"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

FP7-SCIENCE-IN-SOCIETY-2013-1

Grant Agreement Number 612345

Supporting Action

MAPPING

WP4 INTERNET GOVERNANCE
WP leader: RUG

D4.2
Report on "The EU Internet Vision: past, present & future" – Interim Report

Project co-funded by the European Commission within the 7th Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Document Version Control:

Version 0.1	Originated by:	B. Zhao	On 29 July 2014
Version 0.2	Reviewed by:	J.P. Mifsud Bonnici	On 07 Aug 2015
Version 0.3	Revised by:	B. Zhao	On 21 Dec 2015
Version 0.4	Revised by:	J.P. Mifsud Bonnici	On 03 Feb 2016
Version 0.5	Reviewed by:	J. Cannataci	On 03 Feb 2016

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

TABLE OF CONTENTS

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Executive summary

This interim deliverable documents part of the work carried out in Task 4.1 - Organising fragments of the vision: towards a cohesive and coherent EU policy about Internet governance, participative freedoms, ethics and security.

As noted in the Description of Works of the MAPPING project, "this task is to collect, categorise and make public all EU legislative instruments and policy documents which somehow embody or otherwise contribute to an EU vision of Internet Governance. Given the current state of fragmentation of effort at the European level, it is expected that this would also at least partially take the form of a gap analysis of those aspects which need to be discussed more deeply and decided upon. This will be done through: a review of literature as well as access to primary sources which would then in turn inform the project's stakeholder exchange of knowledge and experience; providing a forum for the different stakeholders to further identify gaps in EU vision, discuss issues, understanding seemingly opposing perspectives and evaluating novel solutions as well as existing key practices that can qualify as best practices."

The work in this task serves a number of purposes, *inter alia*:

a. As a basis for informed debate with different stakeholders involved in Internet governance;

b. As a source of information for other tasks carried out within this Internet Governance work package;

c. Serves as a basis for links with other work packages, such as WP5 on Privacy and Business Models and WP6 on Intellectual Property protection.

From the review carried out in this task, one can confirm that there is no one single coherent EU vision for Internet Governance. The vision, if one can call it so, consists of many aspects, including the a human rights perspective (privacy, data protection, freedom of expression, etc. on the Internet), an economic perspective with an ambition for a single digital market in the information age, and a technical perspective including interoperability, super-connectivity and efficiency, and net-neutrality, and the political perspective including national security, anti-terrorism aspects in particular.

Furthermore this collection of aspects and ensuing visions is not a product of one single stakeholder, but many including the EU authorities, Member States, civil society organizations, the industrial (private)

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

sector that includes not only EU IT companies, but more U.S. IT Giants, EU citizens (limited roles in shaping the vision, mostly as consumers and litigants), etc.. Each of these players and stakeholders all have their own vision/plan for the future Internet and work towards achieving this.

Moreover, the EU vision cannot be separated from a bigger vision of Internet governance including other countries and regions, including China, the U.S., Russia and Brazil, which to different extents shape Internet governance through political and diplomatic means. Given this, there seems to be an increase of EU participation in Internet governance fora, including in multi-stakeholder Internet governance fora such as Netmundial.

In some instances, different perspectives of the EU vision conflict with each other. However, even in at times conflicting stances there is a common core in the EU position in particular on the protection of EU values including protection of fundamental human rights and an open Internet over a fragmented Internet.

What has been noted from the start of the MAPPING project is that the EU's Internet Vision is to a great extent a 'work-in-progress', suffice it to mention the ongoing legislative reforms of the data protection framework, safe harbour rules on the cross-border use of personal data, net neutrality, standardisation exercises of e.g. privacy-by-design and several other political debates that follow from international acts of violence or terrorism on the use of encryption on the Internet and Internet services, mass surveillance etc. These ongoing, sometimes fast, sometimes excruciatingly slow, developments mean that the task in 4.1 is also a work-in-progress: this is an interim report to be followed upon and updated as the project progresses in the coming months. It is only an ongoing updating process that can ensure that the purposes of this review are achieved.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

List of Abbreviations Used in this Document

AWFs Analysis Work Files

BCR Binding Corporate Rules

CERTs Computer Emergency Response Teams

CIIP Critical Information Infrastructure Protection

CLP Cloud Legal Project

DoS Denial-of-Service

DPA Data Protection Authority

DPIA data protection impact assessment

DPD Data Protection Directive

DPRP Data Protection Regulation Package

DPFD Data Protection Framework Decision

EC European Commission

EC3 European Cyber Crime Centre

EDPD European Data Protection Board

EDPS European Data Protection Supervisor

EEA European Economic Area

eID Electronic Identification

ENISA European Network and Information Security Agency

ENU Europol National Units

EPCIP European Programme for Critical Infrastructure Protection

eTS Electronic Trust Services

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

EU European Union

EU ISS EU Internal Security Strategy

EWS Amazon Web Services

FISAA Foreign Intelligence Surveillance Amendment Act

FRA European Union Agency for Fundamental Right

HTCC High Tech Crime Centre

IaaS Infrastructure-as-a-Service

ICT Information and Communication Technology

iOCTA Internet Facilitated Organised Crime Report

IPRs Intellectual Property Rights

Joint PCP Agreement Joint Pre-Commercial Procurement Agreement

LEA Law Enforcement Agency (Authority)

LEs Law Enforcement Sector

LIBE – the European Parliament's Civil Liberties, Justice and Home Affairs Committee

NASA National Aeronautic Space Administration

MEAT Most Economically Advantageous Tender

MLAT Mutual Legal Assistance Treaty

MiDs Mobile Internet Devices

MS Member States

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

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

PCP Pre-commercial Procurement

PGDPR Proposal for a General Data Protection Regulation

PPCJDD Proposal for a Police and Criminal Justice Data Protection Directive

SaaS Software-as-a-Service

Policy Department C: Citizens' Rights and Constitutional Affairs

SHA Safe Harbour Agreement

SIS Security and Intelligence Services

SLA Service Level Agreement

SME Small and Medium Enterprises

WP29 Article 29 Data Protection Working Party

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

1. Introduction

Commission Vice-President Neelie Kroes is reported to have said: "The next two years will be critical in redrawing the global map of Internet governance. Europe must contribute to a credible way forward for global internet governance. Europe must play a strong role in defining what the net of the future looks like."[1]

20 months later how much of this claim is achieved is debatable. From a review carried out in pursuance of MAPPING *Task 4.1 - Organising fragments of the vision: towards a cohesive and coherent EU policy about Internet governance, participative freedoms, ethics and security* - one can confirm that there is no one single coherent EU vision for Internet Governance. The vision, if one can call it so, consists of many aspects, including the human rights perspective (privacy, data protection, freedom of expression, etc. on the Internet), an economic perspective with an ambition for a single digital market in the information age, and a technical perspective including interoperability, super-connectivity and efficiency, and net-neutrality, and the political perspective including national security, anti-terrorism aspects in particular.

Furthermore this collection of aspects and ensuing visions is not a product of one single stakeholder, but many including the EU authorities, Member States, civil society organizations, the industrial (private) sector that includes not only EU IT companies, but more U.S. IT Giants, EU citizens (limited roles in shaping the vision, mostly as consumers and litigants), etc.. Each of these players and stakeholders all have their own vision/plan for the future Internet and work towards achieving this.

In the next sections of this document we trace some of these visions and actors, under the following rubrics:

a. Visions on Net neutrality and open internet
b. Visions on Cloud computing
c. Building trust
d. Mass surveillance
e. Cyber security
f. International transfer of personal data and exterritorial jurisdiction

[1] COMMISSION TO PURSUE ROLE AS HONEST BROKER IN FUTURE GLOBAL NEGOTIATIONS ON INTERNET GOVERNANCE PRESS RELEASES DATABASE, http://europa.eu/rapid/press-release_IP-14-142_nl.htm (last visited Aug 20, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

g. Privatization of Internet Governance

h. EU Data protection laws and remedies

What has been noted from the start of the MAPPING project is that the EU's Internet Vision is to a great extent a 'work-in-progress', suffice it to mention the ongoing legislative reforms of the data protection framework, safe harbour rules on the cross-border use of personal data, net neutrality, standardisation exercises of e.g. privacy-by-design and several other political debates that follow from international acts of violence or terrorism on the use of encryption on the Internet and Internet services, mass surveillance etc. These ongoing, sometimes fast, sometimes excruciatingly slow, developments mean that this report too should be considered a work-in-progress: this is an interim report to be followed upon and updated as the project progresses in the coming months. It is only an ongoing updating process that can ensure that the purposes of such a review are eventually achieved.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

2. The technical perspective

2.1. Net neutrality and open internet

Net neutrality is one of the recent hot issues in Internet governance that has trigged numerous debates at EU level since the recent drafted law by the European Council a digital single market. Though many may find it hard to define what exactly network neutrality is or networks Neutrality,[2] the EU net neutrality laws is getting more precise on the matter. Initially, the Framework Directive on electronic communications defines net neutrality from the perspective of "as the ability of end users to access and distribute information or run applications and services of their choice." Most recently the Amendment 234 of Regulation on the Single Telecoms Market, passed by the European Parliament in April 2014, offers a detailed, strong definition of the net neutrality principle that" traffic should be treated equally, without discrimination, restriction or interference, independent of the sender, receiver, type, content, device, service or application."[3]

Net neutrality is crucial for EU's Internet Governance due to the fact that it involves many fundamental issues, including the openness of the Internet and innovation, matters of competition and antitrust, new business models, EU citizens' fundamental rights to free speech and privacy, and EU's political and economic harmonization. As thus perceived, it is one of the crucial issues of EU's Internet Governance whose regulatory policies and rules attract multiple criticisms although net neutrality and the open Internet are desired by all stake holders in debate of the future of the Internet.

