" released at the World Economic Forum annual meeting in Davos in 2009. To avoid the risk of inflation in assessments of cybercrime, it seems that legal clarity and precision are important: the iOCTA report describes in length "internet facilitated organised crime", without clarifying what cybercrime covers and does not cover. In the meantime, iOCTA remains conservative for what concerns cloud computing. Echoing the findings of the 2009 ENISA risk assessment of the cloud, iOCTA actually implies that **cybercrime is less central than the customer-provider relationships**:

> whilst corporate owned servers are evidently themselves subject to hacking, the lack of direct control entailed by cloud computing raises concerns about whether security measures will be properly enforced by the storage provider, or understood by the data owner or customer. In the cloud computing scenario, for example, the personal and financial data of retail customers could be stored on the Internet by a third party without that customer's knowledge, and without the direct control of the organisation who has processed that data. The key to cloud computing's success and long-term uptake will be whether the convenience of remote access will be matched by confidence in its security provisions. (p.10)

There is no doubt that computer-related crimes are serious matters affecting citizens as well as public infrastructures and private businesses. **The question, however, is whether the priority lies in a technological build-up and proactive measures, or in the pursuit of traditional criminal justice aims**. Section 4 below outlines in this regard the critical importance of having legal certainty on the ownership over one's data, and thus the importance of consent of the customers. With regard risks of financial fraud, botnets, hacking, phishing, spamming, the new opportunities offered by the cloud, are also real. One should however not lose sight of what is at stake in the emphasis placed on security provisions related to the cloud, and whose interests are thereby promoted. Moreover, the lack of legal certainly that surrounds the concept of cybercrime, as well as the lack of certainty when it comes to its costs, raises concerns towards the EU policy framework in the field.

2.2.2. The EU legal and policy framework

The EU legal and policy framework regarding cybercrime, fundamental freedoms and rights

including the right to privacy has already been described in detail elsewhere[15]. **The principal, general-purpose legal instrument in this area remains the 2001 Council of Europe Convention on Cybercrime (ETS 185)**. In addition, and although a number of policy documents have sought to provide a strategic overview of EU measures – most recently the European Commission's communication on 'Tackling crime in our digital age' - [16], **there is no overall policy orientation** on the issue. It remains to be seen whether the upcoming EU strategy on cybersecurity, announced in May 2012, will provide such a framework.

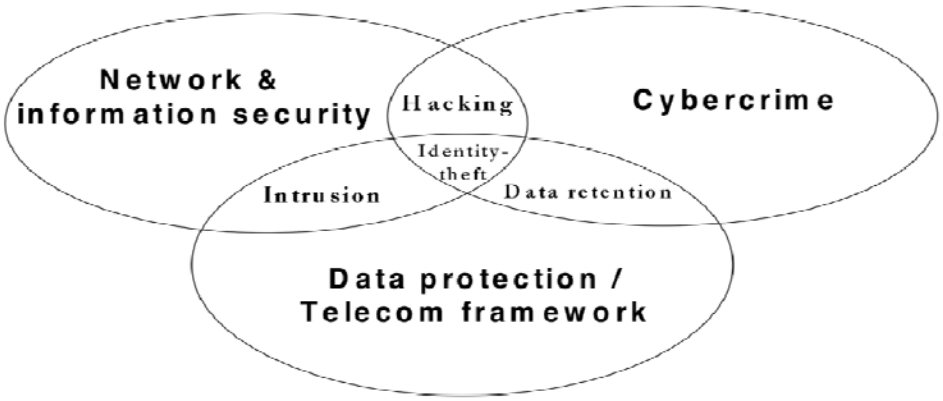
Criminal law measures adopted through the EU on the question of cybercrime have focused most substantively on the question of attacks on information systems. The relevant instrument here is Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[17]. The implementation of this Decision was reviewed in July 2008, with the Commission report highlighting the need for an update in light of the increase of 'botnet'-based attacks[18]. In September 2010, the Commission published a proposal for a directive repealing Framework Decision 2005/222/JHA, which is currently awaiting Parliament first reading[19]. References to cyber-crime can also be found in criminal law instruments targeting the sexual exploitation of children and child pornography. Measures listed in Council Framework Decision 2004/68/JHA target both online and offline conducts[20]. The Framework Decision has been replaced by Directive 2011/92/EU of 13 December 2011, which establishes minimum common rules among Member States (beyond the objective of approximation contained in the Framework Directive), incorporates elements from the relevant Council of Europe Convention adopted in 2007 (ETS 201), and includes elements regarding new criminal offences in the IT environment[21]. Criminal law measures related to cybercrime and adopted through the EU, finally, are also said to include the 'online' components of other offences[22]. This comprises terrorism, as provided for by Council Framework Decision 2008/919/JHA[23] as well as acts of racism and xenophobia[24].

The question of cybercrime is also considered in the context of EU measures related to network and information security (NIS) and critical information infrastructure protection (CIIP). NIS and cyber-crime (understood as 'computer-related crime') were initially considered within the same framework, as the Commission's first 'cybercrime communication' of January 2001 illustrates[25]. As early as June 2001 however, the

[15] Peers, S. (2009), *Strengthening Security and Fundamental Freedoms on the Internet – An EU Policy on the Fight Against Cybercrime*, PE 408.335, European Parliament, Brussels, January 2009.
[16] European Commission (2012(d)).
[17] Council of the EU (2005), Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69/67, 16.3.2005.
[18] European Commission (2008), *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, COM(2008) 448 final, Brussels, 14.7.2008.
[19] European Commission (2010(b)), *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, COM(2010) 517 final, 30.9.2010.
[20] Council of the EU (2004), Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, OJ L 13/44, 20.1.2004.
[21] European Parliament and Council of the EU (2011), Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335/1, 17.12.2011.
[22] For a summary see Peers, S., op.cit.
[23] Council of the EU (2008(b)), Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, OJ L 330/21, 9.12.2008.
[24] Council of the EU (2008(a)), Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328/55, 6.12.2008.
[25] European Commission (2001(a)), *Creating a Safe Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM(2000) 890 final, Brussels, 26.1.2001.

Commission's DG INFSO tabled a separate communication on 'network and information security'[26]. The document states in particular that 'the proposed policy measures [..] have to be seen in the context of the existing telecommunications, data protection and cyber-crime policies [..][and] will provide the missing link in this policy framework'. The communication envisaged this framework through Figure 1 below.

Figure 1: The relation between NIS, cybercrime and data protection seen by DG INFSO[27]



The focus of NIS activities is 'the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious action'[28]. Attention is thus directed to the conditions through which such confidence can be achieved and guaranteed. The original purpose of the ENISA, initially established in 2004[29] was to foster such conditions. NIS activities sponsored through the focus of a 'secure information society' have since been relabelled as part of the EU's developing European Programme for Critical Infrastructure Protection (EPCIP) steered in the framework of the area of freedom, security and justice[30]. While NIS persists as a policy identifier, a number of activities related to it are now undertaken as part of the so-called CIIP framework[31].

As suggested so far, then, **the various components of the EU's cybercrime policy framework fall under the responsibility of different services and involve different groups of experts and 'stakeholders'**. The Commission's first 'cybercrime communication' of January 2001 was a joint endeavour between the institution's directorate generals in charge of information society (DG INFSO, now CONNECT) and justice and home affairs (DG JHA/JLS/HOME). The 2001 Commission communication on network and information security was steered only by the former. In 2006-2007, DG INFSO led the

[26] European Commission (2001(b)), *Network and Information Security: Proposal for a European Policy Approach*, COM(2001) 298 final, Brussels, 6.6.2001.
[27] Ibid, p. 3.
[28] European Commission (2001(b)), p. 3.
[29] European Parliament and Council of the EU (2004), *Regulation (EC) No 464/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (ENISA)*, OJ L 77/1, 13.3.2004.
[30] European Commission (2006), *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, COM(2006) 251 final, Brussels, 31.5.2006. On EPCIP, see: European Commission (2005), *Green Paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final, Brussels, 17.11.2005.
[31] European Commission (2009), *Critical Infrastructure Protection – Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM(2009) 149 final, Brussels, 30.3.2009; and more recently: European Commission (2011), *Critical Information Infrastructure Protection – Achievements and next steps: towards global cyber-security*, COM(2011) 163 final, Brussels, 31.3.2011.

drafting of the Commission communication on a strategy for a secure information society[32] while DG JLS tabled the communication on a general EU policy on cybercrime[33]. Annex 1 provides a chronological overview of the main initiatives (strategic documents and legislative proposals) related to the question of cybercrime in the EU framework, associating them with the 'lead' Commission services in charge as well as the responsible committee in the European Parliament.

Having different agencies, bodies or services taking the 'lead' or intervening on the issue of cybercrime also entails that different policy outlooks are generated. Efforts to integrate these different outlooks have so far **mostly taken the form of consolidated lists of actions to be undertaken**. A good example of this is the so-called "Pillar III" of the Digital Agenda for Europe initiative on "Trust and security" (Action 28 to 41)[34] that encompasses priorities ranging from the reinforcement of NIS policies to the establishment of Computer Emergency Response Teams (CERTs), and including measures for the fight against cybercrime, trust-building or preparedness against cyber-attacks. The question is whether such a list-based approach should be upheld. **What is the priority, and how should resources be allocated given the limited and contested available knowledge on cybercrime?** Based on the example of the Digital Agenda actions, there seems to be at least three policy domains involved: infrastructure protection, criminal justice, and defence. As shown so far, EU activities have developed primarily in the first two domains. Since these entail very different perspectives on the information society and how security should be pursued in this context, **it might be counter-productive for the Commission to provide a long list of priorities without a proper estimate, for each of them, of personnel and equipment costs, of their feasibility, and without determining which agency is best placed to be in charge** (see below, 2.2.3.). The objective should rather be to define precisely what are the aims of the EU in each policy domain and outline clearly the boundaries between them**. Giving priority to the individual, her or his fundamental rights and freedoms as the core objective of the Union's policy would furthermore give it a sense of direction**. As we will suggest in Section 3 below, in the current "triangular" configuration of policies related to cloud computing, the individual indeed tends to disappear in favour of a focus on the global regulation of the Internet. Reasserting this priority would give EU policies in this area a clear driving principle, in line with the objectives of the Treaties. It is also important given the current development of the EU operational framework in the field of cybercrime.

2.2.3. The EU operational framework in the field of cybercrime

The EU operational framework in the field of cybercrime consists mainly of two sets of measures. Cybercrime is approached through NIS, in relation with the establishment of ENISA, and in the context of EUROPOL's activities in the field of law-enforcement.

ENISA was established in 2004 and is based in Heraklion in Greece. ENISA was set up as a response to cyber security issues faced by the European Union. ENISA, however, is not a JHA body (it contributes to the EU's information society policies) and does not operate directly in the field of law-enforcement. The EU ISS adopted in 2010 failed in this respect to clarify ENISA's future role in the area of internal security, especially with regard cybercrime. In its memorandum submitted to the House of Lords Sub-Committee dedicated to the EU ISS, ENISA defined its contribution to the ISS by an application of proven risk management techniques (identification of information security risks, global risk management and risk assessment, emerging threats and dissemination of good practices

[32] European Commission (2006).
[33] European Commission (2007).
[34] See details on the DAE's website at: http://ec.europa.eu/digital-agenda/en/our-targets/pillar-iii-trust-security.

for risk Management and IT Contingency). In particular, the ENISA Work Programme 2011 included efforts to enhance European cooperation to generate awareness about Networks and information Security, disseminate security relevant information and to assist Member States in coordinating these activities internationally. ENISA had a mandate that was due to expire in March 2012. The EP and the Council recently decide to extend ENISA's mandate to 13th September 2013, which will allow time for debate on how to shape the Agency to meet future needs and challenges in network and information security. As highlighted in a EP report dedicated to the role and future of ENISA,[35] a possible extension of ENISA's mandate is foreseen in the area of cybercrime. In his speech given at the European parliament in May 2011, ENISA's Director stated the following:

> ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between Computer Emergency Response Teams (CERTs) and law enforcement because we need the CERTs in the fight against cyber-crime. The important role of ENISA is to provide an interface between Law Enforcement and the cyber security community[36].

Operational EU law-enforcement measures on cybercrime, on the other hand, have been channelled through EUROPOL.[37] Through its Analysis Work Files (AWFs) information system in particular, the agency has conducted analysis activities[38]:

1. on several cybercrime issues including Internet and ICT related criminal activities falling under Articles 2-8 of the 2001 Cybercrime Convention (AWF/Focal point CYBORG), on payment card fraud (AWF/Focal point TERMINAL), and on sexual exploitation of children through the Internet (AWF/Focal point TWINS);
2. on so-called "cybercrime-related" issues, including counterfeiting and product piracy (AWF/Focal point COPY), suspicious financial transactions (AWF/Focal point SUSTRANS) and Islamist terrorism propaganda on the Internet (AWF/Focal point CHECK THE WEB).

These activities have recently been redeployed following the decision to establish a European Cybercrime Centre in EUROPOL. The Commission announced its intention to establish such a structure in the 'EU Internal Security Strategy in Action'[39] adopted on 22 November 2010. It commissioned a feasibility study funded under the ISEC programme, which was delivered by RAND EUROPE in the early weeks of 2012. The study served as the basis of the Communication on a European Cybercrime Centre, released in March 2012[40]. According to this document, the centre is expected to start operations in January 2013 and is entrusted with the following tasks**:**

- Act as a European focal point in fighting cybercrime.
- Prevent cybercrimes affecting e-banking and online booking activities, thus increasing e-consumers trust

[35] Scott Marcus, J. *et al.* (2011), *The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally*, Brussels: European Parliament, PE464.432.
[36] Helmbrecht, U., (2011), *ENISA today and in the future*, Committee on Industry, Research and Energy, Mini-Hearing on ENISA, Brussels: European Parliament.
[37] In the course of researching for this note, the authors have been contacted by EUROPOL Assistant Director and Head of EC3 Troels Oerting. Two researchers (Didier Bigo and Julien Jeandesboz) visited EUROPOL on 24.10.2012 and had an extensive discussion with Mr. Oerting and members of his team, as well as with Senior Advisor to EUROPOL's Data Protection Office Jan Ellermann. The following points draw partly from the results of this visit.
[38] A full overview of EUROPOL's cybercrime activities, including issues related to data protection, can be found in Drewer, D. and Ellermann, J., (2012), 'EUROPOL's data protection framework as an asset in the fight against cybercrime', *ERA Forum: Journal of the Academy of European Law*, forthcoming.
[39] European Commission, *EU Internal Security Strategy in Action*, IP/10/1535 and MEMO/10/598.
[40] European Commission (2012(d)).

- Protect social network profiles from e-crime infiltration and help the fight against online identity theft
- Focus on cybercrimes which cause serious harm to their victims, such as online child sexual exploitation
- Focus on cyber-attacks affecting critical infrastructure and information systems in the Union
- Warn EU Member States of major cybercrime threats and alert them of weaknesses in their online defences.
- Identify organised cyber-criminal networks and prominent offenders in cyberspace.
- Provide operational support in concrete investigations, be it with forensic assistance or by helping to set up cybercrime Joint Investigation Teams.
- Serve as a knowledge base for national police in the Member States
- Pool European cybercrime expertise and training efforts

To achieve its tasks, the Centre is expected to fuse information from open sources, private industry, police and academia, and will serve as a platform for European cybercrime investigators.

The way in which the European Commission envisages the role of EC3 calls for a number of observations. Firstly, **it perpetuates the habit of providing a consolidated list of activities** we have discussed above in relation to the Digital Agenda for Europe. The tasks allocated to EC3 lack a clear hierarchy of priorities and a sense of direction. It seems that the real added value of a cybercrime centre placed in Europol would be to establish a specific team of specialised law enforcement officers, concerned with and aware of the complexity of the tasks involved in finding out criminals through a moderately regulated Internet and with the possibilities offered by cloud computing. Such a measure might also give assurances to citizens that something is being done and that criminal activities will be investigated. In the meantime, **other tasks such as critical infrastructure protection are beyond the scope of EC3. The same holds true for the preventive monitoring of online activities of the kind supported by private Internet security companies, or conducted by Member State intelligence services** (see in this respect the annex featuring the list of priorities provided by the current head of the EC3).

Secondly, **it does not consistently address the issues of resources allocated to the functioning of EC3**, given the wide scope of the centre's remit. The communication specifies that the estimates provided by the RAND Europe study "will need to be further assessed [..] to be coherent with the overall staffing and budgetary requirements for agencies in the 2013 budget and the next Multiannual Financial Framework" [41]. This point was at the centre of the discussion during the meeting arrange with the EC3 team at EUROPOL for the purpose of this study. The credibility of the new centre requires that the means are adequate to the envisaged tasks. It seems preferable to have a more precise scope of activities, focusing exclusively on crime, and to be effective in this respect. This implies that the European Commission needs to rethink the elements contained in its communication. The document **does not provide a sense of the repartition of tasks between EU bodies, taking into account the differences between NIS and law-enforcement policies discussed previously**. The Commission's decision to locate the cybercrime centre within EUROPOL raises the question of the place and role of ENISA. The list of tasks allocated to the EC3, typically, mentions the "focus on cyber-attacks affecting

[41] Ibid, p. 6.

critical infrastructure and information systems", an area that falls under ENISA's remit, but which also relates to the scope of activities usually undertaken by Member States' defence and intelligence bodies (the fight against cyber-spying and cyber-sabotage). **Does this mean that the Commission foresees EUROPOL as the future EU lead agency in "all things cyber"?** In the current situation, this holistic outlook contrasts with the envisaged remit of EC3 within Europol, which is much more limited. EC3 officials would directly take over the AWF/Focal points CYBORG, TERMINAL and TWINS, and concentrate on the establishment of a fusion centre as a priority.

Thirdly, and **more importantly, the question of who will be in charge of data protection and fundamental rights for the citizens whose data is processed in a context of cloud computing needs to be addressed**. The legal implications of data protection "in the cloud" and in relation with cybercrime-related, law-enforcement matters will be addressed in more details in point 4.5 below. In any case, **a new repartition of tasks and cost assessment, different from that provided by the RAND Europe feasibility study and better reflecting the overall priorities entailed by cloud computing, would be useful.**

The question of the respective roles of EUROPOL and ENISA can thus bear significantly on the EU's policy with regard cloud computing. In this area, ENISA holds a recognised expertise, as exemplified by its 2009 cloud security risk assessment[42], as well as by its proposed assurance framework governing information security risks in the move towards cloud computing[43]. ENISA published in 2011 a report on security and resilience in governmental clouds[44]. ENISA is also undertaking various activities in the domain, including surveys on the security parameters, workshops with third parties such as the Organization for the Advancement of Structured Information Standards (OASIS), a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society as well as risk assessment studies on the impact of a cloud service failure, and in which circumstances cloud services should be considered "critical infrastructure". By contrast, EUROPOL has so far demonstrated little interest in this issue. The "Cloud Computing" section of its 2011 iOCTA is fairly short, at least in the abridged public version. It mentions that the move towards cloud computing poses "both a threat to the individual and a challenge to law enforcement" (p.11) but does not specify this threat or challenge further, only mentioning that cloud data is "vulnerable to external attacks". On the basis of existing risk assessments, however, the degree to which "external attacks" are the main concern arising from the growing reliance on cloud computing is unclear. This observation goes some way to suggest that there is a need to clarify the respective responsibilities of EUROPOL and ENISA with regard cloud computing, if only to avoid duplication of activities and costs and ensure more effective undertakings. Such a clarification, however, should be informed by a clear assessment of what is at stake in the development of cloud computing. As the next section will show, cloud computing is usually envisaged as a matter related to the global regulation of the Internet. In the meantime however, and following the overview of risk assessments provided previously, this issue shadows the question of the individual, her or his rights and freedoms.

[42] Europen Network and Information Security Agency (ENISA) (2009(a)).
[43] Europen Network and Information Security Agency (ENISA) (2009(b)), *Cloud Computing Information Assurance Framework*, Heraklion, November 2009.
[44] Europen Network and Information Security Agency (ENISA) (2011), *Security and resilience in governmental clouds*, Heraklion, January 2011.

3. THE TRIANGULAR DIPLOMACY OF CLOUD COMPUTING AND THE IMPLICATIONS FOR THE INDIVIDUAL

KEY FINDINGS

- The set of relations currently defining cloud computing technologies encompasses negotiations and tensions between public authorities, private entities and public and private authorities. In this set of relationships, data protection and privacy are often objects of negotiations to the detriments of the individuals' rights.
- If one places the individuals and her/his rights at the centre of the discussion, the cybercrime dimension is but one of the pending issues. Where cloud computing is possibly the most disruptive is in the fact that cloud computing breaks away from the forty-year-old legal model for international data transfers.
- In the field of cybercrime, the challenge of privacy in a cloud context is underestimated, if not ignored. In most European *fora* dealing with cybercrime, Data Protection laws appear to be very marginal in the agenda and inadequately addressed to meet the challenges.
- The question of privacy and data protection is furthermore challenged by exceptional measures taken in the name of security and the fight against terrorism. The US context is here particularly highlighting, both in the case of the Patriot Act and in the case of the Foreign Intelligence Surveillance Amendment Act of 2008. These elements have been totally neglected, despite very strong implications on EU data sovereignty and the protection of its citizens' rights.

3.1. The triangular diplomacy of cloud computing: states, companies and inter-state relations

In its 2012 'Sopot Memorandum' on cloud computing, the International Working Group on Data Protection in Telecommunications outlined among other points that this technology 'is boundless and transboundary' and that in this respect 'data processing has gone global'.[45] One can question this assessment. The data transfers associated with cloud computing involve **multiple locales (data centres) distributed across different jurisdictions and different private handlers**, but they are not, from a technical, legal and political point of view, global. Under present conditions, it is ultimately impossible for cloud computing users to know exactly "where" their data is being held. From this point of view, then, cloud computing is bound insofar as the data processing operations it involves take place **across different sovereign jurisdictions** (see section 4.2), and bound again by the relations it entails between a range of public and private authorities.

The most obvious of these relations is regulation, whereby public authorities establish rules regarding the conduct of private entities in the provision of cloud-based services to private citizens and companies. As recent discussions within the EU exemplify, private authorities are intimately tied with the process of developing public regulations regarding cloud computing. In November 2011 for instance, a group of industry representatives forwarded

[45] International Working Group on Data Protection in Telecommunications, *Working Paper on Cloud Computing – Privacy and Data Protection issues – "Sopot Memorandum*, 675.44.8, Sopot, 24.3.2012.

their recommendations on a 'European cloud computing strategy' to Vice-President of the European Commission Neelie Kroes, outlining their views on the various challenges raised by cloud computing, including on issues of privacy, trust and security[46].

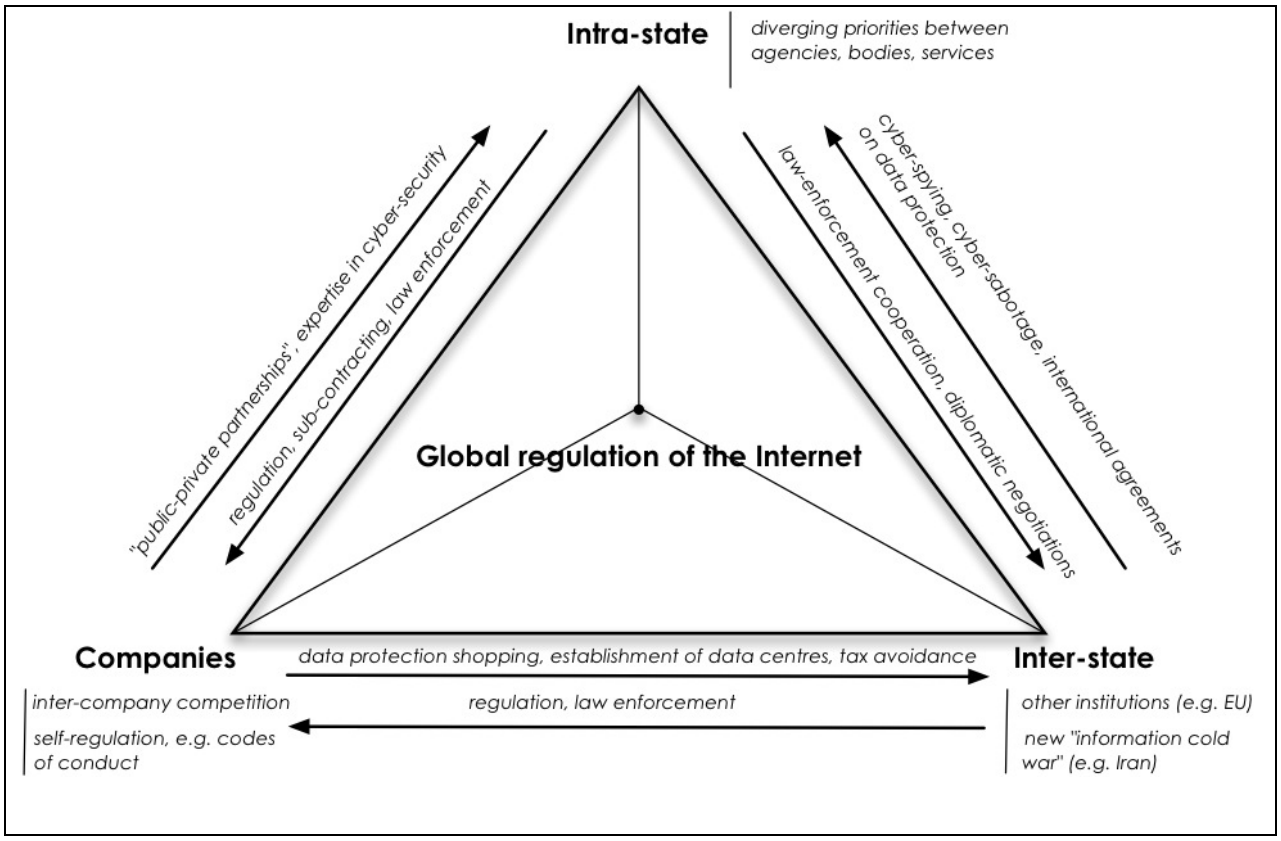
In the meantime, cloud-computing infrastructure is today almost exclusively owned by companies. The cloud services provided by well-known US based company Amazon (under the label Amazon Web Services, EWS), for instance, is presumed to account for 1% of all Internet consumer traffic[47]. With the current economic and financial crisis bringing budgetary control into the spotlight, furthermore, public authorities have tended to opt for outsourcing cloud computing to private entities, sometimes to the detriment of other initiatives. A good example is the June 2012 decision by US space agency NASA to shift part of its infrastructure to the aforementioned Amazon EWS to the detriment of its efforts in the development of open-source cloud platform OpenStack, an initiative it had founded with company Rackspace Hosting[48]. Another aspect of the relations through which cloud computing is bound, then, is the relation of the "public-private partnership" kind between state authorities and companies. Also involved here is the commercial competition between different cloud providers.