Net neutrality can be regarded as having its support from the Charter of Fundamental Rights, in particular "the respect for private and family life, the protection of personal data and freedom of expression and information."[4] For this reason, any legislative proposals in this area will be subject to an in-depth assessment of their impact on fundamental rights and of their compliance with the Charter of Fundamental Rights of the EU." The European Commission declared its full commitment to "preserving the open and neutral character of the internet, taking full account of the will of the co-legislators now to enshrine net neutrality as a policy objective and regulatory principle to be promoted by national

[2] See different definitions and related scenario discussed by Kraemer and others, at: JAN KRAEMER ET AL., NET NEUTRALITY: A PROGRESS REPORT (Social Science Research Network) (2013), http://papers.ssrn.com/abstract=2344623 (last visited Aug 20, 2014).

[3] See: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0190&language=EN&mode=XML#

[4] Article 8 of the Charter.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

regulatory authorities". [5] This lays out the principle of openness and net neutrality.[6] The 2009 Electronic Communications Regulatory Framework supports Net Neutrality in the following aspects: Choice (Art. 8(4) of the Framework Directive), Transparency (Art. 20 & 21 of the Universal Service Directive), Quality of Service (Art. 22(3) of the Universal Service Directive), and E-privacy (Art. 5 of the e-Privacy Directive).[7]

However, Net Neutrality has not been provided with the desired legal safeguard.[8] The approach taken is to ensure enough competition among market players so that network users can freely choose and switch among competitors. As evidenced in BEREC's investigation in 2012, however, the Telecoms Package approach is insufficient in safeguarding net neutrality. [9] It is most recently revealed in the 2014 Eurobarometer survey that a quarter of Europeans still confront blocking of internet content including music, videos and applications.[10] Net Neutrality principle has been violated by network operators in business practices in forms of restrictions of the use of certain apps, content or technologies, providing specialised services, prioritizing preferred services, or even data caps.[11] How to make a balance between proper traffic management and openness of the Internet is not an easy task when they have to both make profits on competitive markets and follow regulations and policies to the best.

In contrast to the above realities is the fact that "At this moment, the EU has no clear legal protection for Net Neutrality, leaving 96% of Europeans without legal protection for their right to access the full

[5] See attached deceleration on Net Neutrality to the 2009 Regulatory Framework of Electronic Communications, at:

[6] Chris Marsden, *Net Neutrality: Measuring the problem, Assessing the legal risks*, IBEI WORKING PAPERS , 13 (2014), http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fcatedratelefonica.ibei.org%2Fwp-content%2Fuploads%2F2013%2F06%2FIBEI-%25C2%25B7-42.pdf&ei=SmrrU7f8C4XGPM68gTg&usg=AFQjCNEIXj00ksHNM_eV8bJl0TSLHvR3JA&sig2=Ki_cM841wLqJ9fUX8kdoog&bvm=bv.72938740,d.ZWU (last visited Aug 13, 2014).

[7] See reference at: http://ec.europa.eu/digital-agenda/about-open-internet

[8] EDRi booklet on net Neutrality, at:

[9] See BEREE's research released in May 2012, at: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf

[10] http://europa.eu/rapid/press-release_MEMO-14-136_en.htm?locale=en

[11] See BEREE's research released in May 2012, at: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf

[11] http://europa.eu/rapid/press-release_MEMO-14-136_en.htm?locale=en

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

open internet."[12] In 2010 European Commissioner Neelie Kroes then announced that regulations at that time were adequate enough to ensure Net Neutrality in the EU.[13] It is since 2011 that EU authorities started to take substantial steps to strengthen net neutrality protection and end the risky "wait-and-see" strategy, including investigations, several public consultations, and new policy drafting.[14] Member States have different approaches regarding Net Neutrality. Among Member States, the UK, Hungary and Sweden are taking an approach of self-regulatory initiatives based on code of practice; Belgium and Luxemburg were considering legislation, Finish Government proposed to the Parliament a telecoms legislative package with Net Neutrality provisions, and Netherlands and Slovenia passed Net Neutrality laws. [15] Other further moves in Member States are pending after the EU Commission proposed single market regulation.

On the 3rd of April, most recently, the European Parliament approved a proposed legislation prohibiting Internet service providers from restricting or enhancing services of selected Internet traffic. It added to the draft law that "These tendencies require clear rules ... to maintain the open Internet and to avoid fragmentation of the single market resulting from individual Member States' measures."[16] The passed Telecoms Single Market Regulation that supports Net Neutrality principle and the open internet was welcomed by civil society organizations and human rights activists. The dedication of this new law to Net neutrality no doubt will pave the way for a single European telecoms market. Two of the three loopholes pointed out by critics, namely, freedom of end users, and the open purpose to "prevent or impede serious crime", have been patched by the Parliamentary amendments, with the broad definition of "specialized services" to be fixed in either the future Council's reading(s) or in future legal practices. [17]

[12] On Commitment to Net Neutrality, European Commission at: https://ec.europa.eu/digital-agenda/en/eu-actions

[13] EUROPEAN PARLIAMENT APPROVES "NET NEUTRALITY" PROPOSAL JURIST, http://jurist.org/paperchase/2014/04/european-parliament-approves-net-neutrality-proposal.php (last visited Aug 7, 2014).

[14] See a description of such efforts.

[15] Commission Staff working document: implementation of the EU regulatory framework for electronic communications-2014, p. 18.

[16] Recital 45, draft proposal.

[17] For the three loopholes revealed of the Council's draft, see: EUROPEAN PARLIAMENT TO DECIDE ON THE FUTURE OF THE OPEN INTERNET, http://history.edri.org/NN-EP (last visited Aug 20, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Under the draft law, web services defined as "specialized services" can be treated differently by Internet Service Providers and thus be exempted from the net neutrality principle. Most critiques focus on this vague definition and its potential negative influences on new start-ups.[18] It might be the case that specialized services can be a leeway to circumvent net neutrality regulations, "While diverting traffic away from the public Internet to a less regulated premium priced alternative".[19] As BEUC (The European Consumer Organization) analysed, for instance, ISPs can take an online service and serve it separately from the general internet access service, while regarding this as a "specialised" service and this is against the net neutrality principle.[20] As Save the Internet noted, the broad definition does not provide clear legal guidance and specialised services should be limited to services provided by ISPs such as IPTV, but not be confused with services on the open Internet, like YouTube or Spotify. [21]

The reaction from the European electric communications industry, mainly network services providers which obviously are against more regulations and restrictions on their services although support net neutrality and an open internet, cannot be overlooked. In the joint communications after the Parliament's vote in April by the industrial lobbying groups, it was said that the European Parliament position "would put in jeopardy services currently provided to broadband users," "reduce European users' choice" by restrictive rules, "distort competition with restrictive open internet provisions" and "create legal uncertainty" with hyper-prescriptive and complex provisions. However, such claims made in the communications are rather general without specificities mentioned against the proposed net neutrality policy. How these general comments would be taken in the Council's further reading is another issue to be observed in the near future.

[18] EUROPEAN PARLIAMENT PASSES STRONG NET NEUTRALITY LAW, ALONG WITH MAJOR ROAMING REFORMS, http://gigaom.com/2014/04/03/european-parliament-passes-strong-net-neutrality-law-along-with-major-roaming-reforms/ (last visited Jul 25, 2014).

[19] Marsden at 19.

[20] BEREC MONITORING QUALITY OF INTERNET ACCESS DEVICES IN THE CONTEXT OF NET NEUTRALITY 4, http://www.beuc.org/about-beuc/who-we-are (last visited Aug 20, 2014).

[21] A MISSED OPPORTUNITY FOR NET NEUTRALITY IN EUROPE ACCESS NOW, https://www.accessnow.org/blog/2014/03/18/a-missed-opportunity-for-net-neutrality-in-europe (last visited Aug 20, 2014). http://arstechnica.com/tech-policy/2014/03/eu-net-neutrality-vote-would-let-isps-charge-for-internet-fast-lane/

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

2.2. Cloud computing

In short, "Cloud computing is the locating of computing resources on the Internet in a fashion that makes them highly dynamic and scalable."[22] . The concept of cloud computing refers closely to IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) and collectively EaaS (Everything as a Service), all of which imply a service-oriented architecture.[23] Though not a new technology, cloud computing has been changing the way of how we store, access and use data largely and can be beneficial for economy, individual life and governance. But this technology also brings many problems in general regarding data privacy, data security, copy right protection, mass surveillance, Cybersecurity, diplomatic controversies, and jurisdiction conflicts, etc. This may prevent many entities from using the service in Europe especially after Snowden's revelation.[24] Among other risks, what's worthy our close attention is the improper use and/or mismanagement of data by cloud providers and the marginalization of individual users,[25] especially when they are private companies and foreign enterprises.

At the EU level, upon realizing the importance of the cloud computing technology for future development, the Union started pacing up legislation and policy making process since 2010. However, up till 2012, "there is no overall policy orientation on the issue", as partially evidenced in the various components of the EU's cybercrime policy framework that falls under the responsibility of different services and involves different groups of experts and stakeholders. [26] One of the major drawbacks of the policy debates on cloud computing is the overlook of the right of individuals among the triangular-relations among state, interstate and private companies, in view of individuals' changing role from data subjects and customers to products and commodities.[27]

---

[22] PAUL M. SCHWARTZ, INFORMATION PRIVACY IN THE CLOUD 1264 (Social Science Research Network) (2013), http://papers.ssrn.com/abstract=2290303 (last visited Aug 24, 2014).

[23] THE FUTURE OF CLOUD COMPUTING OPPORTUNITIES FOR EUROPEAN CLOUD COMPUTING BEYOND 2010 DIGITAL AGENDA FOR EUROPE 1, 8/10, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf. (last visited Aug 24, 2014).

[24] EUROPA - PRESS RELEASES - PRESS RELEASE - WHAT DOES THE COMMISSION MEAN BY SECURE CLOUD COMPUTING SERVICES IN EUROPE?, http://europa.eu/rapid/press-release_MEMO-13-898_en.htm (last visited Aug 23, 2014).

[25] Fight cybercrime in Europe, *Id.* at 16-17.

[26] *Id.* at 21 & 22.

[27] *Id.* at 27–38.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

In Oct. 2012, the report on Fighting cybercrime and protecting privacy in the cloud requested by the EP's Committee on Civil Liberties, Justice and Home Affairs pointed out many "new" challenges to EU's legal framework and policy making. In general, this includes the underestimation of privacy invasion in a cloud context, the controversial roles of different EU institutions in fighting cybercrimes such as EUROPOL, European Network and Information Security Agency (ENISA) and the newly-established European Cyber Crime Centre (EC3), lack of clear sense of direction, priorities and practical coordination in relation to cybercrime, and weak protection of consumers' rights, Cybersecurity in cloud context, harmonization of Member State laws, and the jurisdiction issue. This also includes concrete issues ranging from conceptual uncertainties relating to the wide discretion by Member States, to definitional dilemma regarding the concepts of Cybersecurity, Cybercrime and adequate protection, to contractual to self-regulatory data protection regimes when assessing data transferred to third countries, and to the overestimation of cybercrime.[28] The Report also reviewed that, at the moment of 2012, Data Protection Directive (DPD) and the Proposal for a General Data Protection Regulation (PGDPR) did not apply to law enforcement activities, nor to domestic processing under notational regulatory systems in different areas of law with cloud computing involved; neither are the Framework Decision (DPFD) and the Proposal for a Police and Criminal Justice Data Protection Directive (PPCJDD) applicable to cloud computing providers and EU home Affairs Agencies like EUROPOL. [29]

The report proposed to address these loopholes with the following measures. First, general priorities shall be given to cloud computing related privacy protection and cybercrimes so that data protection offences be recognized a type of Cybercrime; secondly, it suggested the harmonization of fundamental legal concepts of jurisdiction, data processor and data controller at EU level; third, the scope of data protection shall be extended, including the application of the safe harbour principle to telecommunication common carriers providing cloud computing services, the effective use of Mutual Leal Assistance Treaties (MLAT) between the EU and Third countries regarding access to personal data for national security and law enforcement uses, and the oversight over EUROPOL's data exchange activities due to the fact of its becoming a data controller itself. [30] More importantly, the report strongly

[28] Fighting cybercrime crime and protecting privacy in cloud.

[29] Id., 35-46.

[30] Id., 46-48.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

proposed the EU ownership over data and close attention to be paid to U.S. laws that authorizes the surveillance of Cloud data of non-U.S. residents.[31]

Since the publication of the report, the situation has been changed and many of the problems singled out in the report have been improved more or less. In September 2012, the European Commission adopted a strategy for "Unleashing the Potential of Cloud Computing in Europe". Based on an analysis of the overall policy, regulatory and technology landscapes and a wide consultation with stakeholders, the strategy identifies ways to maximise the potential offered by the cloud and sets out the most important and urgent additional actions. It presents a political commitment of the Commission with three key action areas, namely, cutting through the jungle of different standards, identifying safe and fair contract terms and conditions, establishing a European Cloud Partnership (ECP). These works have been under substantial development like setting up expert groups or institutions to work on the three issues in the context of establishing a European digital single market.[32] However, other significant problems still exist to be solved in the near future, in particular in view of the impacts of cloud computing on law and policy making fields.

Hellemans' recent report offers the overview of such problems of EU's cloud computing policies and laws in two perspectives.[33] The first concerns the challenges to the public sector including public procurement legislation related issues that hinder the use of cloud computing service. These problems may be partially addressed by a new Public Procurement Directives (adopted in Jan. 2014, to be implemented by Apr. 2016), but may lead to potential fragmentation again.[34] Other specific public domain services problem concerns various matters ranging from languages, to archiving laws, to national defence and state secrets, criminal and fiscal procedural laws, fiscal and bookkeeping, and

[31] Id., 48. In particular to the USA PATRIOT ACT (S.215) and FISSA (Foreign Information Service

[32] For example the issuance of the Cloud Service Level Agreement Standardization Guidelines by the European Commission. See: For other substantial works in the three key areas, see: THE EUROPEAN CLOUD STRATEGY DIGITAL AGENDA FOR EUROPE, ec.europa.eu//digital-agenda/en/news/european-cloud-strategy-0 (last visited Aug 29, 2014).

[33] LIESBETH HELLEMANS, CLOUD FOR EUROPE: STUDY ON THE LEGAL IMPLICATIONS OF CLOUD COMPUTING (KU Leuven) (2014), http://www.cloudforeurope.eu/news/-/blogs/study-on-the-legal-implications-of-cloud-computing (last visited Aug 29, 2014).

[34] *Id.* at 32–34.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

medical law, with more specific problems aroused in the context of using cloud computing for public service.[35]

Other challenges and legal or policy gaps regarding the private sector cloud computing services in general cover a much broader scope. This includes the problems of applicable law when in absence of a contractual agreement, dispute resolution and jurisdiction, Data protection (i.e. the general application of data protection legislation to cloud data, scattered European framework on data protection, sensitive data, qualification of various actors), liability and accountability problem,[36] contractual problems,[37] data portability, government access to cloud data weather via legal approach or as intelligence surveillance.[38] Other problems seriously enough to be paid attention to or addressed by regulators are net neutrality in the context of cloud services, copyright, interoperability and portability of cloud services, and international transfers, as listed in BEUC's report on cloud computing.[39]

[35] *Id.* at 35–40.

[36] For a more detailed discussion of accountability problem under the new proposal of General Data Protection Regulation, see a discussion by: W. KUAN HON ET AL., CLOUD ACCOUNTABILITY: THE LIKELY IMPACT OF THE PROPOSED EU DATA PROTECTION REGULATION (Social Science Research Network) (2014), http://papers.ssrn.com/abstract=2405971 (last visited Aug 27, 2014).

[37] Except the author's discussion, more discussion on cloud computing unfair contract terms can be found in BEUC's recent report issued in May 2014.

[38] HELLEMANS at 14–30

[39] BEUC CONTRIBUTION TO THE EUROPEAN COMMISSION'S EXPERT GROUP ON CLOUD COMPUTING CONTRACTS- UNFAIR CONTRACT TERMS IN CLOUD COMPUTING SERVICE CONTRACTS DISCUSSION PAPER (2014), http://www.beuc.org/publications/beuc-x-2014-034_are_ec_expert_group_on_cloud_computing_contracts.pdf. (last visited Aug 29, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

3. The political perspective: building trust

3.1. Mass(ive) surveillance

An analysis of the gap of EU's Internet Governance (IG) policies and laws at this critical moment of time cannot and shall not avoid mentioning Snowden's big revelations and the problems that have been pointed out in so many aspects by the follow up investigations on the issued called upon by the Parliament.[40] If such problems are not to be solved in a short term, they have to be paid sufficient attention in future policy-law making processes and political-diplomatic decisions.

The disclosed mass surveillance both by the U.S. intelligence agency NSA and the European ones indicates the blurring of many boundaries or fine lines that had been drawn for protection of individuals before, or at least seemingly as such regarded by the public. This includes the transfer, both inside and outside the EU, from targeted surveillance to mass surveillance that is enabled by new technologies, from national security to cyber security, from intelligence activities to law enforcement activities, from mere state intelligence activities to a mixture of activities of both state intelligence agencies and private companies possessing large quantity of data collected in commercial activities, and from domestic interception to foreign interception due to data exchange between intelligence services. The changes in these aspects have endangered the legal and political framework developed in the pre-digital era.

The first big gap or problem of the present legal framework is the lack of protection and remedy of the large scale violations of fundamental rights to private life, dignity and personal data under EU law.[41] This gap is fundamental according to the claim of Privacy International to the Strasbourg Court in July 2013.[42] The protection of EU citizens' and residents' data transferred to the U.S. or other third countries is not guaranteed as judging from the present situation in that such data are not treated equally as their own citizens' in the U.S.[43] Moreover, even the data collected and transferred from Member States to the UK

[40] Didier Bigo et al., *National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law*, (2013), http://dare.uva.nl/record/496718 (last visited Aug 24, 2014).

[41] Article 8 of the ECHR (right to respect for private and family life, home and correspondence), Articles 7 and 8 of the Charter of Fundamental Rights (respect for private and family life, right to data protection), and in specific Directive 95/46/EC and Convention 108.

[42] PRIVACY INTERNATIONAL SUBMISSION TO THE INVESTIGATORY POWERS TRIBUNAL-STATEMENT OF GROUNDS 45, https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy_international_ipt_grounds.pdf (last visited Sep 3, 2014).

[43] Bigo et al. at 9. Though recently

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

for intelligence use purpose also cannot be protected equally as these of UK citizens.[44] It is clear that though the national security issue is not under the authority of the European Union, it has the legal duty to protect the fundamental rights as such and there must be a solution found under the present circumstances.

Second, there is short of minimum democratic rule of law standards regarding mass surveillance conducted as foreseen in Member States' constitutional systems, of which a key element is the effective judicial control and supervision of executive or governmental actions under the guise of national security. In particular there is need of transparency, predictability, foreseeability and accountability in intelligence works regarding cyber-mass surveillance. What's also challenged are the mutual trust and sincere cooperation among Member States, as well as the security of the Union as a whole,[45] which shall be repaired or remedied in the future through policy/law making and strict law implementation.

Third, as addressed in other contexts of this report, processing and sharing data by EU home Affair agencies such as Europol, INTCEN (Intelligence Analysis Centre), Eurojust, etc. may need to have a more transparent and oversight mechanism.[46]

Fourth, though there are already bilateral agreements between the EU and the U.S. regarding data transfer in the law enforcement sector and national security and intelligence sectors, whether such standards and procedures have been seriously taken or followed is problematic judging from a series of recent revelations.[47] In view of the uneven privacy protection between the EU offering protection regardless of nationalities, and others only of their own citizens, it seems that "a digital bill of rights concerning all data subjects" is a necessity in the future,[48] if feasible.

[44] *Id.* at 35–36.

[45] *Id.* at 35.

[46] *Id.* at 37–38.

[47] Bigo et al.