A third set of relations at stake in cloud computing lies with the inter-state/international system, which involves transnational bodies such as the European Union itself, but also conflicts between states. Over the past couple of years, high profile developments such as the discovery of the Stuxnet, and more recently Flame cyber-attacks have emphasised the risks associated with inter-state conflicts throughout our "information societies". By the same token, the so-called "Megaupload" case reflects another aspect of inter-state relations, in this case law-enforcement cooperation, but also the legal problems associated with this kind of activities.

The set of relations currently defining cloud computing therefore encompasses negotiations and tensions between public authorities (on the regulation of cloud computing, but also on its use by administrations), between private entities (as they compete for providing cloud-based services, or contract each other in this regard), and between public and private authorities. To characterise these relations, we draw from the model developed by political economist Susan Strange in an effort to understand the redefinition of relations between transnational corporations and governmental authorities in the context of globalization, which she coined as 'triangular diplomacy'[49]. Figure 2 below adapts Strange's argument to the question of cloud computing. It outlines the predominant argument in discussions of this issue, which relates cloud computing to the question of the global regulation of the Internet.

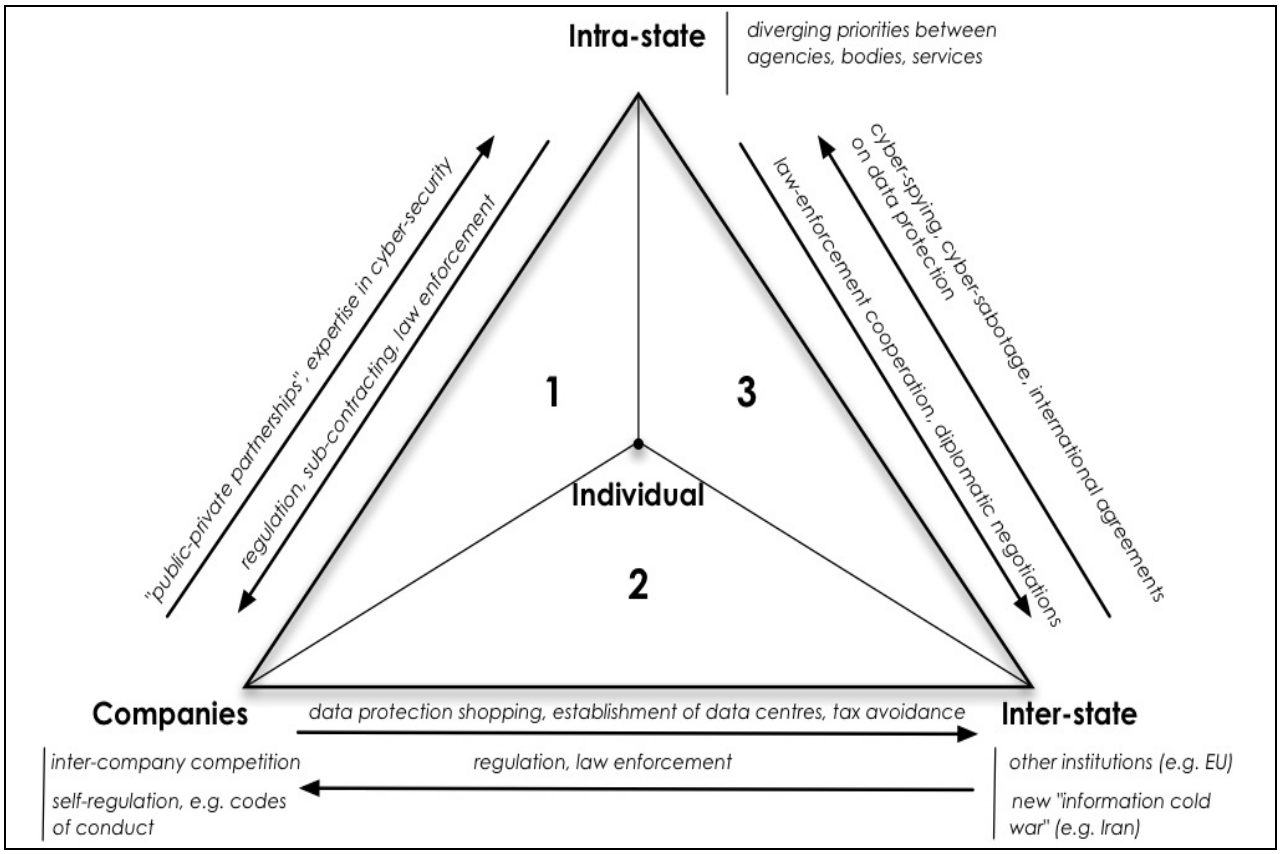
[46] E. Sweeney (rapporteur), *Industry Recommendations to Vice President Neelie Kroes on the Orientation of a European Cloud Computing Strategy*, Brussels, 11.2011.
[47] Based on estimates by US-based start-up Deepfield, see: Labovitz, C., op.cit.
[48] See the announcement by NASA Chief Information Officer Linda Cureton, op.cit.
[49] Strange, S. (1992), 'States, Firms and Diplomacy', *International Affairs*, 68(1): 1-15.

Figure 2: The triangular diplomacy of cloud computing from the point of view of the global regulation of the Internet



With regard to cybercrime, predominant concerns related to cloud computing **involve the establishment of rules allowing for the association between persons and specific IP addresses**. This includes the avoidance of developments stemming both from relations between states and companies and states and the inter-state system that would result in the development of regional Internets undermining interoperability. What is lost in the process, however, is the issue of the protection of the individual, which is as argued previously identified as the most central risk in relation to cloud computing. Figure 2 raises a different set of questions if instead of the global regulation of the Internet, one places the individual at the core of policy concerns, as displayed in Figure 3 below.

Figure 3: The triangular diplomacy of cloud computing from the point of view of the individual



Triangular diplomacy functions across the various policy domains involving cloud computing, including law-enforcement. In this area, one concern widely echoed in specialised news outlet over the past months is the fact that the largest providers of cloud services are legally or physically located in the US, which makes the data processed through their cloud liable to interception and seizure by US authorities. While cloud computing has made data processing global, as argued by the Sopot Memorandum, it is important to reiterate that **jurisdiction still matters** (see section 4.2). **Where the infrastructure underpinning cloud computing (i.e. data centres) is located, and the legal framework that cloud service providers are subject to are key issues**, especially in a law-enforcement context where challenges to the right to data protection and to privacy are particularly stringent. These concerns have been dealt with as a business opportunity for some EU-based companies, which have advertised their services as safe from any interception on the basis of the US PATRIOT Act[50], and as a potential liability which has seen other companies turning down cloud-based services from US providers – such as UK-based defence company BAE Systems' reported decision to abstain from using Microsoft's Office 365 cloud-based software suit in fear of industrial espionage[51].

Figure 2 further highlights that the cybercrime dimension involved in the issue of cloud computing is but one of the pending issues if one places the individual and his rights,

[50] E.g. Baker, J. (2011), 'European cloud vendors cleaning up with data protection fears', *Techworld*, 5.12.2011, available from http://news.techworld.com/security/3322757/europe-cloud-vendors-cleaning-up-with-data-protection-fears/, retrieved 20.8.2012.

[51] Whittaker, Z. (2012), 'Defense giant ditches Microsoft's cloud citing Patriot Act fears', *ZDNet*, available from http://www.zdnet.com/blog/london/defense-giant-ditches-microsofts-cloud-citing-patriot-act-fears/1349, retrieved 20.8.2012.

including the right to data protection and the right to privacy, at the centre of the discussion. **Law-enforcement matters are reflected in this triangular diplomacy, but they are arguably not the most central.** For the individual, surface **1** is the least problematic, it represents the classical configuration in which data protection law has historically developed. With regard to the issue of cybercrime, surface **1** is also where the individual enjoys the best protection and best guarantees in terms of legal certainty and redress. Surface **2** is more problematic, especially in a cloud computing context, because it involves cross-border data transfers. Surface **2** also raises a question on which issue is most central: transnational "cybercrime" or the handling by company of data on a transnational scale. Surface **3** is the most problematic because in the confrontation between states and the inter-state system, especially with regard issues of cyber-espionage and cyber-sabotage, the individual and her rights all but disappear.

Where cloud computing is possibly the most disruptive, then, is not in the new possibilities it offers to criminals and fraudsters, but in the fact that it breaks away from the forty-year-old legal model for international data transfers. This is the issue we will discuss in the remainder of this section by examining successively each tip of the triangular diplomacy system at work in cloud computing.

3.2. The companies/ states/ inter-state relations

The cloud is first a field of competition for private companies. Major IT companies are advertising cloud computing with unprecedented urgency, because they fear that their customers could switch to competitors' platforms offering irresistible cost-savings[52], thus destroying long-held business franchises. The market for cloud services is heavily subcontracted, both for the physical infrastructure comprising data centres as well as the "stacks" (layering of levels) of software that provide the functional elements compromising the totality of the service. Both software and hardware have to be maintained, and these are governed by "service level agreement" (SLA) contracts which guarantee overall levels of performance, reliability, and security. There is intense price-driven competition, and providers will arrange for reserve capacity with diverse subcontractors to cope with anticipated variations in demand. Advanced forms of cloud computing, but also costs in non-standard PaaS, may also create powerful "lock-in" effects, which lead to strategic games between industry, regulators and standards bodies. Given the complexity of these relationships, the **policy discussions of cloud computing have become very confused by the term being informally applied to almost any Internet service offering some combination of communications and remote storage of data provided by an intermediary**.

Even though the marketing deployed around cloud technologies have blurred what is really new in these technologies, two new features can be underlined: data-at-rest are becoming vulnerable and massively-parallel computation are becoming a commodity, and this will have profoundly disruptive policy implications for privacy, security and data sovereignty. **The main challenge in this companies/ companies relationship is the rights of individuals whose data is being processed.** These rights are indeed subsumed into a complex mesh of contracts that are primarily concerned with abstracting the details of where and how processing actually takes place, in the interest of economic efficiency. The legal section 4.3 details further the aspect of legal responsibilities.

In any case a data controller, defined as the organisation(s) which determine the "means

[52] Up to 90% savings compared to "on-premise" computing according to industry figures.

and purposes" of processing, must make a contract to specify the conduct required of any Processor employed to perform limited operations on behalf of the controller. A critical question therefore is **which kinds of cloud provider qualify as controllers or processors**. The challenge of legal definitions of both is detailed further in the section 4.3. In general, PaaS and IaaS providers know nothing about the function of the programs run or meaning of the data processed by their commercial customers, and will have no relationship with the individuals whose data is processed. Therefore the customer will be the controller and must ensure their contract with the cloud provider guarantees effective protection for the individuals whose data is processed.

However SaaS is normally restricted to authorised users through some form of identity management system, which requires autonomous operational decisions by the provider (for example if a user requests a reset of their password, an immediate security assessment must be made whether this is an attempt to break into the system). SaaS providers are therefore likely to be deemed joint controllers together with the customer organization. The main question that arises then is: if there are joint controllers, what form of contract should govern that relationship? The EU DP Directive of 1995 did not really foresee this situation. cloud computing is dominated by US companies, many of whom presumed that Safe Harbour self-certification would relieve them of the obligation to agree contracts with their customers. However as we have seen, PaaS and IaaS are intrinsically Processor roles which cannot fulfill any of the privacy principles on which Safe Harbour is founded. This was never satisfactorily resolved[53] by the Commission before the agreement was hastily concluded over the objections of European DPAs[54]. As a result many US cloud providers advertise Safe Harbour certification with insupportable claims that this legalizes transfers of EU data into US clouds, and since 2009 several have altered their self-certification filings to claim the oxymoronic status of Safe-Harbour-as-a-Processor. The Article 29 Data Protection Working Party (WP29) have clarified that this is insufficient their recent opinion[55].

The concepts of controller and processor are thus subject to contested interpretation, and this was true even before the advent of cloud computing[56]. The legal definitional challenges of these interpretations are analysed in depth in section 4.

3.3. The states/ inter-state/ companies relations

In the field of cybercrime, the challenge of privacy in a cloud context highlighted above is also underestimated, if not ignored. What is at stake here is the second 'segment' of triangular diplomacy, i.e. the states/companies relationship and how they unfold with respect to the question of data protection. In *fora* such as the Council of Europe "Octopus" Cybercrime conferences for instance, Data Protection laws appear to be very marginal in the agenda set priorities, and inadequately addressed to meet the challenges.

In 2007, the Council of Europe - under the Project on Cybercrime - set up a working group with representatives from law enforcement, industry and service provider associations that prepared draft guidelines which were adopted by the global Octopus Interface conference in Strasbourg in April 2008. The European Union's Justice and Home Affairs Council

[53] There is no support in EU materials for the substance of US Department of Commerce Safe Harbour FAQ 10.

[54] "Having examined the new version of the documents received on 28 April and 2 May, the Working Party confirms its previous Opinions and considers it essential that the following issues and recommendations be given due consideration." See Article 29 Data Protection Working Party (WP29) (2000), Opinion on the level of protection provided by the "Safe Harbour Principles", 2000.

[55] Article 29 Data Protection Working Party (WP29) (2012), Opinion 196 on Cloud Computing, July 2012.

[56] Article 29 Data Protection Working Party (WP29) (2010(c)), Opinion 169 on the concepts of "controller" and "processor", February 2010.

recommended in November 2008[57] that the European Commission work on the basis of the guidelines adopted by the Council of Europe conference and took note of eight specific recommendations.

Allegedly, the question of the protection of fundamental rights and the role of the Internet industry in this respect is being addressed by a number of initiatives, such as the Global Network Initiative - Protecting and advancing Freedom of Expression and Privacy in Information and Communications technologies[58]. This initiative establishes principles on Freedom of Expression and Privacy and has been developed by companies, investors, civil society organizations and academics[59]. **A careful analysis of these initiatives however shows a worrying lack of clarity in definitions used, and cannot be considered as adequate tools to meet the challenges**. Despite welcoming attempts to clarify the issues at stake[60], the question of Law enforcement/Internet service provider cooperation in the investigation of cybercrime is still critical. In a European context, the newly created cybercrime centre raises concern: if the Centre is intended to fuse information from open sources, private industry, police and academia, and is intended to serve as a platform for European cybercrime investigators, what legal framework are in place to deal with privacy and data protection in relation to cloud computing? The potential for misuses and abuses by law enforcement actors and agencies becomes an issue of serious concern, and this critical challenge is addressed in section 4.4.

The question of privacy and data protection is furthermore challenged by exceptional measures taken in the name of security and the fight against terrorism. The US context is here particularly highlighting, both in the case of the Patriot Act and in the case of the US Foreign Intelligence Surveillance Amendment Act of 2008. These examples illustrate conflicts that can arise in the state/companies relationships. The major Cloud providers are transnational companies subject to conflicts of international public law. Which law they choose to obey will be governed by the penalties applicable and exigencies of the situation, and in practice the predominant allegiances of the company management. So far, almost all the attention on such conflicts has been focussed on the US PATRIOT Act, but there has been virtually no discussion of the implications of the US Foreign Intelligence Surveillance Amendment Act of 2008. §1881a of FISAA for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, which applies to Cloud computing. Although all of the constituent definitions had been defined in earlier statutes, the conjunction of all of these elements was new.

The law was passed in the aftermath of allegations of "warrantless wiretapping" affecting US citizens after the attacks of 9/11. Accounts emerged in the US media in 2005 that surveillance of Internet and telephone communications had been conducted in violation of strict constitutional and statutory protections afforded to US citizens (and legal residents). In response to mounting public concern, in 2007 Congress enacted the Protect America Act as a temporary measure, which aimed to legalize whatever surveillance activities were still being conducted, and to grant retroactive immunity to telecommunications companies implicated (who would otherwise have been liable for heavy damages for their complicity).

[57] See Council of the EU, *Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime*, Brussels, 27-28 November 2008, available at: http://www.eu2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf

[58] See Global Network Initiative website, available at: http://globalnetworkinitiative.org/principles/index.php

[59] Participants are listed on the GNI website through the following link: http://globalnetworkinitiative.org/participants/index.php

[60] See for instance: van Genderen, R., (2008), *Cybercrime investigation and the protection of personal data and privacy*, Discussion paper, Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, France, 25 March 2008.

There followed a test case at the Foreign Intelligence Surveillance Court of Review, which held definitively that the Fourth Amendment requirement for a specific warrant only applied to surveillance directed at US persons[61]. This opened the door for Congress to enact FISAA §1881a in 2008, which authorized mass-surveillance of foreigners (outside US territory), but whose data was within range of US jurisdiction. However, the most significant change escaped any comment or public debate altogether. **The scope of surveillance was extended beyond interception of communications, to include any data in public cloud computing as well.** This change occurred merely by incorporating "remote computing services" into the definition of an "electronic communication service provider"[62].

3.4. The inter-state/ states/ companies relation

The scope of surveillance acted in the above described FISAA, and the fact that it has been extended beyond interception of communications to include any data in public cloud computing as well, has very **strong implications on EU data sovereignty and the protection of its citizens' rights**. The implications for EU Fundamental Rights flow from the definition of "foreign intelligence information", which includes *information with respect to a foreign-based political organization or foreign territory that relates to the conduct of the foreign affairs of the United States*[63]. **In other words, it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US Clouds**.

This represents a sea change from the concerns expressed in 2001 by the European Parliament over the "ECHELON" system of strategic communications surveillance[64]. Following concerns about "cookie hijacking" attacks on web browsers using wireless connections, most popular US based web sites now encrypt communications in transit, and so would not be (directly[65]) vulnerable to interception. But FISAAA 1881a means that any data-at-rest formerly processed "on premise" within the EU, which becomes migrated into Clouds, becomes liable to mass-surveillance – for purposes of furthering the foreign affairs of the US (as well as the expected purposes of terrorism, money-laundering etc.).

As a consequence, **FISAA §1881a can be seen as a categorically much graver risk to EU data sovereignty than other laws hitherto considered by EU policy-makers**:

- new NSA data centres constructed for storage and analysis on an unprecedented scale[66]
- the extension of scope from communications-in-transit to include data inside US Clouds[67]
- whistleblower reports of the sophistication of data analysis contemplated[68]
- the express targeting of foreign data without safeguards applicable to US citizens[69]

[61] See: www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.
[62] See: §1880 the provision "to the public of computer storage or processing services by means of an electronic communications system".
[63] By truncating and substituting limbs of clauses §1801e and §1801a.
[64] European Parliament (2001), *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, PE 305.391 A5-0264/2001.
[65] See: http://paranoia.dubfire.net/2011_09_01_archive.html
[66] Wired Magazine, The NSA Is Building the Country's Biggest Spy Center, 1th March 2012, available at: http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/
[67] See: 18 USC § 2711(2) t*he term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system*.
[68] W. Binney's Keynote at HOPE 9 conference (New York City, 13th July 2012, 1hr 12m, available at: http://www.youtube.lu/watch?v=hqN59beaFMI.

- a doctrine of indiscriminate *collection,* which only seeks to control subsequent *access*[70]

Remarkably, **it does not appear that the EU Commission, national DPAs, or the European Parliament had any awareness of FISAAA 1881a until mid-2011**. Most attention continues to be focussed on the US Patriot Act of 2001, which certainly contains powers for direct access to EU data, but nothing like 1881a's heavy-calibre mass-surveillance fire-power aimed at the Cloud. A few EP questions have now been asked and in February 2012 Commissioner Reding speculated that any such conflicts of law arising might have to be settled at the International Court of the Hague[71] (although the US does not recognize its jurisdiction).

The root problem is that cloud computing breaks the forty year old legal model for international data transfers[72]. The primary *desideratum* would be a comprehensive international treaty guaranteeing full reciprocity of rights, but otherwise exceptions ("derogations") can be recognized in particular circumstances providing there are safeguards appropriate to the specific situation. Cloud computing breaks the golden rule that "the exception must not become the rule". Once data is transferred into a Cloud, sovereignty is surrendered. In summary, it is hard to avoid the conclusion that **the EU is not addressing properly an irrevocable loss of data sovereignty, and allowing errors made during the Safe Harbour negotiations of 2000 to be consolidated, not corrected**.

4. CLOUD COMPUTING AND CYBERCRIME: LEGAL CHALLENGES FOR DATA PROTECTION LAW

KEY FINDINGS

- Conceptual uncertainties emerge in relation to the wide room of discretion by the Member States at times of establishing jurisdiction i.e. the applicable implementing law of the Member State under the DPD. This most directly causes uncertainty for any affected individual who might face conflict of laws resulting from the multiple national implementing legislations. A targeting/directing test would establish jurisdiction in relation to data connected to the EU, but would not rule out conflict of laws nor preclude secret surveillance by third countries. Yet, these initiatives should be seen as valuable tool to ensure that US companies are "in principle" covered by EU DP Law.

- An 'accountability approach' would imply the vesting of obligations and liabilities upon every actor with considerable power, i.e. knowledge and control of the personal data. This explains why anonymous data, i.e. data to which there is a minimized risk of unauthorized access, are no 'personal data' in the DPD. Standard setting on the EU level as regards what constitutes personal data would contribute to a harmonized approach to the "who" question (see Annex 2), i.e. who is the cloud

[69] FISCR 22nd August 2008 judgement on Protect America 2007, available at: www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.

[70] "Before the enactment of the FAA... in effect, the Intelligence Community treated non-U.S. persons located overseas like persons in the United States, even though foreigners outside the United States generally are not entitled to the protections of the Fourth Amendment", *Background Paper on Title VII of FISA Prepared by the DoJ and ODN, Feb 2012*, available at: www.fas.org/irp/news/2012/02/dni020812.pdf

[71] See: http://news.bbc.co.uk/democracylive/hi/europe/newsid_9695000/9695923.stm

[72] Hondius, F., (1975), *Emerging Data Protection in Europe*, North-Holland/American Elsevier.

user data (joint) controller, data processor, data subject. This "who" question is important in light of the question of jurisdiction and the resulting or potential responsibilities, liabilities and obligations towards the individual.

- Definitional uncertainties also emerge in relation to self-regulatory data protection regimes 'quite separate from the wider EU level framework on data protection', when assessing data transfers to third countries. The notion of 'adequacy' as regards data transfers to third countries is defined on several levels (Member States, EC and EUROPOL), and this further expands the vulnerability of the data subject as regards what actually are 'adequate data protection standards', and the capacity to control her/his data as a fundamental right. This is exacerbated by the lack of a concept of cybercrime within the EU, which creates even more legal uncertainty for the individual as regards the justification of lower data protection standards for cybercrime.

As underlined above, cloud computing raises several challenges related to legal uncertainty about fundamental legal concepts and general principles in the current multiple, fragmented and incomplete EU data protection legislative framework. A key guiding question is the extent to which the Union's legislative regime is well-equipped to deal with the data protection challenges posed at the intersection of cloud computing and crime prevention/fighting. Although the Treaty of Lisbon formally abolished the distinction between the First and Third Pillars (this last one corresponding to Police and Judicial Cooperation in Criminal Matters),[73] the existing EU legal complex still remains 'pillarised' in nature and guided by this old division. The Data Protection Directive (DPD)[74] and the Proposal for a General Data Protection Regulation (PGDPR)[75] do not apply to law enforcement activities,[76] nor to domestic processing, which is still governed by various national regulatory systems in the different areas of law touched by cloud computing (i.e. civil law, administrative and commercial law). Furthermore, old third pillar instruments such as the Framework Decision (DPFD)[77] and the Proposal for a Police and Criminal Justice Data Protection Directive (PPCJDD)[78] do not apply to 'cloud computing providers' and to EU Home Affairs Agencies such as EUROPOL[79].

[73] The first and third pillar respectively correspond to title IV of the Treaty establishing the European Community ('Visas, Asylum, Immigration and Other Policies related to the Free Movement of Persons') and title VI of the Treaty on European Union ('Provisions on Police and Judicial Cooperation in Criminal Matters').

[74] European Parliament and Council of the European Union (1995), *Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995.

[75] European Commission (2012(b)), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels, 25.01.2012.

[76] Other relevant first pillar instruments for cloud computing are the e-Privacy Directive and the Data Retention Directive: European Parliament and Council of the European Union (2002), *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),* OJ L 201, 31.7.2002*;* European Parliament and Council of the European Union (2006), *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,* OJ L 105, 13.44.2006. Whereas the e-privacy Directive applies to public communications services (Recital 10 and Article 3.1), the DPD applies to non-public communications services.

[77] Council of the EU (2008(a)), *Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,* OJ L 350, 30.12.2008.

[78] European Commission (2012(c)), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes*

4.1. Definitional dilemma in the EU data protection legal framework

The EU data protection legal framework is affected by important definitional dilemmas. First, **conceptual uncertainties in the context of the old First Pillar relate to the wide room of discretion by the Member States at times of establishing jurisdiction i.e. the applicable implementing law of the Member State under the DPD**. This most directly causes uncertainty for any affected individual who might face conflict of laws resulting from the multiple national implementing legislations. This touches most directly upon the relationship 'company-company' in our 'triangular diplomacy' conceptual framework, as the applicable substantive law determines both the obligations of data controllers and processors and the rights and level of protection of the individual as 'data subject' or 'consumer'.

Secondly, **definitional uncertainties also emerge in relation to self-regulatory data protection regimes 'quite separate from the wider EU level framework on data protection',[80] when assessing data transfers to third countries**. This question touches upon the relationship 'state-state' and 'state-company' due to increasing cooperation between the private sector and law enforcement agencies (LEA's), at national and EU levels, in the 'fight against crime' 'in the cloud'. De Hert has stressed that 'it is very likely that data collected by commercial data controllers in the course of their duties are used by law enforcement agencies'[81]. This is indeed likely to be occurring independently of the actual existence of any applicable or common legal framework setting the necessary data standards and regulations framing this relationship and safeguarding the capacity of the individual to control her/his data as a fundamental right. The potential for misuses and abuses by law enforcement actors and agencies becomes henceforth an issue of serious concern. The lack of a concept of cybercrime in EU law raises even more concerns for the individual about the justification for lower data protection standards or the application of exceptions to those[82].

The European Commission has confirmed that 'cloud computing' has caused a loss of control by the individual over her/his data.[83] This Section shows how from a data protection

---

of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.01.2012.

[79] Recital 15 and Article 2.3(b) PPCJDD; EUROPOL is governed by another third pillar instrument: Article 23.2 *Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL) 2009/371/JHA),* OJ L 121, 15.05.2009.