[48] *Id.* at 9.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

3.2. Cyber security

Cyber security often refers to cyber crime, cyber espionage, and cyber war.[49] Nowadays, cyber security has been one of the priorities of EU politicians and IT experts due to the nature the borderless Internet. The recent large-scale cyber-attack against the Non-Profit Organisation Spamhaus, was the biggest Distributed Denial of Service (DDoS) attack in internet history, caused noticeable delays for internet users, primarily in the UK, Germany and other parts of Western Europe.[50] Cyber-attacks could be backed by nation states, as seen in the mutual accusations between China and the U.S. of cyber-spying,[51] and can be organized by Mafia or hackers, both at different scales, causing economic loss and other damages. With data economy and information society gradually becoming the ordinary life of Europeans, cybercrimes and cyber-attacks can lead to considerable damages due to the technology developments and increasing penetration of the Internet and Telecommunications networks in the EU. The EU authority has to act in multiple aspects to confront the reality judging from the status quo according to the recent studies.[52]

According to Silva's study, there are a couple of problems with EU's fragmented cyber security approach.[53] First of all, at the EU level, there is no consensus in terminology of cyber security and Member States have different approaches so that the phrase can be used for multiple and

[49] *European Cyber Security Policy within a Global Multistakeholder Structure*, 18 EUROPEAN FOREIGN AFFAIRS REVIEW 155–180, 158 (2013), http://www.kluwerlawonline.com/abstract.php?area=Journals&id=EERR2013011 (last visited Sep 6, 2014).

[50] EU AGENCY ENISA: INTERNET SERVICE PROVIDERS FAIL TO APPLY FILTERS AGAINST BIG CYBER ATTACKS, http://www.enisa.europa.eu/media/press-releases/eu-agency-enisa-internet-service-providers-fail-to-apply-filters-against-big-cyber-attacks (last visited Aug 21, 2014).

[51] Associated, *China demands halt to "unscrupulous" US cyber-spying*, THE GUARDIAN, May 27, 2014, http://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying (last visited Aug 21, 2014).

[52] For a brief review of EU's cyber security policies and strategies, see: DUNN CAVELTY & MYRIAM, A RESILIENT EUROPE FOR AN OPEN, SAFE AND SECURE CYBERSPACE 4–5 (Social Science Research Network) (2013), http://papers.ssrn.com/abstract=2368223 (last visited Sep 6, 2014). Also refer to Bendiek and Porter's work on the Emerging European security structure in the context of national, international and transnational and private actors: Andrew Porter & Annegret Bendiek, *European Cyber Security Policy within a Global Multistakeholder Structure*, 18 EUROPEAN FOREIGN AFFAIRS REVIEW 155–180, 163–177 (2013), http://www.kluwerlawonline.com/abstract.php?area=Journals&id=EERR2013011 (last visited Sep 6, 2014).

[53] Europe's xx.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

indiscriminate purposes when defined broadly.[54] The newly launched cyber security Strategy for the EU prescribes no clear definition and does not have such demands for Member States to harmonize policies.

Second, while the borderless character of the internet requires a consistent approach across the Union, the overall EU cyber security status is fragmented in the sense that heterogeneous cyber security policies and unequal levels of protection coexist inside the EU.[55]

Third, as ENISA's analysis showed, market regulation or self-regulation failed in implementing cyber security standards that have been around for almost 13 years; and this is the context where the EU authority shall act with much stronger measures. A good policy balance has to be maintained between the differences between cyber security related private sectors who used to "advertising" dangers, and others including ISPs, mobile operators and ICT equipment manufacturers who are against stricter regulations.

Furthermore, it is needed for EU's cyber security policy to be more user-driven safety approach and pro-fundamental rights, while the present policy focus is still on national defence. Although the cyber security policy must be made by shared values including respect for fundamental rights, this point hardly affects the EU's security policies and programs; it neglects to develop in parallel a compressive framework for the protection of fundamental, informational rights of citizens against invasive government policies.[56]

Another concern regarding the civil society's participation of cyber security issues, which is dominated by the state or EU authority, is confirmed by the Commission's observation in its most recent report on the implementation of the Internal security strategy. The Commission has recognized it as a guiding principle to carry out the citizen-centred approach for EU internal security and for the challenges that lie ahead.[57]

---

[54] Europe's fragmented approach towards cyber security, p. 3.

[55] Id., p. 3

[56] Porter & Bendiek at 175

[57] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL THE FINAL IMPLEMENTATION REPORT OF THE EU INTERNAL SECURITY STRATEGY 2010-2014, http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20140365.do (last visited Aug 21, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Most recently, the new legislations on Cyber security, namely the *Cybersecurity strategy* and the *Proposal for a Directive of the European Parliament and of the Council Concerning Measures to ensure a high common level of network and information across the Union* have attracted criticisms. One of them is that the EU's cyber security strategy should be extended to cover malicious state behaviour and to strengthen IT security and resilience of IT systems.[58] Manuel David Masseno commented that "this is not a consolidation of the *acquis*, but only a residual regulation for some sectors not covered before," with many micro issues left unregulated. He mentioned issues in the Directive like regulation of electronic signatures and certification-service-providers (Art. 1.3), the regulation of critical infrastructures (Art. 1.2), regulation of personal data protection (though mentioned in Article 17 regarding a security incident involving personal data).[59]

Problems in other areas exist and need to be tackled while seeing from regulatory governance perspective according to Bendiek and Porter's research.[60] For instance, the distinct separation between domestic and foreign policy in European security policy compromises the EU's ability to respond to cyber attacks.[61] Yet another problem is that while more private firms are involved and responsible for large amounts of critical infrastructures in energy, health, transportation, etc., they lack the technical know-how to identify and guard against cyber threats.[62] Last, there is no systematic, quantitative scheme to detect and disseminate information about cyber security threats,[63] the present risk assessment methodologies are fundamentally flawed in the context of complex networks and complex risks,[64] and the reluctance to cooperate in sharing information of the national states and bend to a

[58] EU APPROACH TO CYBER-SECURITY EUROPEAN PARLIAMENTARY RESEARCH SERVICE, http://epthinktank.eu/2014/04/02/eu-approach-to-cyber-security/ (last visited Aug 21, 2014).

[59] COUNCIL OF THE EUROPEAN UNION, 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) – PARTIAL GENERAL APPROACH ON CHAPTER V (2014), http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT. (last visited Aug 31, 2014).

[60] Porter & Bendiek

[61] *Id.* at 156.

[62] *Id.* at 157.

[63] *Id.* at 157.

[64] CAVELTY & MYRIAM at 5.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

regulative power at the EU level such as ENISA (European Network and Information Security Agency) which has no binding power.[65]

[65] EUROPE CYBER SECURITY POLICY UNDER ATTACK NEWS, http://www.sbs.com.au/news/article/2014/05/05/europe-cyber-security-policy-under-attack (last visited Sep 6, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

4. The legal perspective: international transfer of personal data and exterritorial jurisdiction

4.1. International transfer of personal data

Transborder information flows are an inherent element of today's globalised and interconnected world.[66] The proposed Data Protection Reform Package (DPRP), including the General Data Protection Regulation and the Directive regulating the criminal Justice and Law enforcement activities, will be promulgated in the near future after the EP's approval in April, in view of the present strong support among the European politicians against the backdrops of the disclosure of cross border mass surveillance not long ago.[67] This will largely impact the legal regime of international data transfer and sharing in private sector.

The regulation on the whole gives positive permission to data transfer to third countries and international organizations given that several enumerated conditions are to be met.[68] According to EDRi's position paper, however, the essential safeguards to protect personal data under the general principle of Article 40 are "not sufficiently specific", thus creating serious risks of their "misrepresentation, circumvention or other abuses".[69] This echoes Costa and Poullet's study that besides the adequacy decision as the primary method of undertaking international data transfers, new modalities of transfers – including under the Regulation Binding Corporate Rules (BCR), standard data protection clauses adopted by the Commission or the supervisory authority, and contractual clauses between controllers and processors and the recipient of the data authorized by a supervisory authority – imply much flexibility and uncertainty in the new data transfer regime that is in favour of free

[66] COUNCIL OF THE EUROPEAN UNION, 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) – PARTIAL GENERAL APPROACH ON CHAPTER V 1 (2014), http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT. (last visited Aug 31, 2014).

[67] EUROPA - PRESS RELEASES - PRESS RELEASE - PROGRESS ON EU DATA PROTECTION REFORM NOW IRREVERSIBLE FOLLOWING EUROPEAN PARLIAMENT VOTE, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (last visited Sep 1, 2014).

[68] Luiz Costa & Yves Poullet, *Privacy and the regulation of 2012*, 28 COMPUTER LAW & SECURITY REVIEW 254–262, 261 (2012), http://www.sciencedirect.com/science/article/pii/S0267364912000672 (last visited Aug 31, 2014).

[69] POSITION ON THE REGULATION 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) 22, http://edri.org/files/1012EDRi_full_position.pdf. (last visited Aug 31, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

movement of data,[70] in contrast to the previous principle under Directive 95/46 prohibiting cross border data transfer to third countries.

The wordings of derogations (Article 44) prescribed by the Regulation are problematic according to EDRi's recent position report.[71] For instance, the definition of "public interests" in Article 44 (1) (d) is too broad, in particular while being read with Recital 87,[72] and similarly the concept of "legitimate interests" of Article 44 (1) (h) as a legal ground for data processing is open for interpretation. Article 44 (1) (h) is a big concern here due to the open possibilities created by this clause for transferring data to third countries. The term "Consent" prescribed in Article 44 (1) (a) may also lead to future problems in data transfer. At its present state, it means that without an adequacy decision or any of the four alternative modalities set out in the regulation, controllers and processors can still "legitimate and sign off data transfers", since it is sufficient to obtain the consent of data subjects when parties have unbalanced powers. This means that the Regulation "opens the possibility to ground the legitimacy of a data transfer exclusively on consent, even without safeguards".[73] Such case is also likely to happen to

[70] Costa & Poullet at 261–262.

[71] European Digital Rights at 23–24

[72] "…for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters or for public health , or to competent public authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. Transferring personal data for such important grounds of public interest should only be used for occasional transfers. In each and every case, a careful assessment of all circumstances of the transfer should be carried out." THE EUROPEAN PARLIAMENT, REPORT ON THE 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) - A7-0402/2013 (2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN (last visited Aug 31, 2014).

[73] Costa & Poullet at 262. Though the Regulation text the authors analysed changed in the most recent report of the Council, their analysis stands in general in the context of Article 7.4 of the Regulation preventing "consent" to be made between significantly imbalanced data subjects and controllers.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

the European Data Protection Seal (Article 39) exempting data controllers from "having to obtain authorisation before transferring data to third countries".[74]

The drafted Regulation in the present version does address the challenge of data transfer to third countries by virtue of extra-territorial laws, regulations and other legislative instruments, including for the purpose of law enforcement based on Article 43(a). This Article was added by during the Parliament reading for the purpose of restoring the Article 42 in the previous draft proposal before December 2011 that was taken out for unknown reasons. The old Article 42 was partially designed to provide some safeguard or defence to EU-based controllers of personal data, [75] which were upon requested to transfer personal data to a third non-EU country requested by law enforcement agencies or according to Mutual Legal Assistance Treaty (MLAT) or an international law agreement between this country and a Member State, but regards such requests as against the proposed Regulation.

But the problem is not changed since if the involved data supervisory authority refuses such a transfer, it is therefore again in the hands of a data controller or a processor to decide which law to follow, which means that it is trapped in a dilemma that is only to be solved by political efforts of both parties. Besides, if the data supervisory authority allows such a transfer, then how can it further ensure that the transferred data would not be used later for other purposes against the EU law?

With respect to the proposed Directive in the Data Protection Package regarding data sharing and transfer for the law enforcement sector (LES), it is unlikely that the Directive would be very much successful in the future. First, as the most recent report on the Rec(87) 15 indicated, "by and large the Recommendation has been widely adopted across Europe to an extent that many European states prima facie already regulate police use of personal data in a way comparable but not necessarily identical to that envisaged in the current draft of the European Commission's proposal"; and this finding does not show the urgent need for action on this sector.[76] Even if there is such a need, the problem is that, due to the blurring lines of data processing for criminal justice purposes and for national security

[74] THE EUROPEAN PARLIAMENT, REPORT ON THE 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) - A7-0402/2013 (2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN (last visited Aug 31, 2014).

[75] Discussion paper, pp. 24.

[76] 25 years on, p 2 & 32.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

and intelligence purposes, Member States may still argue that national security falls into the sole responsibility of Member States according to Article 4 (2) of the Treaty of the European Union, despite that in the first instance there is no agreement on the right type of legal instrument.[77] But though there is the procedural difficulty, the Parliament has passed both proposals with amendments, and it is the time to see what would be the next move with the Council.

While an international treaty establishing certain agreed standards of data protection is at present not feasible,[78] though scholars may have strongly suggested and probed into the possibility, the cross-border data transfer seems to be trapped in the conflicts of state interests in particular regarding state security and political divergences, and economic interests, not even mentioning the cultural divergences in approaching the concept of privacy.[79] Such conflicts and divergences make it impossible to draw common ground for mutual trust in the previous efforts between the EU and the U.S., which is very much well seen in FRA's recent report by FRA (Fundamental Rights Agency), following a call by the Parliamentary Resolution of 12 March 2014.[80]

In this report,[81] it is recommended to consider the large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour which does not per se meet the criteria for derogation under national security, and such transfer under it shall be carried out under other instruments, such as contractual clauses or BCRs setting out specific safeguards, as well as suspending Commission Decision 520/2000 admitting the adequacy of the Safe Harbour privacy principles. This position on the adequacy

[77] Joe, discussion paper, p. 21 & 24.

[78] See: PARALLEL INTERNETS, ANOTHER INTERNET TREATY OR BOTH? THE NEXT PIECES OF THE INTERNET GOVERNANCE JIGSAW PUZZLE - PART 1., http://www.mappingtheinternet.eu/node/41 (last visited Sep 1, 2014).

[79] See in general a discussion by Whitman. J. Q. Whitman, *Two Western Cultures of Privacy: Dignity versus Liberty, The*, 113 YALE LJ 1151 (2003), http://www.yalelawjournal.org/pdf/113-6/WhitmanFINAL.pdf (last visited Sep 5, 2012).

[80] EUROPEAN PARLIAMENT RESOLUTION OF 12 MARCH 2014 ON THE US NSA SURVEILLANCE PROGRAMME, SURVEILLANCE BODIES IN VARIOUS MEMBER STATES AND THEIR IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS AND ON TRANSATLANTIC COOPERATION IN JUSTICE AND HOME AFFAIRS (2013/2188(INI)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230 (last visited Sep 2, 2014).

[81] AD HOC INFORMATION REQUEST: NATIONAL INTELLIGENCE AUTHORITIES AND SURVEILLANCE IN THE EU: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES – GUIDELINES FOR FRANET ON WHICH INFORMATION TO COLLECT FOR MEMBER STATES 20–21 (2014), http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and (last visited Sep 2, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

of Safe Harbour Rules has been under severe scrutiny of the Court of Justice of the European Union in Case C - 362/14 *Maximillian Schrems v Data Protection Commissioner* decided on 6th October 2015. In its judgment, the Court of Justice held that the Commission's US Safe Harbour Decision is invalid.

4.2. Exterritorial jurisdiction

The International Law Commission of the United States defines the concept of extraterritorial jurisdiction as an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law. [82] At present, the EU law's exterritorial jurisdiction is mainly prescribed by the Direct 95/46/EC in particular Article 4. According to a report of Working Party 29 issued in 2010, possible improvements need to be found in some areas regarding different aspects of the application of Article 4.

Furthermore, the Court of Justice of the European Union, in its decision in Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* decided on 1st October 2015 has started addressing some of the difficulties of Article 4 of Directive 95/46/EC.

[82] ILC Report (n49), Annex E, para. 2.2, cf: Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY eaq004, 227 (2010).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

5. EU's present internet governance strategies

5.1. Pre-emptive regulation v. rule of law

This is even more obvious when we look at EU's role in promoting the Digital Single market. The policy deficiencies in EU's telecommunications may not all be matching EU's Internet polices, but at least be, with some symbolic significance, helping with understanding similar patterns in other fields of Internet Governance. According to Savin, there are several policy deficiencies in the digital single market context.[83] First, the European internet policy making is replete with the relatively non-assertive preambles and lacks of a proper empirical basis. It shall make more efforts in gaining good evidences and proper empirical basis for its policy makings, as such observed recently in public calls for Copy right Directive Reform from 2008, 2010 and 2013, as well as the article 39 of the 2013 Connected Continent. At this point, the Global Internet Policy Observatory (GIPO) aiming at creating an online platform to improve knowledge of and participation of all stakeholders across the world in debates and decisions on internet policies" is an important initiative in this direction with potential significant impact on EU Internet law making. [84]

Second, according to Savin, the EU shall be cautious with its fast steps in harmonizing its internet policies. It should keep writing technology-neutral laws and should stick to minimum rather than full harmonization, which "antagonises Member States and increases resistance". [85] Third, the single market approach, when confronting real boundaries and realities of cultural, political, social, economic and linguistic differences, must consider the limit to what legal intervention can achieve.[86] What is more practical and realistic is a more long-term focus on innovation and knowledge in general rather than a single market, when the EU is lagged behind the U.S. and Japan. Third, it is important that the EU shall make original policies when dealing with Internet regulatory problems than just following the traditional examples set by the U.S. politics and internationally binding documents such as the TRIPS agreement and Berne Convention.[87] The most recent EU's declaration of trying to be the honest broker of the

[83] How Europe formulate, p. 7.

[84] Ibid.

[85] Ibid.

[86] Idid

[87] Ibid.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Internet Governance is the positive signal.[88] Last, the EU must in its policy making process bear in mind the convergence of IT, media and telecommunications services, and the possible merging of carrier and content regulatory policies.[89] It would be very difficult to put, take the U.S. and the EU for example, the legal protection of personal data and privacy in both countries at even roughly near level, because of the impossibility of modifying "the Privacy Act and Either a Constitutional Amendment or the overturning of several Supreme Court precedents", when with the so-called "home-field advantage" in hands.[90]

5.2. The privatization of Internet Governance

A number of authors claim that there seems to be a move toward 'privatization' of Internet governance. The arguably 'delegated' power by the Court of Justice of the European Union to Google to decide on which claims to delete links to honour and which not is one example given for this move towards privatisation. Another, often quoted, example of privatization relates to increasing expectation from Internet service providers (ISPs) to 'police' the Internet and to assist law enforcement agencies at all times.[91] This is one more area that needs to be watched closely and further investigated during the course of the MAPPING project.

[88] Commission to pursue role as honest broker in future global negotiations on Internet Governance.

[89] How Europe formulates, p. 8.

[90] Ian Brown, *The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance*, AVAILABLE AT SSRN 2433912 , 8 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2433912 (last visited Sep 1, 2014).

[91] Europe's fragmented approach towards cyber security, p. 5.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

6. EU Data protection laws and remedies

Data protection is one of the fundamental pillars of the new information age because if personal data are not to be well protected, our society will not benefit as a whole from the recent developments of new Internet-related technologies when information will all be digitized and super-connected. If personal data would be used largely against our fundamental rights to privacy, family life, dignity and reputation for the purposes of other collective interests such as state security and public order in inappropriate ways, the application of such new technologies would be under doubts and impeded due to the untamed potential harms. In addition, personal data play an increasingly important role in people's life especially in view of the forthcoming of the big data age in which massively collected personal data is supposed to be analysed for improving human life.

6.1. The legal base of the right to personal data protection

The right to effective remedies is in a sense based on the fundamental right to personal data protection recognized by EU basic laws. Article 8 of the Charter established this right as a fundamental right distinguished from the right to private life. This article prescribes that "Everyone has the right to the protection of personal data concerning him or her." and "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." This right has its base or origin in Article 16 of the Treaty on the Functioning of the European Union, the 1995 Data Protection Directive, Article 8 of the ECHR,[92] and the Convention 108 (the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) which has been ratified by all EU Member states. It is also worth mentioning the Directive 2002/58/EC regrind the processing of personal data and the protection of privacy in the electronic communications sector (or the E-privacy

[92] ECtHR in its case law interpreted this as a right encompassed in Article 8 of the ECHR and found in the same Article both negative and positive obligations of Member states. See X and Y v. Netherlands, Judgment of 26 March 1985, para 23. In a series of case laws, ECtHR defines the scope of this fundamental right. See a discussion by FRA at: Data protection in the European Union: the role of National Data protection Authorities, at: DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES (STRENGTHENING THE FUNDAMENTAL RIGHTS ARCHITECTURE IN THE EU II), http://fra.europa.eu/en/publication/2012/data-protection-european-union-role-national-data-protection-authorities (last visited Jun 24, 2014), pp. 12-13.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Directive amended in 2009),[93] harmonizing the different national provisions on the protection of the right to privacy and complementing Directive 95/46/EC.