[80] The international agreements are available on: https://www.EUROPOL.europa.eu/content/page/international-relations-31; De Hert, P. and B. de Schutter (2008), 'International Transfers of Data in the Field of JHA: The Lessons of EUROPOL, PRN and Swift', in B. Martenczuk and S. van Thiel (eds.), *Justice, Liberty, Security: New Challenges for EU External Relations*, Brussels: VUBPress, p. 320; De Busser, E. (2012), 'The Adequacy of an U-US Partnership', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Dordrecht/Heidelberg/London/New York: Springer, 2012, p. 191; European Parliament (2011), *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies. Frontex, EUROPOL and the European Asylum Support Office*, PE 453.196, August pp. 28, 73, 69, 74; European Parliament (2011), *Developing an EU Internal Security Strategy, fighting terrorism and organised crime*, PE 462.423, November, p. 49.

[81] De Hert, P. and V. Papakonstantinou (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, No. 6, February/March, p. 2.

[82] Without, however, violating the core-periphery of human rights: Porcedda, M.G., *Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?*, EUI Working Paper, Law, p. 7.

[83] European Commission (2010(c)), *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 4.11.2010, pp. 2, 11; European Commission (2012(a)), *Data protection reform: Frequently asked questions*, MEMO/12/41, Brussels, 25.01.2012.

viewpoint, **cloud computing has fundamentally transformed the individual, located in the centre of the** 'triangular diplomacy' conceptual framework (cf figure 2), from a '**data subject' or 'consumer' to a product or commodity in relation with the private sector and law enforcement** within the Member States, the EU, and beyond. **At this stage there is not really any possibility for DPAs to guarantee the conformity of data processing "in the cloud" with EU DP law.** Harmonization of key fundamental legal concepts at Union levels could be a welcome step forward if guided by the accountability principle, transparency[84], ownership and integrity of data, with a view to respect the right to data protection (Article 16.1 Treaty on the Functioning of the EU and Article 8 EU Charter of Fundamental Rights). The data subject 'should thus be at the heart of policy attention'[85], and full transparency would be central as regards basic fundamental legal concepts such as jurisdiction, data processor/data controller, transfers of data and cybercrime, as well as the implications of EU level law enforcement agencies activities such as EUROPOL, which we now enter into analysing.

4.2. The challenge of jurisdiction

The first legal challenge laying at the intersection between cloud computing and crime fighting is that of jurisdiction. This concept determines both the responsibilities and legal liabilities of data controllers and processors and the rights of the individual as 'data subject'. As said above, data processing operations take place **across different sovereign jurisdictions**, and the market for Cloud services is heavily subcontracted for the physical infrastructure comprising datacentres. The DPD contains two main jurisdictional grounds: Article 4§1 DPD, based on the establishment of an 'EU controller' or the EU equipment of a 'non-EU controller', and Article 17.3 DPD, based on the establishment of an 'EU processor'[86]. The key challenge under both grounds is how to distinguish the relationships data processor/controller and establishment/equipment in cloud computing? Such definitional uncertainty brings the individual in a vulnerable position with regard to the applicable national law. The PGDPR has replaced the latter distinction by a 'targeting test' to establish jurisdiction on the basis of data connected to the EU. Yet, definitional uncertainty still remains, and conflicts of laws would not be ruled out[87].

[84] Article 29 Data Protection Working Party (2010(a)), *Opinion 3/2010 on the principle of accountability*, 00062/10/EN WP 173, Brussels, 13.07.2010; European Parliament (2011(b)), *Towards a New EU Legal Framework for Data Protection and Privacy*, Committee on Civil Liberties, Justice and Home Affairs, PE 453.216, September, pp. 21-22; Article 29 Data Protection Working Party (WP29) (2010(b)), *Opinion 8/2010 on applicable law*, 0836 02/10/EN WP 179, Brussels, 16.12.2010, p. 29.

[85] European Parliament (2011(b)), pp. 10, 11.

[86] See also Article 30 and Recital 66 Draft Regulation.

[87] ''Main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union.'; Hon, W.K., J. Hörnle and C. Millard, 2011, p. 12.

According to Article 4§1 DPD,[88] jurisdiction is established independently of the physical location of the data, or the citizenship or residence of the data subject.[89] Instead, it should, firstly, be verified whether an 'EU cloud user' is a data controller in his own right, or in relation to a non-EU controller, whether the EU cloud user is an establishment within the meaning of Article 4.1(a) DPD, or equipment within the meaning of Article 4.1(c) DP (in case the non-EU controller installs cookies on installations of the user) – *the establishment/equipment test*[90]. Following a negative answer to both questions, it must be verified whether the non-EU controller has an EU data centre. An first question is whether space rented by a non-EU provider in an EU data centre also constitutes 'establishment'[91].

The next question is whether the EU data centre is processing 'within the context of its activities'. In that case, that establishment can be considered a (relevant) establishment under Article 4.1(a) DPD. The WP29 proposed that 'in the context of the activities of an establishment of the controller' includes both processing activities and other activities (such as marketing)[92]. If, on the other hand, the EU data centre is processing within the context of the non-EU controllers' activities, a distinction should be made between whether or not the non-EU controller owns an 'EU data centre'. Following a positive answer, the EU data centre (often IaaS and PaaS providers) can be considered as equipment (or an irrelevant establishment) under Article 4.1(c) DPD[93]. In those cases where the EU data centre is a mere subsidiary (often SaaS providers) of the non-EU controller, the EU data centre can also be considered as both equipment under Article 4.1(a) DPD. Yet, looking through the corporate veil can show that such processors are controllers in their own right.

[88] '1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.'

[89] Hon, W.K., C. Millard and I. Walden (2011 (b)), *Who is responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2*, Queen Mary School of Law Legal Studies Research Paper No. 77/2011, March, p. 7; Yet, under Article 4.1(c), the location of equipment or means of processing could overlap with the location of processing.

[90] Article 29 Data Protection Working Party (WP29) (2008), *Opinion 1/2008 on data protection issues related to search engines*, 00737/EN WP 148, Brussels, 04.04.2008, pp. 10, 11; Article 29 Data Protection Working Party (WP29) (2009(b)), *Opinion 5/2009 on online social networking*, 01189/09/EN WP 163, Brussels, 12.06.2009, p. 5; Article 29 Data Protection Working Party (2010 (b)), *Opinion 8/2010 on applicable law*, 0836 02/10/EN WP 179, Brussels, 16.12.2010, pp. 21, 22.

[91] Hon, W.K., J. Hörnle and C. Millard (2011), "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3", Queen Mary School of Law Legal Studies Research Paper No. 84/2011, February, p. 18.

[92] Article 29 Data Protection Working Party (WP29) (2008), p. 10; This stance has been criticized: Hon, W.K., J. Hörnle and C. Millard 2011, p. 10.

[93] Article 29 Data Protection Working Party (WP29) (2010(b)), p. 19; The definitions 'relevant' and 'irrelevant' establishment were introduced by the WP29 because the wording of Article 4.1(c) DPD applies that article only when 'the controller is not established on Community territory'. As seen above, a controller can be established on Community territory but without processing personal data in the context of that establishment's activities, so that Article 4.1(a) does not apply. Yet, in that case Article 4.1(c) DPD can also not apply as the controller is established on Community territory'. It has therefore been suggested that the article should be read as 'the controller does not have any establishment on the territory of a Member State in the context of which it processes personal data'. For the same reason, Article 3.2 Draft Regulation (see below) should arguably be modified. There is however no similar loophole for processors which. Article 3.1 of the Regulation applies the Regulation if a provider processes personal data in the context of the activities of an establishment of a provider in the Union, which seems to imply that the processor would be 'subject to the draft Regulation in relation to its worldwide activities'.: Hon, W.K., J. Hörnle and C. Millard, 2011, pp. 20, 32, 37, 38.

Within a Cloud Legal Project (CLP), it has been proposed to abolish the rigid 'establishment/equipment test' in favor of a targeting/directing test in relation to data connected to the EU[94]. The WP29 has confirmed this position: 'Article 4(1)c strives to ensure the right to the protection of personal data provided by the EU Directive even where the controller is not established in EU/EU territory but where the processing is in some way connected with the EU.[95]' The protection of individuals inside the EU is also one of the main purposes of Article 4.1(c) DPD[96], and therefore, Kuner argued to make this idea explicit by focusing on 'the application of EU law to situations in which the data controller determines in an untransparent way how data are processed on the individual's computer'.

A targeting test denotes an accountability approach that would solve key questions about applicable law, as mapped by the EC and the EP: '[..] in case where the relevant place of establishment of a cloud provider may be hard to determine, e.g. for a non-EU user of a non-EU provider operating equipment in the EU;'[97] 'In terms of *applicability of the law*, there is a clear gap when both the provider and its equipment (data centres, servers, etc.) are located outside the EU but the service is used by EU citizens [..].[98]' Article 3.2 PGDPR introduces a targeting test, and applies the Regulation 'to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour'. A similar proposal was made by Spoenle within the COE's discussions to extend the jurisdictional scope of Article 32(b) Cybercrime Convention:[99] the power of disposal as a legal connecting factor detached from location parameter would connect any data to the person that hold the right to 'alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever'[100]. However, such initiatives won't rule out conflict of laws and a targeting test cannot preclude secret surveillance by third countries. These initiatives should be seen as valuable tool to ensure that US companies are "in principle" covered by EU DP Law.

4.3. The challenge of responsibility: data controller, data processor and personal data

The distinctions between cloud user, data processor, data (joint) controller[101] and data subject are further blurred by cloud computing[102]. This "who" question (see Annex 2) is

[94] Hon, W.K., J. Hörnle and C. Millard, 2011, pp. 34-37.
[95] Article 29 Data Protection Working Party (WP29) (2010(b)), p. 29.
[96] Article 29 Data Protection Working Party (WP29) (2002), *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, 5035/01/EN/Final WP 56, Brussels, 30.04.2002, p. 7.
[97] European Commission (2012(e)), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions*: *Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 /2, Brussels, 27.09.2012, p. 8.
[98] European Parliament (2012(a)), *Cloud Computing*, Policy Department Economic and Scientific Policy, PE 475.104, May, p. 59.
[99] Council of Europe (2001), *Convention on Cybercrime*, Budapest, 23.11.2001: 'Article 32 – Trans-border access to stored computer data with consent or where publicly available: A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'
[100] Council of Europe (2010 (b)), *Cloud Computing and cybercrime investigations: Territoriality vs. The power of disposal*, discussion paper, prepared by J. Spoenle, 31.08.2010, p. 10.
[101] Council of Europe (2010 (a)), *Cloud computing and its implications on data protection*, discussion paper, March, prepared by Research Centre on IT and Law (CRID), p. 16; Article 24 Draft Regulation introduced the concept of joint controllers.

important in light of the question of jurisdiction and the resulting or potential responsibilities, liabilities and obligations towards the individual. It is important that the individual has legal certainty and keeps the ownership over her/his data, and this explains the importance of his/her consent with the allocation of responsibilities. De Hert defended to boldly abolish the notion of data processors from the new Regulation and 'vest the data controller title, rights and obligations upon any one processing personal information, regardless of its means, conditions or purposes[103]. Likewise, the CLP proposed to abandon the binary distinction between controller and processor in a cloud computing context[104]. The COE's 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' does not even distinguish between these categories[105]. The WP29 stated that it is important to soundly read the contract that can give indications for the power relationships between parties[106]. With regard to joint-controllers, it is questioned what form of contract should govern that relationship?

An 'accountability approach' would then imply the vesting of obligations and liabilities upon every actor with considerable power, i.e. knowledge and control of the personal data. This explains why anonymous data, i.e. data to which there is a minimized risk of unauthorized access, are no 'personal data' in the DPD (Recital 26 DPD)[107]. The relation between the definition of anonymous data and the definition of data controller/processor is also apparent in a recent study of the European Parliament (EP) that successively identifies the definition of data controller and data processor, ownership and confidentiality as outstanding regulatory issues[108].

A first question is whether the process of anonymisation of data is 'data processing' covered by the DPD. Secondly, the definition of 'anonymous data' is in itself an open debate. Information to which there is only a remote, highly theoretical risk of identification, due to sufficient protection measures against unauthorized access, is arguably not considered as personal data[109]. The WP29's focus on preventing identification has, therefore, been questioned in favor of an assessment of the risks to individuals' privacy. The CLP finds that information temporarily exposed unencrypted due to transient processing operations, or law enforcement access, could arguably still be considered as

[102] Article 29 Data Protection Working Party (WP29) (2009(a)), *The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 02356/09/EN WP 168, 01.12.2009, p. 12.

[103] De Hert, P. and V. Papakonstantinou (2012), op.cit., *Computer Law & Security Review*, Vol. 28, No. 2, April, p. 134.

[104] Hon, W.K., C. Millard and I. Walden, 2011 (b), op.cit., p. 24.

[105] Council of Europe (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' does not make a distinction between data controller and data processor*, Strasbourg, 21.1.1981.

[106] Article 29 Data Protection Working Party (WP29) (2010 (c)), *Opinion 1/2010 on the concepts of 'controller' and 'processor'*, 00264/10/EN WP 169, Brussels, 16.02.2010, p. 9: 'The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is [...].'

[107] The DPD does also not apply to individuals who upload data for purely personal purposes or in the course of a household activity, to legal persons and trade secrets. Yet, legal persons are protected under the privacy and electronic communications Directive (Article 1.2); Council of Europe (2010(a)), p. 14; Poulet, Y. et al. (2011), "Data Protection in the Clouds", in. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht/Heidelberg/London/New York: Springer, 2011, p. 388; Compare with the U.S. where 'there is something like privacy of a legal person': Ruiter, J. and W. Martijn, "Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice", in S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht/Heidelberg/London/New York: Springer, 2011, pp. 361-376.