The right to personal data protection has been better protected via a couple of legal measures regarding the treatment of such data by the EU institutions and agents, including Article 16 of the Treaty on the Functioning of the European Union, Regulation (EC) No 45/2001 of the European Parliament and of the Council of the 18 December 2000, with the establishment of the European Data Protection Supervisor (EDPS) and internal Data Protection Officer (DPOs).[94] Furthermore, Directive 2006/24/EC, though challenged by the recent Google v. Spain judgment of ECJ,[95] addresses the retention of data in publicly available electronic communications services and public communications networks. The impacts of the new ECJ decision shall be observed in the near future at national law levels of the Member States. Last, the Lisbon Treaty recognizes that the right to personal data protection of Charter of Fundamental Rights has binding legal power and shall be an autonomous fundamental right with full legal validity, rather than merely being formal and symbolic declaration.[96]

Another important part of personal data protection concerns the law enforcement activities using collected personal data in various ways and having serious influences on individual lives. In the first instance regarding the Council of Europe, three legal documents regulate the use of personal data for law enforcement and protect personal data from abuse and misuse. Convention 108 covers in general all fields of processing personal data and applies to data protection regarding police work and criminal justice albeit with limitation from the Contracting states. Also the ECtHR holds coherent opinion that "storing and retention of personal data by police or national security authorities constitutes an

[93] See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML . Amendment available at: http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2009%3A337%3A0011%3A0036%3Aen%3APDF&ei=q8-_U_S3Ls3KOf34gPAB&usg=AFQjCNGf_v3QrBBKdVbK5M2FWCzdTKYrUQ&sig2=JlFWNlYO9GkVpd_2ZS3u_A&bvm=bv.70810081,d.ZWU

[94] For a more detailed discussion, refer to FRA's report on DPAs; ibid.

[95] Court verdict available at: http://www.scribd.com/doc/216980523/Judgment-of-the-ECJ-in-Digital-Rights-Ireland-data-retention-challenge

[96] Data protection in the European Union, pp. 18.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

interference with Article 8(1) of the ECHR".[97] The CoE Police Recommendation (Recommendation No.R(87)15) is an important legal document, though non-binding, providing guidelines for law enforcement practices in the use of personal data by law enforcement agencies (LEAs).[98]

The CoE Convention on Cybercrime offers protection of personal data that can be violated by criminal activities and prescribes Contracting States to assure adequate protection of the data protection right among other rights protected by the ECHR.[99] A 1995 Recommendation for data protection regarding telecommunication limits the purposes of collecting and processing personal data to what's necessary for service providing, relating to network connection, billing, verifying, ensuring optimal technical operation and developing the network and service. Further, under the general principles of Convention 108 different CoE recommendations propose guidance on personal data protection in areas of employment, medical data, financial data and statistical data.[100]

At the EU level, data protection in law enforcement is only regulated when cross border cooperation of police and judicial authorities is involved, and the DPD does not apply in this area. The Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Data Protection Framework Decision), relying on Convention 108 and DPD, prescribes the duties of receiving Member States in data processing and the legal rights of data subjects, in particular their right of access, rectification, erasure or blocking.[101] Besides, there are more legal instruments on data protection regarding police and law-enforcement, as well as other cross border cooperation activities. This includes the Council Framework Decision 2009/315/JHA, Council Decision 2008/615/HJA (the Prum Decision), and the data protection regime

[97] Philippe Boillat & Morten Kaerum, Handbook on European data protection law (Publications Office of European Union Belgium) (2014), http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (last visited May 8, 2014), p. 144. For example: Leander v. Sweden, No. 9248/81, 26 March 1987; M.M. v. the United Kingdom, No. 24029/07, 13 November 2012; M.K. v. France, No. 19522/09, 18 April 2013. Id., p. 145.

[98] For the evaluation of the Recommendation, see a recent evaluation report by

[99] Data Protection Handbook, pl 157.

[100] As such in turn: Recommendation Rec(89)2 to member states on the protection of personal data used for employment purposes, Recommendation Rec(97)5 to member states on the protection of medical data, Recommendation Rec(90)19 on the protection of personal data used for payment and other related operations, Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes.

[101] Data Protection Framework Decision.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

governing Europol Information System and Eurojust Data Protection Rules, as well as data protection measure regarding the Schengen Information System, the Visa Information System, Eurodac (a centralized system containing the fingerprint data of third country national applying for asylum in the EU Member States), Eurosur (the European Border Surveillance System) and Customs Information System (CIS).

In other specific areas, the E-privacy Directive (Amended in 2009) differentiates three kinds of data regarding telecommunications and prescribes their related protection and conditions for processing; amendments include setting restrictions on sending emails for market purposes, prescribing obligations for Member States to provide judicial remedies, and forbidding use of cookies unless with consent. Regarding employment data, DPD only concerns sensitive personal data.[102] Medical data is regarded as sensitive data according to Article 8(1) of the DPD and their possible uses are prescribed in Article 8(3) in certain restricted contexts and related conditions such as "preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services". Regarding collected data for statistical use, Article 6(1) of the DPD allows the waiver of purpose limitation with necessary safeguard laid down, and Article 13(2) allows for limitations of access rights by national law under certain conditions. For official statistics, Regulation (EC) No. 223/2009 on European statistics (European Statistics Regulation) contains important rules for data protection. There are a bunch of legal measures for regulating data protection regarding personal financial status and cross border payment, or "regulating markets in financial instruments and the activities of credit institutions and investment firms".

One important issue regarding data protection laws and policies is the data protection in the context of video surveillance increasingly used for purposes like public security, private safety, and surveillance of workers at work locations. The DPD has not detailed guidance for video surveillance which falls within its scope of personal data defined by Article 2. Article 33 singled out this issue of interest "The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society." Regarding the use of CCTV, the EDPS issued the video-surveillance Guidelines offering practical guidelines to the European Union institutions and bodies to comply with the Regulation 45/2001 on the protection of personal data by Community institutions and bodies with effective safeguards in place. Besides this general clause, regulation of CCTV is generally a country-by-

[102] in particular ARticle 8(2) of the Directive.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

country issue, due to the lack of standardized criterion at the EU level, so that FRA suggested "a separate EU legislative measure ought to be considered in the future", while taking into account of "the intrinsic technical particularities of sound and image data, as well as the wide-ranging potential impact on individuals' rights".[103]

6.2. The right to an effective remedy

As FRA pointed out, the right to effective remedies is guaranteed by two important legal treatises. Article 47(1) of the EU Charter (The Charter of Fundamental Rights of the European Union) prescribes that "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this article." Article 13 of the European Convention on Human Rights (ECHR) ensures that everyone shall have an effective remedy "before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity".[104]

This is further explained by ECtHR as providing "a means whereby individual can obtain relief at national level for violation of their Convention rights before having to set in motion the international machinery of complaint before the Court".[105] And this right is further guaranteed by the procedural right to "a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law", prescribed by Article 6 of the ECHR.[106] Both Article 47 of the EU Charter and Article 13 of the Convention are more interpreted broadly to include not only judicial remedy, but also other remedy mechanisms.[107] In particular ECtHR interpret the word "the national authority" in Article 13 as not necessarily to be "a judicial authority in the strict sense".[108]

[103] DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES (STRENGTHENING THE FUNDAMENTAL RIGHTS ARCHITECTURE IN THE EU II), http://fra.europa.eu/en/publication/2012/data-protection-european-union-role-national-data-protection-authorities (last visited Jun 24, 2014), p. 46.

[104] Presidium of the convention.

[105] ECtHR, Kudla v. Poland, no. 302010/96, 26 October 2000. Also reiterated in the Court's judgment in Lyanova and Aliyeva v. Russia, Nos. 12713/02 and 28440/03, 2 October 2008, para 134.

[106] ECtHR, Kudla v. Poland, No. 30210/96, 26 October 2000, paras,. 146-156.

[107] FRA, Access to data protection remedies in EU member states, p. 16.

[108] ECtHR, Leander V. Sweden, Series A No. 116, 26 March 1987.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Article 22 of DPD prescribes that "Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question". Article 8(d) of Convention 108 allows any person to have a remedy if request for confirmation, communication, rectification, or erasure as referred to in articles b) and c) of the same article is not complied with.[109]

In addition, under the 2008 Data Protection Framework Decision regarding data processed in the context of police and judicial cooperation in criminal matters, data subjects should be "informed of the possibility provided for in national law for lodging a complaint or seeking judicial remedy", given his right of access, rectification, erasure or blocking is refused;[110] and "Without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject shall have the right to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law".[111]

6.3. Responsible remedy institutions and the accompanying problems

The first move of data subjects upon noticing the violation of their data protection right is to exercise their right against data controllers. Data controllers must identify requesters to avoid a serious breach of confidentiality, sometimes required by national law; and the fair processing principle may restrict the overly burdensome conditions for acknowledging identification and the authenticity of the request.[112] Article 12 (a) of the DPD and Article 8 (b) of Convention 108 guarantee that upon requests of data subjects, data controllers must respond timely according to national laws without excessive delay or expense.

[109] Article 8 of the Council 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, available at: http://eur-lex.europa.eu/legalcontent/EN/ALL/;ELX_SESSIONID=mZ2RTFPdMSD01VLjwHLw61nhnzy9v8x55YpB1mw8HRyWKX5TSQ96!570781914?uri=CELEX:32008F0977.

[110] Article 18 of the Council Framework Decision. Ibid.

[111] Article 20 of the Council Framework Decision. Ibid.

[112] Data protection Handbook, p. 120.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Once a requester is not satisfied with the data controllers' response, he or she has several choices for a further remedy, including resorting to a local data protection authority (DPA) or European Data Protection Supervisor (EDPS) given that EU institutions or bodies act as data controllers involved, Intermediaries (such as civil society organisations, Trade Unions etc.), non-judicial bodies and other administrative institutions (such as ombudsman institutions, communication authorities etc.), national courts, and CJEU if certain conditions are to be met.

6.3.1. Non-judicial mechanisms

According to FRA's recent empirical study on access to data protection remedies in EU Member States, non-judicial bodies play a supplementary role on matters such as "providing advices, taking complaints, and providing a valuable addition to the statutory data protection framework".[113] This includes seeking remedy via different forms of ombudsman in Member States. Such a role varies in different Member States from asking DPAs to rectify a mistake, to ordering access to data denied temporality or permanently, to delivering breach of confidence report, to issuing complaints to governmental departments, etc. Other non-judicial bodies have the power from annulling decisions taken by other authorities, to ordering rectification of violations, to granting, denying or deleting information, to revoking a permit or licence of a business violating data protection laws, and to issuing fines for data protection violations, and last to demanding a public or written apology or ordering compensation in form of both pecuniary and non-pecuniary damages.[114]

The Intermediaries, such as civil society organisations or other individual professionals, play a role "in providing advice, guiding and taking complaints, providing a valuable added value to the statutory data protection framework". [115] But there are some issues to be noticed in FRA's reports. First, the number of civil society organisations in the field of data protection is rather low according to FRA's recent finding. Second, though offering assistance in bridging gaps such as providing information and advice to individuals, providing legal assistance or representation, and communicating with governments and other bodies, they have limited resources such as lack of financial resources to cover lawsuits. Last, there shall be more cooperation and coordination with other agents in the area of data protection, including other civil society organizations and DPAs.[116]

[113] Access to Data protection remedies, p. 19.

[114] Access to data protection remedies in EU Member States, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states (last visited Jun 22, 2014), p. 19.

[115] Id., p. 22.

[116] Id., p. 20 & pp. 22-24.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

6.3.2 Data Protection Authorities

According to Article 28 of the DPD, DPAs in different Member States monitor the application and respect of the Directive in Member State with an independent legal status and different financial and human resources. Members States must endow their DPAs with the powers prescribed in Article 28 of the DPD, namely: the power to advise in legislation or regulation procedures regarding personal data protection, the power of investigation, intervention and engagement in legal proceedings, and the power to hear claims. In addition, Article 25 of the DPD regulates the transfer of data to non-EU countries and leaves the potential for the intervention of DPAs.

According to FRA's recent research, DPAs are the first point of contact for victims of data protection violations and therefore of importance in remedying violation of individuals' data protection right.[117] In reality, DPAs in different Member States have powers in securing their directive purposes to various extents allowed by national legislation. According to FRA, half of the Member States allow them to issue warnings or formal objections to the practices of data controllers; all DPAs have the capacity of issuing orders or injunctions to remedy certain types of data protection violations, including ordering the disclosure of information by data controllers, implementing specific security measures, discontinuing an operation, suspending the transfer to a third state, as well as rectifying, erasing or blocking specific data. Substantive action against violations by DPAs in practice also includes measures such as issuing a fine or pecuniary sanction, or revoking licences for processing data. Some DPAs can refer cases to domestic courts or the public prosecutors.[118]

As the first contact point of data protection violation victims, DPAs play a significant role to remedy them with the directive-prescribed powers, albeit such powers are limited or restricted by the different implementation of the DPD at national level. FRA's recent reports have pointed out the multiple needs to strengthen their role in providing instant remedies for the increasing data protection complaints.[119] These policy gaps to be patched to improve their functionalities are:

a) The effective independence of DPAs is under doubt due to normative or practical obstacles. For instance, regarding the nomination of the officers in different Member States and their legal status regarding issues such as retirement or dismissal and confidentiality etc., or the affiliation of the DPAs

[117] Access to data protection remedies in EU Member States, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states (last visited Jun 22, 2014), p. 20.
[118] Access to data protection remedies in EU Member States, pp. 20-21.
[119] Access to data protection remedies in EU Members States, pp. 46-49.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

with other political bodies or which is under doubt in some countries due to the appointment of the governing staff members by political bodies and supervisory institutions, as well as "limited action taken against other public institutions";[120]

b) Lack of human resources especially qualified staff with legal and technical expertise to handle internet-related new technologies and relative laws, as in evidence gathering process, or the right combination of expertise; the situation is even worsened by the problem of lack of financial support from Member States; the shortage of finance and expertise has negative impacts on DPA's role in data protection;

c) Public relations and communications with the complainants are a problem for some DPAS, due to the duration of procedure, timings and clients' desire to have quick response;

d) the uncertainty of the implementation and compliance of DPAs' issued instructions and decisions, in particular when public administrations are involved and complainants won't take cases to court, and pecuniary fines are symbolic against such public institutions; [121]

e) lack of transparency and publicity in DPAs' activities before the public,[122] as well as of a formal procedure of selecting priorities of handling complaints;[123]

f) issues of raising awareness about data protection rights among data subjects not only of the related EU laws and domestic laws, but also DPAs' own role and functions in the data protection mechanism.[124]

FRA's report on the remedy mechanism partially discussed how the above mentioned problems in DPAs' daily works may have been tackled by the Draft General Data Protection Regulation in order to harmonise data protection legislation and strengthen the ability of DPAs to remedy violations. Most of

[120] Access to data protection remedies in EU Member States, p. 46.
[121] Id., pp. 48-49.
[122] Ibid.
[123] Oral communication with Dutch DPA officer Ms. XX expressing that the selection of complaints to be tackled by the Dutch DPA is rather dependent on the head officer's ad hoc decision rather than based on internal procedures that may also recognized by other DPAs. Ms. xx of the German DPA said at the Rome EGA Meeting of the MAPPING that the Germany is at the stage of developing such selective criteria in handling received complaints.
[124] See also Data Protection in Europe Union: the role of data protection authorities, pp. 43-44.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

the problems reflected in FRA's field works have been addressed by the Draft with specific Articles. For example, Article 52(2) of the Draft Regulation prescribes the duty of DPA to promote the awareness of data protection rights and related rules and risks; Article 52 (1) requires DPAs to inform the data subject of the progress of investigation and outcome of the complaint within a reasonable period, in particular in case of the need of further investigation and cooperation with other DPAs is necessary.

Article 53, among other more detailed defined powers, empowers DPAs to bring violations of the Draft Regulation to the notice of judicial authorities and participate in legal proceedings, as well as to sanction administrative offences. But the problem is whether the new Draft Regulation would be adopted by the EU in the near future and how would it be implemented in legal practice remains a major concern of all stakeholders of data protection. Regarding better sanctioning power, Article 79 confers DPAs the power to impose administrative sanctions; they can issue pecuniary fines with significantly increased scope to a maximum of 1,000,000 or 2 % of an enterprise's annual global turnover, although how such fines would be enforced remains for further observation.

Further the Draft Regulation contains special clauses to enhance the cooperation between DPAs to clarify how they may cooperate in supervising and monitoring data processing and data protection as seen in Article 55 of mutual assistance and Article 56 of joint operations. The Draft Regulation also sets up mechanisms to bring different DPAs in line with the Draft Regulation by Article 58 and Article 59 introducing the supervision and control of the Commission and a new institution at EU level called the European Data Protection Board, composed of representatives of DPAs.[125] In particular, though the Draft Regulation approves of the validity of the enforceable measure issued by a DPA that should be enforced in other Members States concerned, Article 63 also prescribes that:

"Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5)", which requires such measures to be communicated to both the European Data Protection Board and the Commission for review, "the measure of the supervisory authority shall not be legally valid and enforceable".

[125] The establishment of European Data Protection Board itself deserves special notice in overseeing the consistency and coordinative operations of DPAs together with the Commission in reviewing of the substantive measures to be taken by and communicated to both institutions whose opinions are crucial for validity of such measures.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

6.3.3 The judiciary's role and its limitations in data protection

The judiciary is in any sense the most important venue to protect and remedy data protection violation, as in the rest of the world. Regarding civil and administrative procedures, most Member States "explicitly recognize the ability to award compensation in the form of damages"; some set out the amount of compensation to be awarded, while others leave it to judges to develop both pecuniary and non-pecuniary damages through case law.[126] Administrative and civil procedures can also lead to orders, depending on jurisdictions, from injunctions, to access to specific data, to rectify, erase or cease data processing, or to notification of relevant third parties of violation or court verdict.[127] Criminal procedures can end up in the issuance of warnings, publication of court judgments, injunctions on data processing by a certain individual, compulsory community service for violation, etc., in addition to imposing fines and prison sentences, or both. [128]

Regarding the judiciary's role in remedying data protection violations in the EU, FRA's field work pointed out three major observations of the judiciary's role in data protection violation remedy. The first observation is that there are fewer cases initiated before domestic courts so that judges lack skills and experience in the data protection field. This means that data protection issues are marginalized and not taken as a priority in court's training and awareness-raising programmes.[129] Second it is rather clear that in most jurisdictions judges have limited specialisation in data protection laws, as pointed out by many lawyers and judges interviewed.[130] The lack of sufficient cases, not being well updated with data protection laws and issues, and the complexity of new laws can account for the status quo of an inactive role of the judiciary. Training and support to help improve the expertise of judges are not sufficient and data protection issues are not prioritized.[131] FRA's findings suggest that more training and updates of data protection issues and laws may be set on the agenda of the judiciary in the near future, even though there are not so many cases to be decided right now. Third, according to FRA's recent assessments the time taken for judicial remedy is too lengthy in general and is a problem for data

[126] Access to Data protection remedies in EU Member States, p. 21.

[127] Ibid.

[128] Id., p. 22.

[129] ACCESS TO DATA PROTECTION REMEDIES IN EU MEMBER STATES, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states (last visited Jul 17, 2014), p. 50.

[130] Id., p. 50.

[131] Id., p. 51.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

protection violation victims to seek remedy.[132] Therefore the speed of the decision making of the judiciary shall be improved in future.[133]

6.4 New Data Protection Framework

The long awaited reform of the Data Protection package – including a reform of Directive 95/46/EC and Framework Decision 2008/977/JHA – seems to have been finally agreed in principle by Council, Parliament and the Commission. As the implications of the reform package become clearer, one can then reflect better on their impact on Internet Governance. This too will be an area which will be closely followed in the coming months.

[132] Also interviewed judges and lawyers share the same opinion themselves. See: Id., p. 38-39.

[133] Id., p. 22.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

7. Conclusion

From the review carried out in this task, one can confirm that there is no one single coherent EU vision for Internet Governance. The vision, if one can call it so, consists of many aspects, including the human rights perspective (privacy, data protection, freedom of expression, etc. on the Internet), an economic perspective with an ambition for a single digital market in the information age, and a technical perspective including interoperability, super-connectivity and efficiency, and net-neutrality, and the political perspective including national security, anti-terrorism aspects in particular.

Furthermore this collection of aspects and ensuing visions is not a product of one single stakeholder, but many including the EU authorities, Member States, civil society organizations, the industrial (private) sector that includes not only EU IT companies, but more U.S. IT Giants, EU citizens (limited roles in shaping the vision, mostly as consumers and litigants), etc.. Each of these players and stakeholders all have their own vision/plan for the future Internet and work towards achieving this.

Moreover, the EU vision cannot be separated from a bigger vision of Internet governance including other countries and regions, including China, the U.S., Russia and Brazil, which to different extents shape Internet governance through political and diplomatic means. Given this, there seems to be an increase of EU participation in Internet governance fora, including in multi-stakeholder Internet governance fora.

In some instances, different perspectives of the EU vision conflict with each other. However, even in at times conflicting stances there is a common core in the EU position in particular on the protection of EU values including protection of fundamental human rights and an open Internet over a fragmented Internet.

What has been noted from the start of the MAPPING project is that the EU's Internet Vision is to a great extent a 'work-in-progress', suffice it to mention the ongoing legislative reforms of the data protection framework, safe harbour rules on the cross-border use of personal data, net neutrality, standardisation exercises of e.g. privacy-by-design and several other political debates that follow from international acts of violence or terrorism on the use of encryption on the Internet and Internet services, mass surveillance etc. These ongoing, sometimes fast, sometimes excruciatingly slow, developments mean that the task in 4.1 is also a work-in-progress: this is an interim report to be followed upon and updated as the project progresses in the coming months. It is only an ongoing updating process that can ensure that the purposes of this review are achieved.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Appendix 1: Law and Policy Documents

- **General principles on Internet Governance**

- Declaration by the Committee of Ministers on Internet governance principles (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies).

- **Cyber security**

- EU Internal Security Strategy in Action: Five steps towards a more secure Europe (IP/10/1535 and MEMO/10/598).

- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

- Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (June 25, 2013).

- JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (ISS) (Feb. 7, 2013).

- 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)(Art. 30, 31 and 32: duties of notification of a personal data breach to the supervisory authority).

- The 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, of March 28 2012.

- Council Conclusions of 31 May 2010 on the Digital Agenda for Europe (10130/10).

- The Digital Agenda for Europe (DAE) (May 2010) (Trust and Security Chapter).

- The Proposal Legislation Data Protection regulation (Articles 30, 31 and 32).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

- Article 15 of the e-Sig and e-ID regulation: "Security requirements".

- The Framework directive (Direct: Article 13a "Security and Integrity".

- 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: (Article 4: Regulation of Security "Security of processing").

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (invalid in 2013).

- Council of Europe Convention on Cyber Crime 185 (Nov. 23, 2001).

- The 95/46/EC Data Protection Directive (Art. 17).

- The Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, of January 28 1981 (Art. 7).

NIS (Network and Information Security)

-PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union {SWD(2013) 31 final} (Passed by the Parliament on March, wait for council reading).

-COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" COM(2006) 251.

-COUNCIL RESOLUTION of 18 February 2003 on European approach towards a culture of network and information security(2003/C 48/01).

-COUNCIL RESOLUTION of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C 43/02).

-Communication Network and Information Security: Proposal for A European Policy Approach COM(2001) 298 final of 6.6.2001.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

CIIP (Critical Information Infrastructure Protection)

- Communication on CIIP of March 2011 on 'Achievements and next steps: towards global cyber-security COM(2011) 163.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure **"**Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience (COM (2009) 149).

- Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised Crime.

- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

- Council Resolution (2007/068/01).

Trust Service Providers

- The Proposal for a Regulation of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market (COM/2012/0238 final), present the 5th July 2012.

-Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

- **Cybercrimes**

- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

- The 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, of March 28 2012.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

- Europol's 2013 Serious and Organised Crime Threat Assessment (SOCTA).

- 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.

- 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.

- 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.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions -Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law COM(2011) 573 final, of September 20 2011.

- The 2001 Council of Europe Convention on Cybercrime (ETS 185).

- **Net Neutrality**

EU policies and laws

-Regulation on the Single Telecoms Market (initially adopted by the European Parliament, April 2014, promoted in 2013) (Articles 23-25).

-Proposal for a Regulation of the European Parliament and of the Council (Sept. 9, 2013, Preambles and Articles 23-25).

-Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 April 2011 - The open internet and net neutrality in Europe [COM(2011) 222].

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

-COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Agenda for Europe [COM/2010/0245 f/2].

-The Telecoms Package (valid since Dec. 19, 2009).

-Directive 2009/140/EC (Framework, Authorisation and Access directives).

-Directive 2009/136/EC (Universal services and E-privacy directives).

-Regulation No 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC regulation).

-European Commission, Declaration on Net Neutrality, appended to Dir. 2009/140/EC, O J L 337/37 at p 69, 18 December 2009.

Council of Europe

-The model framework for net neutrality announced by the Council of Europe.

-Declaration of the Committee of Ministers on network neutrality ((Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies).

-Declaration by the Committee of Ministers on Internet governance principles (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies).

- **Personal data/information protection**

- 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 and to the 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.

- Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

--Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Regulation Directive).

--Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

-- the Charter of Fundamental Rights of the European Union (Article 7 and Article 8).

-- the European Convention on Human Rights (Article 8).

- **Extraterritorial jurisdiction**

-Article 4§1, Article 17.3 of DPD.

-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.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

-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.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

-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. Policy Department C: Citizens' Rights and Constitutional Affairs.

-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 cybercrime, 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.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

-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 Fighting cyber crime and protecting privacy in the cloud 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.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

-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 of24 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.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

-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.

-Reding, V., "Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing", IAPP EuropeData Protection Congress, Paris, 29.11.2011.

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Appendix 2: Related academic literature

BEREC MONITORING QUALITY OF INTERNET ACCESS DEVICES IN THE CONTEXT OF NET NEUTRALITY 4, http://www.beuc.org/about-beuc/who-we-are (last visited Aug 20, 2014).

BEREE's research released in May 2012, http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf

Bigo, Didier et al., National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law, (2013), http://dare.uva.nl/record/496718 (last visited Aug 24, 2014).

Boillat, Philippe & Morten Kaerum, Handbook on European data protection law (Publications Office of European Union Belgium) (2014), http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (last visited May 8, 2015).

Brown, Ian, The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance, AVAILABLE AT SSRN 2433912 , 8 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2433912 (last visited Sep 1, 2014).

CAVELTY, Dunn, et al, A RESILIENT EUROPE FOR AN OPEN, SAFE AND SECURE CYBERSPACE 4–5 (Social Science Research Network) (2013), http://papers.ssrn.com/abstract=2368223 (last visited Sep 6, 2014).

Costa, Luis & Yves Poullet, Privacy and the regulation of 2012, 28 COMPUTER LAW & SECURITY REVIEW 254–262, 261 (2012), http://www.sciencedirect.com/science/article/pii/S0267364912000672 (last visited Aug 31, 2014).

Hellemans, Liesbeth, CLOUD FOR EUROPE: STUDY ON THE LEGAL IMPLICATIONS OF CLOUD COMPUTING (KU Leuven) (2014), http://www.cloudforeurope.eu/news/-/blogs/study-on-the-legal-implications-of-cloud-computing (last visited Aug 29, 2014).

Kraemer, Jan et al., NET NEUTRALITY: A PROGRESS REPORT (Social Science Research Network) (2013), http://papers.ssrn.com/abstract=2344623 (last visited Aug 20, 2014).

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345".

Kuan Hon, W. ET AL., CLOUD ACCOUNTABILITY: THE LIKELY IMPACT OF THE PROPOSED EU DATA PROTECTION REGULATION (Social Science Research Network) (2014), http://papers.ssrn.com/abstract=2405971 (last visited Aug 27, 2014).

Kuner, Christopher, Data Protection Law and International Jurisdiction on the Internet (Part 2), International Journal of Law And Information Technology (2010) 18 (3): 227-247.

Marsden, Chris, Net Neutrality: Measuring the problem, Assessing the legal risks, IBEI WORKING PAPERS, 13 (2014), http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fcatedratelefonica.ibei.org%2Fwp-content%2Fuploads%2F2013%2F06%2FIBEI-%25C2%25B7-42.pdf&ei=SmrrU7f8C4XGPM68gTg&usg=AFQjCNEIXj00ksHNM_eV8bJl0TSLHvR3JA&sig2=Ki_cM841wLqJ9fUX8kdoog&bvm=bv.72938740,d.ZWU (last visited Aug 13, 2014).

Porter, Andrew & Annegret Bendiek, European Cyber Security Policy within a Global Multistakeholder Structure, 18 EUROPEAN FOREIGN AFFAIRS REVIEW 155–180, 163–177 (2013), http://www.kluwerlawonline.com/abstract.php?area=Journals&id=EERR2013011 (last visited Sep 6, 2014).

Savin, Andrej, How Europe formulates internet policy | Internet Policy Review, 1 Internet Policy Review, 6, http://policyreview.info/articles/analysis/how-europe-formulates-internet-policy (last visited Aug 20, 2014).

Schwartz, Paul M, INFORMATION PRIVACY IN THE CLOUD 1264 (Social Science Research Network) (2013), http://papers.ssrn.com/abstract=2290303 (last visited Aug 24, 2014).

Whitman. J. Q. Whitman, Two Western Cultures of Privacy: Dignity versus Liberty, The, 113 YALE LJ 1151 (2003), http://www.yalelawjournal.org/pdf/113-6/WhitmanFINAL.pdf