[108] European Parliament (2011(d)), *Does it help or hinder? Promotion of Innovation on the Internet and Citizen's Right to Privacy*, PE 464.462, December, pp. 84-85.

[109] Hon, W.K., C. Millard and I. Walden (2011 (a)), "The Problem of 'Personal Data' in Cloud Computing – What information is Regulated? The Cloud of Unknowing, Part 1", Queen Mary School of Law Legal Studies Research Paper No. 75/2011, March, pp. 40, 41.

anonymous data[110]. On the other hand, Paul Ohm has warned for the failure of anonymisation as a privacy-protecting tool[111].

There is generally a higher risk of unauthorized data access by certain SaaS providers (such as the usual social networking sites) than by IaaS or PaaS providers as supposedly pure infrastructure providers or neutral intermediaries that host data without any knowledge of the 'personal data' nature of the data[112]. Sartor deems such providers not to be 'data controllers'[113], and according to the CLP they are not even 'data processors', present reasonable protection measures, and absent any line-crossing behaviour following which they would become data controllers[114]. The WP29 stressed that '[s]hould processors [...] communicate them in a way that breaches the contract, they shall also be considered to be controllers [...]'[115]. The European Data Protection Supervisor (EDPS) has stressed that the 'role played by cloud providers will need to be determined on a case by case basis [..].'[116] A recent EP study has additionally stressed that ([t]here are also ambiguities as to the role of the cloud computing providers, who – in some cases – can be treated not only as pure data processors, but also as data controllers, given their impact on how the data is being processed 'in the cloud'[117].

The foregoing explains the importance of the adoption of appropriate security standards against unauthorized access, as confirmed by the EC[118]. Standard setting on the EU level would contribute to a harmonized approach to the "who" question, and as such, help to tackle the related jurisdictional issues.

4.4. Data transfers/ processing to third countries

The notion of 'adequacy' as regards data transfers to third countries is defined on several levels (Member States, EC and EUROPOL), and this further expands the vulnerability of the data subject as regards what actually are 'adequate data protection standards'. The focus could be again on 'the minimized risk' of unauthorized access in third countries[119]. Under the DPD and the PGDPR, the Member States have great influence to determine adequacy requirements for data transfers to third countries[120].

---

[110] Hon, W.K., C. Millard and I. Walden, 2011 (a), pp. 27, 28, 33.

[111] Ohm, P., 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *57 UCLA Law Review* 1701 (2010).

[112] Hon, W.K., C. Millard and I. Walden, 2011 (a), pp. 36, 37; Hon, W.K., C. Millard and I. Walden, 2011 (b), pp.1, 18.

[113] Sartor, G. (2012), *Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?*, EUI Working Papers, Law, No. 24, p. 14.

[114] I.e. unless 'they monitor the processing with a view to accessing or using the personal data', or 'giving third parties access to data without authority: Hon, W.K., C. Millard and I. Walden, 2011 (b), pp. 17, 20, 21.

[115] WP29, 2012, op.cit., p. 14.

[116] Hustinx, P. (2010), *Data Protection and Cloud Computing under EU Law*, Third European Cyber Security Awareness Day BSA, European Parliament, 13 April 2010, p. 3.

[117] European Parliament (2012(c)), *Reforming the Data Protection Package*, PE 492.431, September, p. 18.

[118] European Commission (2012(d)), p. 10; European Commission (2010), *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A Digital Agenda for Europe,* COM(2010) 245 final/2, Brussels, 26.8.2010, pp. 23, 24; The EC is currently also consulting on a future EU Network and Information Security legislative initiative, which would introduce the requirement of risk management practices: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/818; Hon, W.K., C. Millard and I. Walden, 2011 (b), p. 22; Kroes, N. (2011), "Towards a European Cloud Computing Strategy", World Economic Forum Davos 27 January 2011, SPEECH/11/50.

[119] Hon, W.K. and C. Millard, 2012, pp. 28, 53, 54.

[120] Article 25.2 DPD and Article 13.4 DPFD define the adequacy of the level of protection afforded by a third country in the light of several circumstances.: '[p]articular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the

Yet, under the PGDPR and PPCJDD the role of the EC would increase through provisions on delegated and implementing acts, respectively relating to the implementation, and the amending, supplementing or deletion of non-essential elements of legally binding acts of the EU[121]. While this would contribute towards 'uniformity' and national alignment with the common regulatory system, such an approach has raised important concerns. The EP would have a limited role in the adoption of an implementing act, and it has therefore questioned the role and level of discretion that the EC would enjoy through delegated acts[122]. The EDPS stressed that vague notions should not justify the adoption of delegated acts as some of them deal with essential elements in the PGDPR[123]. This is for instance the case for instance in relation to those provisions related to what constitutes the threshold for a personal data breach notification (Articles 31 and 32), what constitutes a high degree of specific risks (Article 34.2 and 8), or 'important grounds of public interest' (Article 44.1 and 7).

The EC has repeatedly emphasized the need for improved cross-border cooperation though non-legislative measures and self-regulation[124].

The EU-US Safe Harbour Principles are an example in that regard, which allow transfers to those US organizations (including cloud providers) demonstrating an 'adequate standard of protection'[125]. Yet, **Safe Harbour does not apply to telecommunication common carriers which also provide cloud computing services**. The CLP and the WP29 have emphasized that the controller needs to check the enforcement of Safe Harbour Certification[126]. Besides, the WP29 has stressed that the PGDPR should add that the use of Mutual Legal Assistance Treaties is obligatory with regard to access to personal data for national security and law enforcement purposes, 'in case of disclosures not authorized by Union or Member State Law'[127]. This would imply extending the scope of application of the PGDPR to law enforcement cooperation with the private sector.

The challenge of data transfers and data processing to third countries is of paramount importance. This is even more salient in the context of the US PATRIOT and FISAA described above. There is indeed no indication that the full effects 1881a have on the human rights of EU data subjects have been addressed by WP29 or the Commission. The WP29 for instance only mentions PATRIOT in one footnote[128] in nearly 140 Opinions issued since 9/11.

---

professional rules and security measures'. Yet, according Article 26.2 DPD and Article 13.3(b) DPFD, the Member States can also apply their national adequacy conditions to data transfer to third countries.

[121] Recitals 90, 129 and 130 PGDPR.

[122] Council of Europe (2010(a)), p. 22; Reding, V., "Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing", IAPP Europe Data Protection Congress, Paris, 29.11.2011; European Parliament (2012), *Working Document on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,* PE491.322v01-00, Brussels, 6.7.2012, pp. 2, 4.

[123] European Data Protection Supervisor (EDPS) (2012)*, Opinion of the European Data Protection Supervisor on the data protection reform package*, 7.3.2012, pp. 12-13.

[124] European Commission (2010(b)), *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, COM(2010) 517 final, Brussels, 30.09.2010, pp. 6, 9;

[125] European Commission (2000), *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 2000/520/E, OJ L 215, 25.8.2000.

[126] Hon, W.K. and C. Millard (2012), pp. 41-43, 48; Article 29 Data Protection Working Party, 2012, p. 17.

[127] Article 29 Data Protection Working Party (WP29) (2012(a)), p. 23.

[128] Article 29 Data Protection Working Party (WP29) (2001), 53 Opinion on the need for a balanced approach in the fight against terrorism, Dec 2001.

The WP29 has for instance proposed that "binding corporate rules"- BCR[129] can be adapted to provide adequate safeguards for EU data exported into the Cloud. However, they foresee and permit secret disclosure of data to "third countries". They say:

> In any case, the request for disclosure should be put on hold and the DPA competent for the controller and the lead DPA for the BCR should be clearly informed about it.

The question arises, if the CEO and corporate counsel of a major US Cloud company are faced with a choice between obeying the soft-law exhortations of WP29 which will result in contempt of the FISA Court for breach of secrecy, or not doing what they "should" (and side-stepping huge risks of reputation damage to their business), which law is more likely to be obeyed?

DPA proponents of BCRs-for-processors say they offer theoretically comparable protection to earlier derogation mechanisms (such as standard contract clauses approved by the Commission), but those are equally unsuitable to prevent the use of Cloud data for surveillance purposes. The standard clauses were originally drafted in 2001 for scenarios such as offshore processing of direct-marketing mailing-lists, but when they were revised in 2010[130], they were weakened to accommodate Cloud computing.

The proposed new DP Regulation normalizes the procedure of BCRs-for-processors, and they are no longer regarded technically as a "derogation". However for the same reasons that Safe-Harbour-for-processors is a problematic concept (because a IaaS/PaaS Cloud cannot by definition fulfil any of the SHA Principles) BCRs-for-processors's role should also be questioned. All they can do is pledge to maintain the Cloud datacentres. They can say nothing about the meaning of the data, or the substantive functions at the software level of **personal** data processing.

Both the WP29 and the Commission place great faith in "audit" procedures to ensure Cloud services are compliant, but no commercial audit methodology can seek to uncover secret surveillance which is "lawful" under the national security rubric of a third country (especially if that audit is conducted by a company from that country). There is no way that an EU DPA can know whether this is happening or not, if the Cloud software fabric is designed and controlled from outside EU jurisdiction.

Another challenge are the negotiations by a "High-Level Contact Group" between the EU and US to arrive at an "Umbrella" agreement governing transfers for law enforcement and national security, because the US position would exclude commercial Cloud transfers:

> The US has rejected the idea to apply the agreement also to data transferred from **private parties in the EU to private parties in the US** and subsequently processed for law enforcement purposes by US competent authorities. Both sides agree in substance that the agreement should be without prejudice to the activities in the field of national security, which remains the sole responsibility of Member States[131].

The foregoing shows the lack of an EU legal framework as regards data transfers to third countries. One step forward would be to extend the scope of application of the PGDPR to law enforcement cooperation with the private sector. Secondly, standard setting on the EU

[129] Article 29 Data Protection Working Party (WP29) (2012(b)), 195 Opinion on the BCRs-for-processors, June 2012

[130] By allowing sub-contracting http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF

[131] EU-US Data Protection Non-Paper On Negotiations During 2011, available at: www.statewatch.org/news/2012/feb/eu-council-usa-dp-agreement-2011-5999-12.pdf

level would contribute to a harmonized approach as regards adequate data protection standards for data transfers to third countries.

4.5. The challenge of regulation for EU Home affairs agencies

The legal challenges stemming from the triangular diplomacy context discussed above when applied to the cloud computing-cybercrime fighting framework becomes even more complex when looking at the role of EU Home Affairs Agencies active in law enforcement ('prevention and fight against crime'), such as EUROPOL. EUROPOL is excluded from the scope of the PPCJDD (Recital 15 and Article 2.3(b)) and has developed a system of 'self-regulatory adequacy data protection procedures' in its agreements with third countries such as the US[132].

EUROPOL's core activity is to facilitate the exchange of information between Member States and to develop criminal intelligence. EUROPOL is also mandated to cooperate and engage in information exchange with third parties including other EU agencies, international organisations and third countries, as well as receive information (including personal data) from 'private parties'[133]. EUROPOL is said to have become a 'data controller in its own right'[134]. While awaiting for an EC proposal that is expected to bring the current EUROPOL Decision in line with the Lisbon Treaty, EUROPOL has signalled its intention to establish 'partnerships' with the private sector (non-law enforcement actors)[135]. De Moor and Vermeulen have expressed concerns about this development[136], by stating that

> The nature of information and intelligence from private partners – often collected in a commercial environment for commercial purposes – requires additional safeguards, in order to ensure the accuracy of this information... the development of new partnerships must not occur at the expense of its own law enforcement professionalism.

EUROPOL is entitled to establish an "outreach" to the private sector on the basis of Article 25 of the EUROPOL Convention Decision. The collection of personal data in this context

[132] EUROPOL's exchange of data with third countries and bodies is both underpinned by safeguards contained in the EUROPOL Council Decision, in the implementing rules governing EUROPOL's relations with partners and by the cooperation agreements with third states and bodies which also include safeguards intended to ensure adequate levels of data protection. Art. 23 of the EUROPOL Council Decision. Council of the European Union, Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing EUROPOL's relations with partners, including the exchange of personal data and classified information, OJ L 325/6, 11.12.2009(b).

[133] See chapter IV of the EUROPOL Council Decision on "Relations with Partners". According to Article 25.1.a 'private parties' shall mean "entities and bodies established under the law of a Member State or a third State, especially companies and firms, business associations, non-profit organisations and other legal persons governed by private law...". For the condition under which data processing between EUROPOL and private parties may take place refer to Article 25.3.

[134] European Parliament (2011(a)), pp. 9, 41, 109. For an overview, see D. Heimans, "The External Relations of EUROPOL – Political, Legal and Operational Considerations", in B. Martenczuk and S. van Thiel (eds), *Justice, Liberty and Security: New Challenges for EU External Relations*, Brussels: VUB Press, 2008.

[135] Council of the EU (2012), *EUROPOL Work Programme 2013*, 12667/12, Brussels, 17.7.2012, p. 27; Article 5.2 EUROPOL Decision states that EUROPOL 'shall provide support to Member States in their tasks of gathering and analysing information from the Internet in order to assist in the identification of criminal activities facilitated by or committed using the Internet.' Article 25.4 EUROPOL Decision allows Internet Monitoring as it states that EUROPOL 'may directly retrieve and process data, including personal data, from publicly available sources, such as media and public data and commercial intelligence providers.'

[136] De Moor, A. and G. Vermeulen (2012), 'The EUROPOL Council Decision: Transforming EUROPOL into an Agency of the European Union', *Common Market Law Review*, Vol. 47, No. 4, p. 1108: "The nature of information and intelligence from private partners – often collected in a commercial environment for commercial purposes – requires additional safeguards, in order to ensure the accuracy of this information... the development of new partnerships must not occur at the expense of its own law enforcement professionalism."

takes place through EUROPOL National Units (ENU). Additionally, while EUROPOL itself cannot send back such data directly to private entities, the situation is much less clear with regard ENUs. Furthermore, EUROPOL is clearly being solicited by private companies with regard its cybercrime activities, especially commercial providers of computer security software. As discussed previously in relation with its 2011 iOCTA report, it also uses the knowledge produced by these companies to build its own strategic analyses. It might be necessary, in this regard, to consider the possibility of revising the 4x4 "handling code" used by the Office to evaluate the quality of sources and codes to take into account the dependence on private sources in the area of cybercrime[137].

Such a measure, however, is a halfway house and needs to be envisaged in the framework of a broader discussion. The lack of a concept or clear definition of 'cybercrime' within the EU has direct implications for the functioning of the proposed European Cybercrime Centre (EC3) as part of EUROPOL[138], and creates a larger degree of uncertainty for the individual as regards lower data protection standards for 'cybercrime' or the application of exceptions to those standards, and whether this differs from other crimes such as 'computer crime' and/or other 'serious crimes'. In that regard, Porcedda distinguishes broad cybercrime from narrow cybercrime. Broad cybercrime would justify lower data protection standards but, however, no violation of the core-periphery of human rights[139].

5. RECOMMENDATIONS

5.1. EU General Priorities

The study clearly suggests that the focus on cloud computing solely from the perspective of cybercrime is inadequate as regards to the challenges raised by cloud computing. The priority has been given to the regulation of internet, traceability of IP adresses, threats to national security through cyber attacks of critical infrastructure, and some spectacular forms of cyber crime like child pornography. Much more emphasis should be put on providing legal certainty in jurisdiction-spanning transfers of data involving a multiplicity of data controllers and processors. **The challenges of privacy and data protection in a cloud context are clearly underestimated, if not ignored**. In most European fora dealing with cybercrime, Data Protection laws appear to be very marginal in the agenda and inadequately addressed to meet the challenges raised by cloud computing.

Furthermore, **Data Protection offences should be recognized as a type of "Cybercrime"**. This current omission unbalances the framework of investigatory powers and Fundamental Rights, and the EU should include data protection offences in any future plans, orientations, and strategies dealing with Cybercrime.

In the area of cloud computing, it is high time that the EU clarifies what it is that EU bodies should be predominantly concerned with in the first place. Given the recent creation of a EC3 within the European Police Office EUROPOL, and the forthcoming adoption of an EU Cybersecurity strategy by the European Commission (foreseen December 2012 at the time of writing), this is a highly needed prerequisite. The priority should be given to the individual: her or his fundamental rights and freedoms should be as the core objective of the Union's policy.

[137] See EUROPOL (2010), *EUROPOL Information Mangement: Products and Services*, The Hague, 2510-271, for further details.

[138] European Commission (2012(d)), p. 7.

[139] Porcedda, M.G., *Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?*, EUI Working Paper, Law, p. 7.

5.2. Extension of the scope of data protection and harmonization of legal concepts

The DPD and the Proposal for a General Data Protection Regulation (PGDPR) do not apply to law enforcement activities, nor to domestic processing, which is still governed by various national regulatory systems in the different areas of law touched by cloud computing (i.e. civil law, administrative and commercial law). Furthermore, old third pillar instruments such as the DPFD and the PPCJDD do not apply to 'cloud computing providers' and to EU Home Affairs Agencies such as EUROPOL.

This calls firstly for a harmonization of fundamental **legal concepts such as 'jurisdiction', 'data processor' and 'data controller' at EU level**. Such harmonization would decrease conflicts of laws and would contribute towards more legal certainty for the data subject/consumer as regards the applicable law. They would also play an important role at times of addressing the challenges of jurisdiction and responsibility identified in this study.

However, the allocation of responsibility and potential liabilities should not merely depend on the definition of data controller and data processor. **An accountability approach should apply** instead, according to which responsibilities, liabilities and obligations should be vested upon every actor with 'considerable power', i.e. knowledge and control of the data. This should go along with the **effective use of existing Mutual Legal Assistance Treaties between the EU and third countries** with regard to access to personal data for national security and law enforcement purposes.

Furthermore, the EU-US Safe Harbour Principles which allow transfers of data to US organizations does not apply to telecommunication common carriers which also provide cloud computing services. The study recommends that Safe Harbour Certification are checked and reinforced. **The 'Safe Harbor' principle should also apply to telecommunication common carriers** which also provide cloud computing services.

In regard to EUROPOL, the fact that this agency is currently excluded from the scope of the PPCJDD calls for careful oversight of its data exchange activities. EUROPOL's core activity is to facilitate the exchange of information between Member States and to develop criminal intelligence. EUROPOL is also mandated to cooperate and engage in information exchange with third parties including other EU agencies, international organisations and third countries, as well as receive information (including personal data) from 'private parties'. In many ways, EUROPOL has become a 'data controller in its own right'. While awaiting for an EC proposal that is expected to bring the current EUROPOL Decision in line with the Lisbon Treaty, it is necessary to **consider the possibility of revising the 4x4 "handling code" used by the Office to evaluate the quality of sources and codes to take into account the dependence on private sources in the area of cybercrime**.

Furthermore, the lack of a concept of 'cybercrime' within the EU has direct implications for the functioning of the proposed EC3 as part of EUROPOL and creates a larger degree of uncertainty for the individual as regards lower data protection standards for 'cybercrime' and whether this differs from other crimes such as 'computer crime' and/or other 'serious crimes'. This is why, as recommended hereafter, close oversight of the EU agencies in the field of cybercrime is required.

5.3. Oversight of EU agencies in the field

The EU operational framework in the field of cybercrime consists mainly of two sets of measures which encapsulate NIS and law-enforcement activities. Here, **the question of the respective roles and responsibilities of EUROPOL and ENISA must be clarified**, if only to avoid duplication of activities and costs and ensure more effective undertakings. Such a clarification, however, should go beyond a mere matter related to the global regulation of the Internet and should take into account the question of the individual, her or his rights and freedoms.

The proposed **EC3 as part of EUROPOL should received careful attention**. The centre is expected to start operations in January 2013 and is entrusted with a great variety of tasks. The way in which the European Commission envisages the role of EC3 clearly demonstrates a lack of established priorities and, according to the EUROPOL staff, insufficient resources given the wide scope of the centre's remit.

According to the analysis conducted in this study, the cybercrime centre could have a significant added value if more resources were allocated to the protection of EU citizens. This includes **members of staff highly qualified in cloud computing technologies, but also well trained in data protection and privacy laws**. However, funding should be carefully allocated. The cybercrime centre should give budgetary priorities to hunt down cybercriminals while protecting EU citizens' rights, and not wasting resources in dubious early warning and vain "preventive" tasks.

5.4. US/ EU Relations

Particular attention should be given to **US law that authorizes the surveillance of Cloud data of non-US residents**. The EP should ask for further enquiries into the US FISA Amendments Act, the status of the 4th Amendment with respect to NONUSPERS, and the USA PATRIOT Act (especially s.215).

The EP should consider **amending the DP Regulation to require prominent warnings to individual data subjects** (of vulnerability to political surveillance) before EU Cloud data is exported to US jurisdiction. No data subject should be left unaware if sensitive data about them is exposed to a 3rd country's surveillance apparatus. The existing derogations must be dis-applied for Cloud because of the systemic risk of loss of data sovereignty. The EU should open new negotiations with the US for recognition of a human right to privacy which grants Europeans equal protections in US courts.

5.5. EU ownership over data

The EU needs **an industrial policy for autonomous capacity in Cloud computing**. The DG INFSO Communication of October 2012 is on this matter not in tune with the challenges analysed in this study. A target could be that by 2020, 50% of EU public services should be running on Cloud infrastructure solely under EU jurisdictional control.

REFERENCES

- Article 29 Data Protection Working Party (2002), *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, 5035/01/EN/Final WP 56, Brussels, 30.04.2002.
- Article 29 Data Protection Working Party (2008), *Opinion 1/2008 on data protection issues related to search engines*, 00737/EN WP 148, Brussels, 04.04.2008.
- Article 29 Data Protection Working Party (2009 (a)), *The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 02356/09/EN WP 168, 01.12.2009.
- Article 29 Data Protection Working Party (2009 (b)), Opinion 5/2009 on online social networking, 01189/09/EN WP 163, Brussels, 12.06.2009.
- Article 29 Data Protection Working Party (2010 (a)), *Opinion 3/2010 on the principle of accountability*, 00062/10/EN WP 173, Brussels, 13.07.2010.
- Article 29 Data Protection Working Party (2010 (b)), *Opinion 8/2010 on applicable law*, 0836 02/10/EN WP 179, Brussels, 16.12.2010.
- Article 29 Data Protection Working Party (2010 (c)), *Opinion 1/2010 on the concepts of 'controller' and 'processor'*, 00264/10/EN WP 169, Brussels, 16.02.2010.
- Article 29 Data Protection Working Party (2012(a)), *Opinion 05.2012 on Cloud Computing*, 05/12/EN WP 196, Brussels, 01.07.2012.
- Article 29 Data Protection Working Party (2012(b)), *Working Document 02.2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*, 00930/12/EN WP 195, Brussels, 06.06.2012.
- Council of Europe (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' does not make a distinction between data controller and data processor*, Strasbourg, 21.1.1981
- Council of Europe (2001), *Convention on Cybercrime*, Budapest, 23.11.2001.
- Council of Europe (2010 (a)), *Cloud computing and its implications on data protection*, discussion paper, prepared by Research Centre on IT and Law (CRID), 05.03.2010.
- Council of Europe (2010 (b)), *Cloud Computing and cybercrime investigations: Territoriality vs. The power of disposal*, discussion paper, prepared by J. Spoenle, 31.08.2010.
- Council of the European Union (2004), *Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography*, OJ L 13/44, 20.1.2004.
- Council of the European Union (2005), Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69/67, 16.3.2005.
- Council of the European Union (2008(a)), *Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,* OJ L 350, 30.12.2008.
- Council of the European Union (2008(b)), *Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, OJ L 330/21, 9.12.2008.
- Council of the European Union (2009*), Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL) (2009/371/JHA)*, OJ L 121, 15.05.2009.
- Council of the European Union (2012), *EUROPOL Work Programme 2013*, 12667/12, Brussels, 17.7.2012.

- De Busser, E. (2012), "The Adequacy of an EU-US Partnership", in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Dordrecht/Heidelberg/London/New York: Springer, 2012, pp. 203-232.
- De Hert, P. and B. de Schutter (2008), "International Transfers of Data in the Field of JHA: The Lessons of EUROPOL, PRN and Swift", in B. Martenczuk and S. van Thiel (eds.), *Justice, Liberty, Security: New Challenges for EU External Relations*, Brussels: VUBPress, pp.303 – 340.
- De Hert, P. and V. Papakonstantinou (2012), "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, Vol. 28, No. 2, April.
- De Hert, P. and V. Papakonstantinou (2012), "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, Vol. 22, No. 6, February/March.
- De Moor, A. and G. Vermeulen (2012), "The EUROPOL Council Decision: Transforming EUROPOL into an Agency of the European Union", *Common Market Law Review*, Vol. 47, No. 4.
- Drewer, D. and J. Ellermann (2012), "EUROPOL's data protection framework as an asset in the fight against cybercrime", *ERA Forum: Journal of the Academy of European Law*, forthcoming.
- European Commission (2000), *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 2000/520/E, OJ L 215, 25.8.2000.
- European Commission (2001(a)), *Creating a Safe Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM(2000) 890 final, Brussels, 26.1.2001.
- European Commission (2001(b)), *Commission Communication on Network and Information Security: Proposal for a European Policy Approach*, COM(2001) 298 final, Brussels, 6.6.2001.
- European Commission (2005), *Green Paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final, Brussels, 17.11.2005.
- European Commission (2006), *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, COM(2006) 251 final, Brussels, 31.5.2006
- European Commission (2007), *Communication to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime*, SEC(2007) 641, SEC(2007) 642, COM/2007/0267 final
- European Commission (2008), *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*, COM(2008) 448 final, Brussels, 14.7.2008.
- European Commission (2009), *Critical Infrastructure Protection – Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM(2009) 149 final, Brussels, 30.3.2009
- European Commission (2010(a)), *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A Digital Agenda for Europe,* COM(2010) 245 final/2, Brussels, 26.8.2010.
- European Commission (2010(b)), *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, COM(2010) 517 final, Brussels, 30.09.2010.
- European Commission (2010(c)), *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions: A*

comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, Brussels, 4.11.2010.

- European Commission (2011), *Critical Information Infrastructure Protection – Achievements and next steps: towards global cyber-security*, COM(2011) 163 final, Brussels, 31.3.2011
- European Commission (2012(a)), *Data protection reform: Frequently asked questions*, MEMO/12/41, Brussels, 25.01.2012.
- European Commission (2012(b)), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels, 25.01.2012.
- European Commission (2012(c)), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM(2012) 10 final, Brussels, 25.01.2012.
- European Commission (2012(d)), *Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final, Brussels, 28.03.2012.
- European Commission (2012(e)), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions*: *Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 /2, Brussels, 27.09.2012.
- European Data Protection Supervisor (EDPS) (2012), *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7.3.2012.
- European Network and Information Security Agency (ENISA) (2009(a)), *Cloud computing: benefits, risks and recommendations for information security*, Heraklion, November 2009.
- European Network and Information Security Agency (ENISA) (2009(b)), *Cloud Computing Information Assurance Framework*, Heraklion, November 2009.
- European Network and Information Security Agency (ENISA) (2011), *Security and resilience in governmental clouds*, Heraklion, January 2011.
- European Parliament and Council of the European Union (1995), *Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995.
- European Parliament and Council of the European Union (2002), *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002.*
- European Parliament and Council of the European Union (2004), *Regulation (EC) No 464/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (ENISA)*, OJ L 77/1, 13.3.2004.
- European Parliament and Council of the European Union (2006), *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,* OJ L 105, 13.44.2006.

- European Parliament and Council of the European Union (2011), Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335/1, 17.12.2011.
- European Parliament (2000), *Resolution of 16 September 1999 on the establishment of the Charter of Fundamental Rights*, OJ C 54, 25.2.2000.
- European Parliament (2001), *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, PE 305.391 A5-0264/2001.
- European Parliament (2011(a)), *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies. Frontex, EUROPOL and the European Asylum Support Office*, PE 453.196, August.
- European Parliament (2011(b)), *Towards a New EU Legal Framework for Data Protection and Privacy*, Committee on Civil Liberties, Justice and Home Affairs, PE 453.216, September.
- European Parliament (2011(c)), *Developing an EU Internal Security Strategy, fighting terrorism and organised crime*, PE 462.423, November.
- European Parliament (2011(d)), *Does it help or hinder? Promotion of Innovation on the Internet and Citizen's Right to Privacy*, PE 464.462, December.
- European Parliament (2012(a)), *Cloud Computing*, Policy Department Economic and Scientific Policy, PE 475.104, May.
- European Parliament (2012(b)), *Working Document on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,* PE491.322v01-00, Brussels, 6.7.2012.
- European Parliament (2012(c)), *Reforming the Data Protection Package*, PE 492.431, September.
- EUROPOL, *EUROPOL Information Management: Products and Services*, The Hague, 2510-271, 2010
- Hon, W.K., C. Millard and I. Walden (2011(a)), "The Problem of 'Personal Data' in Cloud Computing – What information is Regulated? The Cloud of Unknowing, Part 1", Queen Mary School of Law Legal Studies Research Paper No. 75/2011, March; *International Data Privacy Law*, Vol. 2, No. 4, November.
- Hon, W.K., C. Millard and I. Walden (2011 (b)), "Who is responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", Queen Mary School of Law Legal Studies Research Paper No. 77/2011, March, *International Data Privacy Law*, 2012, Vol. 2, No. 1, February.
- Hon, W.K., J. Hörnle and C. Millard (2011), "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3", Queen Mary School of Law Legal Studies Research Paper No. 84/2011, February.
- Hon, W.K. and C. Millard (2012), "Data Export in Cloud Computing – How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Part 4", *SCRIPTed,* Vol. 9, No. 1, April.
- Hustinx, P., "Data Protection and Cloud Computing under EU Law", Third European Cyber Security Awareness Day BSA, European Parliament, 13 April 2010.
- Kuner, C. (2010), "Data Protection Law and International Jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology* , Vol. 18., No. 3., Fall, available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689495&rec=1&srcabs=1496847

- Porcedda, M.G., "Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?", EUI Working Paper, Law, No. 25.
- Poulet, Y. et al. (2011), "Data Protection in the Clouds", in. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht/Heidelberg/London/New York: Springer, 2011, pp. 377-409.
- Reding, V., "Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing", IAPP Europe Data Protection Congress, Paris, 29.11.2011.
- Ruiter, J. and W. Martijn, "Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice", in S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht/Heidelberg/London/New York: Springer, 2011, pp. 361-376.
- Sartor, G. (2012), "Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?", EUI Working Papers, Law, No. 24.
- Strange, S. (1992) "States, Firms and Diplomacy", *International Affairs*, 68(1): 1-15.

ANNEXES

Annex 1: The EU framework on fighting cybercrime and privacy – initiatives and EU bodies involved

The starting point adopted to map each initiative is an initiative from the European Commission. This does not preclude that these initiatives might have been prompted by another body of the EU, e.g. the Council.

N/A = not applicable/ not available.

Initiative	'Lead' service (Commission)	Council configurations	Parliament Committee	
Creating a Safe Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final	DG INFSO DG JHA	Justice and Home Affairs Competitiveness Transport, Telecommunications and Energy	Responsible LIBE	Opinion ECON JURI ITRE CULT
Network and Information Security: Proposal for a European Policy Approach, COM(2001) 298 final	DG INFSO	Transport, Telecommunications and Energy General Affairs Economic and Financial Affairs (ECOFIN)	Responsible LIBE	Opinion JURI ITRE CULT
Proposal for a Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency, COM(2003) 63 final	DG INFSO	Transport, Telecommunications and Energy Justice and Home Affairs	Responsible ITRE	Opinion BUDG LIBE JURI
A strategy for a Secure Information Society – "Dialogue, partnership and empowerment", COM(2006) 251 final	DG INFSO	Transport, Telecommunications and Energy	N/A	

		General Affairs Economic and Financial Affairs (ECOFIN)		
Towards a general policy on the fight against cyber crime, COM(2007) 267 final	DG JLS	General Affairs	N/A	
Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, COM(2007) 861 final	DG INFSO	Transport, Telecommunications and Energy General Affairs	Responsible ITRE	Opinion LIBE
Critical Infrastructure Protection – Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009) 149 final	DG INFSO	Transport, Telecommunications and Energy	N/A	
Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM(2010) 94 final	DG Justice	Justice and Home Affairs General Affairs	Responsible LIBE	Opinion CULT FEMM
Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517 final	DG Home	Justice and Home Affairs	Responsible LIBE	Opinion AFET BUDG ITRE
Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, COM(2010) 520 final	DG INFSO	Transport, Telecommunications and Energy	Responsible ITRE	Opinion N/A
Critical Information Infrastructure Protection – Achievements and next steps: towards global cyber-security, COM(2011) 163 final	DG INFSO	Transport, Telecommunications and Energy	Responsible ITRE	Opinion AFET LIBE
Tackling Crime in Our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final	DG Home	Justice and Home Affairs	Responsible LIBE	Opinion INTA

				BUDG ECON ITRE JURI

Annex 2: Estimates of EC3 staffing requirements and costs

These informations have been forwarded by Europol.

EC3 personnel and expenditures in relation to overall EUROPOL staff and expenditures

Big figures: 800 people are working at Europol. Of them:

- 530 Europol Employees (440 Temporary Agents and 90 Contract Agents.)
- 40 Seconded National Experts,
- 150 Liaison Officers ,
- The rest (variable) about 20 trainees and 60 contractors.

  Note:

  - Contract Agents are mainly working in the Governance and Capabilities Departments
  - SNEs, all of them members of the National Competent LE Services, are fully integrated in different Units of the Operations Department

Temporary Agents in the Establishment Plan 2012: 457. Of them:

- 226 in Operations
- 162 in Capabilities
- 61 in Governance
- 8 (Director, MB Secretariat and Internal Audit Function)

The Operations Department is organized in 4 Business Areas with the following staff (TAs + 40 SNEs):

- Information Hub: 60
- Cybercrime: 31
- Counterterrorism: 55
- Organised Crime 120

The EC3 Cybercrime Centre is organized in 3 main groups:

- Operations and Data fusion
- Research and Development
- Strategy and Outreach

Most of the current staff is in Operations: 22 staff members have been transferred from the old Europol structure working in 3 focal points covering the three areas of the EC3 mandate: Crimes against persons trough the Internet, on-line fraud and crimes affecting the ICT infrastructures. The rest (9) are distributed in the other groups.

That means that only Operations can continue delivering services (although not at the desired level of the EC3 mandate). The other areas must be properly staffed to achieve the mandate of the Centre. Our analysis, based on the products and services to be delivered, is that 60 FTEs will be needed in 2013 and 100 in 2014.

In general terms Operations and Data Fusion (about 75% of the resources of the Centre) will be staffed with TAs, police officers recruited from the Competent Services. The rest 25% distributed in Research and Development and Strategy and Outreach does not need to be recruited from the Competent Services.

All of them need to be specialists in their respective areas and most of them will occupy long-term positions. Only in the case of Outreach some SNEs from the target Countries will be preferred for seconded for maximum 3 years in order to rotate and be replaced by others from a different target country.

It will not be excluded the recruitment of some contract agents to develop specific projects.

Breakdown of EC3 costs for 2013-2014

2013

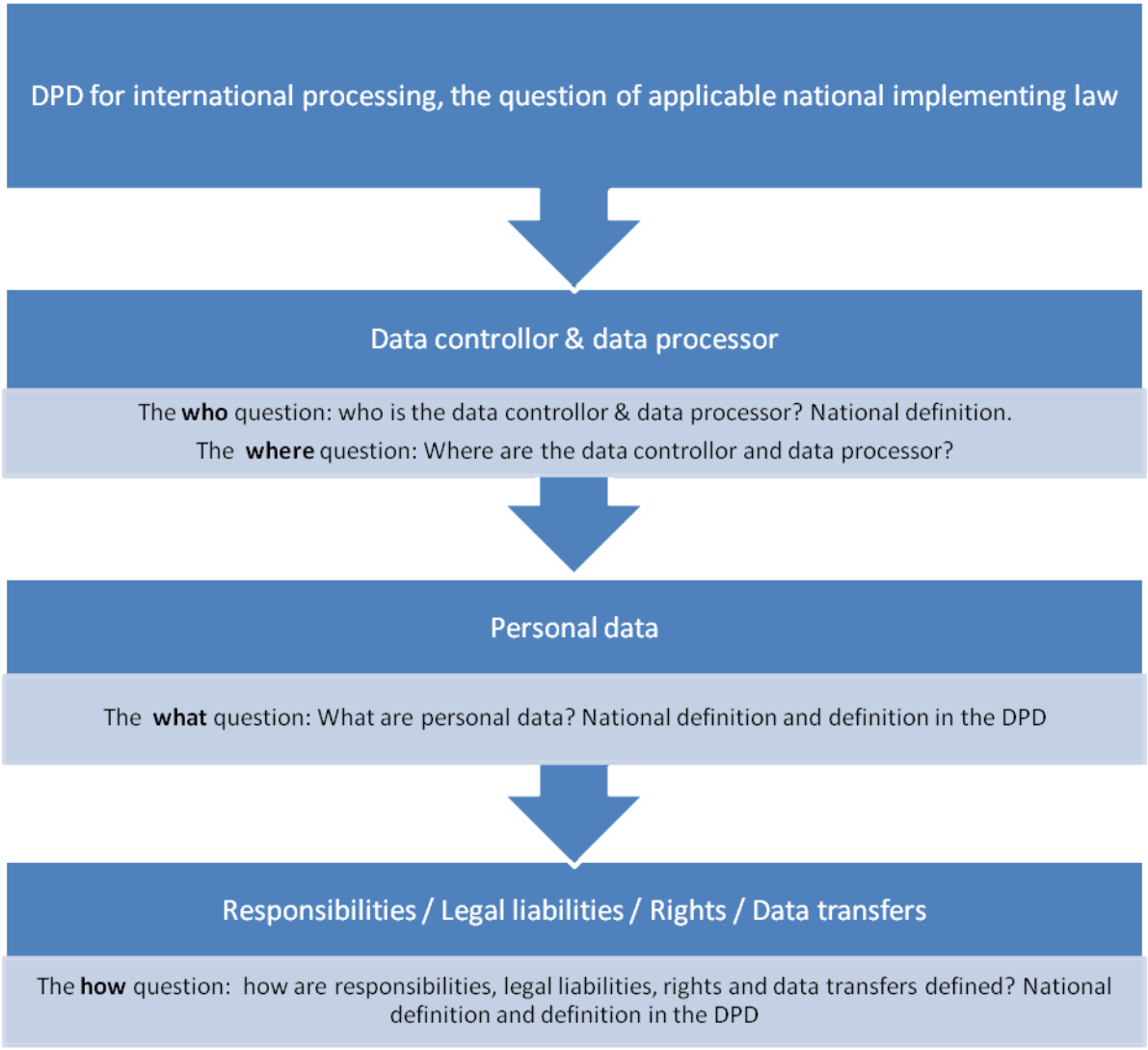
Expense	Explanation	Updated budget
Staff expenditure	29 Total of new recruited staff (31 existed staff are budgeted in general Europol budget - T1) Other staff and recruitment expenditure	2,850,000
One time expenditure - investment	Building related cost, facility and IT equipments	2,200,300
Running activities related expenditure	Day to day running costs for missions, meetings, consultancy, trainings and software upgrades and IT maintenance	1,305,400
		6,355,700

2014

Expense	Explanation	Updated budget
Staff expenditure	69 recruited staff for EC3 (31 existed staff are budgeted in the general Europol budget - T1) Other staff and recruitment expenditure	6,808,000
One time expenditure - investment	Building related cost, facility and IT equipments	760,000
Running activities related expenditure	Day to day running costs for missions, meetings, consultancy, trainings and software upgrades and IT maintenance	2,293,500
		9,861,500

Source : EUROPOL documents EDOC 621532 & 615458

Annex 3: Definitional problems, Member States' discretion under the DPD



EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN