MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

"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

WP2 Dialogue and Participation
WP leader: LSC

D2.2 Guidelines about Management of Dialogue and Participation

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)	

Document Version Control:

Version 0.1	Originated by:	Alfonso Alfonsi, Maresa Berliri	on June 04 2015
Version 0.2	Reviewed by:	Jeanne P. Mifsud Bonnici	on Aug 07 2015
Version 0.3	Reviewed by:	Pedro J. Gómez, Ana V. Pérez	on Aug 27 2015
		Radek Bejdak, Irina Zálišová	on Sept 04 2015
		Alexandra Tsvetkova	on Sept 05 2015
		Patrick Curry	on Sept 16 2015
		Bo Zhao	on Sept 16 2015
Version 0.4	Revised by:	Alfonso Alfonsi, Maresa Berliri	on Sept 17 2015
Version 0.5	Reviewed by:	Rainer Hörbe	on Oct 30 2015
Version 0.6	Revised by:	Alfonso Alfonsi	on Nov 18 2015
Version 0.7	Reviewed by:	Joe Cannataci	on Feb 01 2016

CONTENTS

INTRODUCTION

1. Institutional framework

MAPPING (Managing Alternatives for Privacy, Property and INternet Governance) is a Mobilisation and Mutual Learning Action Plan on Societal Challenges project that is funded by the European Union's Seventh Framework Programme for Research and Technological Development. It is carried out by a consortium of 12 European organisations and 1 international organisation and it is coordinated by the University of Groningen. The goals of MAPPING are:

a)to explore paths for a responsible adaptive and integrated approach to Internet-enabled innovation; and

b)to elaborate a responsive action plan, along with concise policy recommendations, to improve the societal relevance of the digital transition.

At the core of MAPPING's approach is the planned mobilisation of and dialogue with a wide spectrum of ICT-related stakeholders and social actors. Among the first occasions of dialogue, there was a coordinated and comparative consultation of stakeholders, by means of **focus group** discussions, which provided the input for the preparation of this document.

In this framework, the **focus groups' consultation** objective was twofold:

- obtaining comparable informed opinions from a wide range of Internet related actors in several European countries on practices, problems and experiences of change related to current and emerging **Internet uses** where **citizens seek remedies**;
- test some initial **dialogue** and **participation** assumptions and instruments.

This exercise has addressed the three main, interrelated, problem areas considered in the project: **Internet Governance**, **Privacy** and **Intellectual Property Rights**.

According to the DoW of the MAPPING Project, two focus groups were carried out in each of the EU countries of the project's national partners, plus two in Brussels as the seat of the European Commission. France was excluded since Interpol is an international organisation. For similar reasons and because it does not belong to the EU, Switzerland, the seat of DIPLO, was also not included.

Each project partner was responsible for the organization and implementation of the focus groups for their country, starting with the selection of participants to the translation of transcripts into English. LSC – Laboratory of Citizenship Science –, as leader of MAPPING WP2 "Dialogue and participation" was responsible for the general coordination, providing the other partners with instructions and guidelines to ensure that the exercise was conducted consistently in all countries. LSC also carried out the focus groups in Italy and in Brussels.

On the basis of the analysis of the transcripts of all focus groups, the present document was drafted in the form of "Brief guidelines for dialogue and participation activities".

In the MAPPING Dialogue and Participation Plan (D2.1)[1], dialogue strategies are grouped according to content, instruments and approaches, therefore the present guidelines are structured accordingly. Thus, after this introduction and a brief note presenting some basic data on focus group implementation, the guidelines proper are divided into two parts. The first part contains indications on dialogue content and the main points of focus as they emerged from the discussions. The second part provides some operational indications and criteria on how to conduct further dialogue and participation activities, integrating what had previously been foreseen in the Dialogue and Participation Plan.

This document was drafted by Alfonso Alfonsi and Maria Teresa Berliri with the support of LSC Team members.

2. Focus group implementation: some basic information

As mentioned above, 22 focus groups were conducted in 10 European countries: Austria; Bulgaria; Czech Republic; Germany; Italy; Malta; the Netherlands; Romania; Spain; United Kingdom. Two focus groups were also organised in Brussels, to which representatives of international organisations and EU Internet governance bodies were invited. All focus groups took place between July 2014 and March 2015.

For the preparation and implementation of the activities, each national partner was provided by LSC (as leader of WP2) with an "Outline for focus group discussion", providing the needed specifications on the contents and the methodology of the exercise. The Outline was complemented by some "Guidelines for the Focus Groups moderator", which ensured that all sessions were conducted according to a similar script, in order to ensure the comparability of the results. The script proposed the participants to consider several issues in the three areas of MAPPING: Privacy

[1] See MAPPING, Deliverable D2.1 "Dialogue and Participation Plan", June 2014.

and Integrity, Internet Governance and Intellectual Property Rights. After the distribution of the "Outline" and the Guidelines, remote sessions were held between the leader of the WP2 and each partner to provide clarification and tackle specific issues for the implementation of the focus groups. LSC also monitored the progress of the work.

The focus groups were conducted as a form of consultation among a wide spectrum of Internet-related stakeholders and social actors. The approach that was followed called for a form of **consultation** that was: **coordinated**, i.e. guided and facilitated by an expert moderator; **multilatera**l, since it would involve stakeholders from various walks of life, having different visions, backgrounds and expertise; **interactive**, since it would be aimed at maximizing the results of the interaction and also the debate among the participants.

Each focus group was conducted by a moderator, with the help of a rapporteur, both being provided by the national partner concerned. The duration was about three hours per focus group, including the introduction. Each discussion was recorded, transcribed, translated and anonymised by the national partner concerned and then handed over to LSC.

All in all, 152 of the invited stakeholders were able to participate for the full time of the meetings. Only in 3 focus groups were there less than 6 participants, while in the remaining 19, participation ranged from 6 to 9 (the maximum number allowed).

There were about 900 transcript pages, out of which around 2500 different records of content were abstracted.

The relative majority of the participants were **academicians** and **researchers** (about the 25% of the total), but almost all of them were serving or had served as consultants both in the public and private sector, hence they had not only a theoretical, but also a practical experience of the issues being debated. The second category represented consisted of **entrepreneurs**. Also significant was the presence of officials of the **public sector** and **professionals** in the field of ICT. Slightly less represented were **NGOs** and **CSOs**, **international organisations**, **law enforcemen**t agencies and the **media**.

In terms of disciplinary background, there was a prevalence of **law specialists**, followed by people versed in **engineering** and **computer sciences**. Other expertise included **economy**, **political sciences**, **communication** and **social sciences**.

PART I

Content of dialogue and participation activities: *foci* of dialogue

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

A dialogue on digital transition

The major topics that were discussed were organised in the three thematic areas of MAPPING: **Privacy** and **Integrity**, **Internet Governance** and **Intellectual Property Rights**. These areas provide indications of what can be considered major issues on which the expert debate on the Internet is currently focused, hence the denomination: ***Foci* of dialogue**. They illustrate what the participants perceive as the significant changes that the Internet has brought about in society and the effort to anticipate its future developments and their possible societal consequences, which form the concern of law and policy makers, who are still struggling to regulate them and propose remedies to the problems they cause.

In fact, to anticipate one of the findings of the focus group exercise, most of the participants have shown, in one way or another, an awareness of being in a **transitional period**, in which new patterns are emerging and where there are doubts about the effectiveness of consolidated solutions, while new instruments are being sought.

Within MAPPING, this overall process of change is conceptualised as a "**digital transition**". By using the term "transition", we wish to signify that innovation in digital technologies are marking the passage from a set of social, cultural, technological and economic conditions to a new configuration of such conditions. The notion of transition points both to changes that, like in a drift, are brought about by an accumulation of factors, independently of the agency and intentionality of the actors involved, and to the kind of guidance that the concerned actors try to provide to these on-going processes.

We wish to note that, according to the points of view considered, different aspects of the digital transition have been each time put in the forefront, also using different specific expressions such as digital economy (to stress the economic aspects) or knowledge society (to stress the social implications). In this sense, the expression "digital transition" is to be intended as an "overarching concept", which tends to include all these different specific analytical perspectives.

As we said, the discussion of the focus groups has supported this vision, while at the same time has provided the opportunity to collect and organise evidence on the accumulation of factors brought about by developments in the field of ICTs, the related opportunities (and risks) they offer to citizens and social actors, as well as on the policies and legal frameworks that are trying to provide governance to such changes, in order to offer remedies to the problems that they are causing.

In this part of the document, the three thematic areas of the focus group discussion (Privacy, Internet Governance and Intellectual Property Rights) are briefly outlined. For each area the major *foci* of dialogue are presented. Each focus of dialogue is structured with a rationale and a set of emerging issues or contentious points. In a few cases, we quote directly the anonymised views of some of the discussants.

Area A - Privacy and integrity

The first part of the focus group discussion dealt with the significant increase in the technical capacities – and related practices – to collect and process huge quantities of personal data (also provided by the users themselves) on the Internet. Also considered was how the most valuable knowledge and information of companies and other organisations is kept and managed as digital data.

Such a massive array of personal or otherwise sensitive data is utilised for commercial (including new business models), administrative and security purposes. A significant increase in the collection and processing of personal and other digital data is occurring also in the field of surveillance, for the prevention and repression of criminal activities (including cyber crime) and terrorism.

The discussants converged in pointing out how these new opportunities, together with their advantages, create corresponding risks in terms of security and privacy and can expose citizens' fundamental rights to malpractice, abuse and outright violation. It was also mentioned that deployment of new technological capabilities in a very short span of time can substantially alter privacy vs. usability situation. The issues discussed in this area can be grouped into twelve different *foci* of dialogue.

Focus A1 - Risky user behaviours

A large majority of discussants converged in pointing out as an important focus of dialogue a cluster of practices and behaviours by which the users themselves constantly put at risk their personal data, due to a lack of awareness and/or lack of understanding of the technical means they use daily. Of course, it was pointed out that there is a whole spectrum of differences among users, also in relation to social and age groups, ranging from wholly unaware users (those that show an "I don't know, I don't care" attitude) to activists for the protection of their privacy or from "digital natives" to "silver surfers". What is noteworthy is also the fact that almost all current uses of the Internet and online services, from participation on social networks, to making electronic purchases, were perceived by the discussants as implying severe risks to privacy and personal integrity. This first focus of discussion can be articulated into the following points as expressed by the participants.

1. There is a **lack of awareness**. Users are not clear about what personal data are and do not recognise how "open" cyberspace is and how permanent their actions and transactions are. Furthermore, they do not perceive the sheer amount of data they are disclosing and the huge capacity of the Internet to bring together, store and process personal data; they do not care much about the purpose for which their data are being collected nor do they have a very good idea of the consequences and the risks involved.

2. Users show a strong tendency towards and a desire for **self-disclosure**, i.e. to communicate personal information on social networks, as well as establishing contacts and relationships with barely known or unknown people. This widespread social tendency can also expose users – especially the younger generations – to the risk of profiling, cyber bullying, recruitment or conning. In doing so they also disclose personal information of unknowing/unwilling third parties (e.g. by posting and tagging with the names of one's own friends group photos).

3. Users **exchange personal data** for "**convenience**", in order to receive services that require customers to disclose personal information (about their geolocalisation, health, fitness, preferences, etc.). This tendency is greatly increased by the spread of smart mobile devices, which are able to communicate with each other (M2M). Also in this case, users, who accept that applications on their mobile devices access their own address books and other records, in practice also give away personal data of third parties.

4. Users **exchange data for free of charge services and applications** when they provide personal data that are not necessary for the service received but are requested nonetheless by the provider, often (but not solely) in exchange for free of charge services or apps or other advantages (e.g. to download "free" apps, to obtain bonuses in gaming, to obtain discounts in supermarkets, etc.). Users are also constantly using devices, such as smart phones or tablets, that have also in-built mechanisms to collect personal information almost by default, which can be used by providers without the users' awareness.

5. **Users lack knowledge and technical capabilities** to employ all the available instruments to protect their personal data on the Internet, even when they are aware of privacy problems and/or declare they attach a high value to privacy, so that their actual behaviours do not correspond to their concerns.

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

FOCUS A2 - SECURITY PROBLEMS OF ENTERPRISES IN PROTECTING DIGITAL DATA ASSETS

Another focus of discussion was that of the risky practices employed by enterprises and other organisations (including public administration) in storing and managing their digital data. The discussion was centred on the fact that data digitalisation is a pervasive phenomenon, pertaining to all organisations, public as well as private. It was stressed by some discussants that digitally stored information typically constitutes a core asset, especially for start-ups. So enterprises are constantly exposed to the risk of having their business data disclosed. Some participants also pointed to the fact that SMEs are particularly subject to such risks, due to the limited (if any) resources that they can invest in internal security. In fact, attacks on company security are steadily increasing and becoming more and more focused on specific targets, while internal security systems are often outdated, having been devised for contexts in which system isolation was much easier to obtain. Some specific issues that emerged in the discussion are reported below.

6. There is a difficulty in running **closed security systems** in the current business environment. Also, enterprises that have their own closed systems are forced by the necessities of the environment in which they operate, to at least partially open them, thus submitting themselves to risks.

7. **The mobile environment** (providing instant world-wide connection) cannot be well protected by the pre-mobile IT security standards.

8. The ever-increasing recourse to **cloud computing** to store digital data, together with its clear advantages, can produce even more security problems. There is a requirement for trusted cloud where SMEs can collaborate with partners, customers and suppliers with compliance and security.

9. **Small and Medium Enterprises** use **standard commercial software** and **hardware** designed for individual consumers and not to adequately protect the digitalised data assets of an enterprise.

10. **Intense BYOD** (bring your own device) **practices** and the tendency to use unchecked USB pen drives and other devices by employees can jeopardise the security of companies with strict IT security systems.

11. **Sensitive data are part of an enterprise's estate** and are sold in case of bankruptcy.

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

FOCUS A3 - SECURITY RISKS CONCERNING PERSONAL DATA LEGITIMATELY MANAGED BY PUBLIC OR PRIVATE ORGANIZATIONS

Another recurring point is the fact that many organisations, public or private, which legitimately collect and store sensitive personal third party data (such as hospitals, educational institutions or data managing companies) may be increasingly at risk of misuse by their employees or subject to breach of their security by external parties. In some cases, the very rules promoting public administration transparency can have paradoxical effects when "public" documents are stored as digital data rather than physically. Among the issues raised, the ones recurring most often were the following.

12. **Resorting to subcontractors** by organisations that manage sensitive personal can often cause data breaches (e.g. Snowden was a subcontractor).
13. Storing **public information in digital forms on-line** (e.g. lists of participants in meetings) may lead to reconstructing personal trajectories.
14. **Sensitive personal data** legitimately collected and stored by Institutions (e.g. universities) could be easily **misused** by the institution's staff for inappropriate purposes, such as profiling, predictive analysis, etc.
15. Lawyers (even from big law firms) have problems using online services because they cannot any longer guarantee **professional secrecy** (for example in their communications with the client or even in the case of electronic submission of legal documents to courts).
16. **Health related** information is kept in databases which can be accessed by doctors, hospitals, patients, with a risk of being hacked, altered or misused.
17. **Rules for transparency** in public administration (e.g. Italian Act no. 33 2013) risked overexposing personal data when applied on-line.
18. Public administration mandatorily **stores sensitive digital data** on financial circumstances and cost accounts of their providers, which need to be protected from competitors.
19. **Public administration officials utilise devices** (often US produced and conforming to US standards and regulations) and Wi-Fi technologies with unchecked security risks for integrity and confidentiality (e.g. hacking) and are unaware of such problems.
20. **Some enterprises** (SMEs in particular) **choose non-compliance**. They evaluate risks and costs of non-conformity to regulations (to be sanctioned with a fine) against the investments needed to conform. In some cases, in order to

minimise costs and resources, they conclude that it is more convenient not to comply and risk the sanctions.

21. **There is a lack of adequate levels of security incorporated within the devices of the Internet of Everything**. Many such devices do not include adequate protection measures for collected data (personal or non-personal). It seems that more attention is devoted to function and design than to security. An average user would connect one of these IoT devices mainly for what it is capable of doing (and for how cool it looks).

22. **The principle of data minimization** in collecting data is scarcely observed, not only by the private sector but also by the public administration.

FOCUS A4 - EDUCATION AND AWARENESS RAISING

A significant cluster of issues concerns what was perceived by the discussants as a lack of education and training among the public about the use of the Internet. In the case of children and young people, there is the additional problem that educational agencies are not well equipped to teach a subject about which the educators are often less knowledgeable than their learners. This lack of education seems to affect the very notion of what personal data are and involves an uncertainty on what rights the users actually possess in this regard. At a more basic level, discussants highlighted a sort of generalised "illiteracy" concerning both software and operating systems. Some participants, however, emphasized the fact that there can be significant differences in knowledge and capabilities among different age groups. Albeit with different specifications, a large number of discussants expressed the need for educational or awareness-raising initiatives addressed to different groups of internet users. The discussion on both the problems and the remedies included the following points.

23. There is a lack of a **consolidated intergenerational memory** on the Internet and digital devices, which creates a gap in the role usually played by educational agencies (family, schools, etc.) in this regard. This is particularly felt in the case of "digital natives": children that use all types of digital devices without being educated on their risks, about which parents and teachers may know even less.

24. There is a need for policies to **support educational agencies**, with awareness-raising campaigns and developing specific curricula in schools for children and adolescents on the rationale that public authorities should intervene to offer safety instructions to address potentially risky behaviours (in the same way that

they teach other forms of safety e.g. crossing the road, riding a bicycle, learning to swim).

25.It is necessary to **motivate society**, in order to avoid overreliance on regulation that doesn't always work as intended. This might include campaigns to reach target groups according to their specific needs, including the older generations (silver surfers).

26.**On-line handbooks and guides** on specific problems have proved to be useful in several instances (like the guide on safety in social networks by the Italian Authority for Privacy Protection). They can include codes of conduct and tips to users.

27.It is important to recognise and support **Netizens** and organisations that are already **practicing forms of self-protection** on the Internet. Especially among the young generation, a growing number of individuals have an understanding of privacy risks and enact strategies to defend themselves (e.g. using social networks to verify fake identities).

FOCUS A5 - LEGITIMACY/OPAQUENESS OF CURRENT BUSINESS MODELS BASED ON PERSONAL DATA

A related but different focus in the discussion concerns the fact that the digital economy is built on the premise that personal data can be aggregated, sold, resold and repurposed. In this context, personal data has become a commodity and is increasingly central for the business models of online commercial and non-commercial services, with related risks, challenges and opportunities. Most of the discussants pointed out a certain opaqueness on what can be considered legitimate and non-legitimate use of personal data collected in various forms. This includes also the use of cookies and their unchecked pervasiveness. What is perceived as a lack of transparency is the extent to which personal data collected for a specific purpose can be reused in completely different forms of commercial exploitation, including direct marketing, profiling and spamming, without notifying the concerned party. This kind of concern can be articulated into the following points.

28.**Users' data become an asset of the enterprises** that add value to them. Hence they can be exchanged, marketed, or transferred to third parties. However not all enterprises have a clear understanding of the value and the potential of the data they possess. Furthermore, many enterprises do not have an identity regime for the data they collect and manage – i.e. they lack a

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

taxonomy of their data with the privileges attached to it, definitions of identities and roles. Some enterprises, on the basis of a priority based approach, have this regime only for 'important data'.

29.**So-called "big data" and new data analytics create unprecedented opportunities** for business exploitation of personal data in a completely new commercial environment, difficult to manage by the enterprises themselves and to regulate by the concerned authorities.

30.**User generated content or the users themselves are the "product"** in several new business models, like in the case of social networks.

31.**Some codes of conduct and professional standards should be developed** in the community of providers, in the understanding that not all can be regulated by means of legislation, in analogy to what happens in other commercial sectors.

FOCUS A6 - EMERGING "PRIVACY FRIENDLY" BUSINESS MODELS

Together with the discussion on the transparency of the currently predominant business models based on the exploitation of personal data, some participants highlighted the emergence of new models that have at their core respect of privacy and aim at establishing a trusted relationship with users, helping them to preserve their own control over their data. As compared with the topics presented so far, which were perceived as important by a majority of discussants, these models were supported by a minority of participants, but raised interest and originated lively exchanges of views. Among the models discussed in this framework, we can consider the following.

32.**There is the emergence of the "intention economy"**, marking a shift from traditional "customer management relations" to "vendor management relations", which entails the development of trust frameworks (like the RESPECT Network framework[2]) that empower the user to decide what happens to his/her own data. In the intention economy, it is the user who declares his/her intentions and receives only requested advertisements and not those provided by an algorithm, fed by a tracking system in the Internet.

33.The development of **providers** that offer online services, like search engines, which incorporate **privacy by design** and privacy enhanced technologies.

[2] For the Respect Network, see the website: https://www.respectnetwork.com/

34. **Data infrastructure security** and data management procedures by enterprises that establish standards, procedures and clear individual responsibilities in collecting, managing and accessing the data are markedly insufficient. If implemented such measures could in fact prevent loss, deletion or misuse of data and adequately manage requests from users who want to change or delete their data.

35. Increasingly "**trust frameworks**" (like Respect network[3] or the Kantara Initiative[4]) are being formed to support federated trust across organisations to help maximise the sharing and use of information in trusted ways. The technologies and policies implemented depend upon the level of assurance required to mitigate the degree of risk.

FOCUS A7 - PERSONAL IDENTITY MANAGEMENT

Much discussion in the focus groups revolved around the issues connected with the management of personal identity on the Internet. The discussion involved several aspects starting with the very conceptualisation of identity in the digital environment and its relationship with identity in the off-line world. Identity is, in fact, seen as the anchor of all meaningful operations and transactions in the digital world and the building block of trusted exchanges and relations. At the same time, the integrity of personal identity when entering cyberspace is challenged by many opportunities for tracking personal movements and profiling, on the one hand, and for identity theft and impersonation or usurpation, on the other. Another critical point is the possibility of building fake identities and the need of instruments to minimise all kinds of fraud connected to this opportunity. In this regard, several points of debate emerged.

36. **There is a necessity to distinguish between identity**, as the univocal relation to an individual physical human being, whose authenticity is guaranteed by an authority and the many roles or personas he/she can legitimately play on the Internet (identity layer).

37. **The entire concept of identity is changing**. Identity is not only about details such as name and address but also about other characteristics (for example biometrics characters) that can be used to identify a person in a population and take decisions on this basis. In this framework, the term "personal details" needs to be defined, also at a legislative level, taking into account the relationships between the digital and physical world.

[3] For the Respect Network, see the website: https://www.respectnetwork.com/

[4] See the website: https://kantarainitiative.org/

38.**There is the issue of authentication vs. identification**. Secure authentication can be achieved at various levels and by using integrated and multiple mechanisms, such as those implemented for e-banking. Also for identification it is possible to use multiple mechanisms. The establishment of a really digital identity would require a physical check at a certain point. Authentication is based on a previous identification. In contrast with the off-line world, in the digital world, an identification is required to access any services or make any purchase.

39.**In relation to the public sphere, the purposes of identity management** are seen in the light of the government/citizen relationship, in terms of entitlements (rights) and obligations. Identities are generated and authenticated by governments, who can guarantee only some properties of an individual for some specific purposes (e.g. age verification). The process of identity management by the government can be described as an enrolment process that bounds a given attribute to a life form and identity, providing confidence to the chain of trust.

40.In the **commercial sphere**, the first use of **identity management** is for employee authentication which is considered crucial for digital economies and the future of the Internet. Best practices and capabilities developed for employee ID management are increasingly being used for citizen and consumer ID management at lower assurance levels. To some extent, identification and authentication can be provided by the business themselves for specific purposes.

41.There are ongoing developments in the **Digital Rights Management (DRM)** technologies for privacy protection to provide users with easy and viable tools to make informed choices about how their data are used and to include consumers as first class participants. Different models are already commercially available. A salient issue of the current debate is how and when they can be used. According to some discussants, DRM can also be used by some business models to create user profiles, linking each consumer with specific contents. In this view, some DRM systems violate consumers' privacy in a number of ways, for example, in the authentication step and in the tracking step (although they can be justified as forms of fraud prevention). The consumers should be allowed to take part in the determination of the degree of tracking and the degree of anonymity allowed in the system.

42.There is a need for further development of technologies and applications to **access control** and **authentication** in public and commercial environments in the framework of the experimentation of **digital identity schemes** in various

European countries. The implementation of the new EU eIDAS regulation[5] is going to have a strong impact and could force EU nations towards federated identity management.

43. **There is a need consolidate and expand procedures, mechanisms and technological solutions (low-cost and viable) for age verification** on the internet, in order to protect young users and to prevent them from accessing adult content. An example could be the AVMS Audio Visual Media Services European Directive, which is transposed into various European countries.

FOCUS A8 - INFORMATIONAL SELF-DETERMINATION/DATA SOVEREIGNTY

One important issue in the debate concerned the means to allow users to recover control over the personal data that they disclose by navigating the Internet or that are generated by default when they use certain devices. The discussion revolved around how and to what extent users may be able to know at any time what data are collected about themselves, for what purpose, what will be done with the data and whether data are being transferred or sold to third parties. Furthermore, one should be able to opt out. The right to reputation and personal dignity were taken into account. In this regard, a few discussants used the term "data sovereignty", while others preferred the more established "Informational self-determination". The discussion revolved around the following points.

44. The very **definition of what can be considered personal** data was in itself a matter of debate. Beyond the established definition, as in the EU Directive on data protection[6], more subtle elements were pointed out that, once recorded and linked to other, can result into very sensitive personal information. This has consequences on how and on what the "Informational self determination" could and should be exercised.

45. The use of **Big data** and **data analytics** from private and public bodies is considered problematic. There is an on-going paradigm shift in the use of big

[5] Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market.

[6] See the definition of "personal data" in Article 2(a) of the Directive "For the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

data, from collecting data with a clearly predetermined goal, to the "collect it and see what kinds of correlations you can find in that big cloud" approach. Therefore, there is a trend towards more collection, more measurements, more knowledge, which can be used for predictions and profiling people, which create asymmetries of power that can affect the autonomy of people. In this regards there is a lack of legislation.

46. The need to **improve transparency** in the treatment of data disclosed for a specific purpose to a given party that can be reused for different purposes also by other parties. Citizens have a right to transparency in the collection, treatment and management of personal data by enterprises, public and private organizations and by the state, for the various purposes they are collected (surveillance included). There is a request to define rules, limits, responsibilities and standards.

47. There is thought of the possibility of a kind of "**traffic light system**", through which every user can be sure what data he can give away without a second thought, what data can be harmful or what data are really sensitive. This could include opt-in opportunities with differing protection levels, more opt-out possibilities and the "reversibility of actions".

48. There is a viability of implementing systems of **symbols** or **pictograms** to signal the degree (if any) of transaction riskiness. Some service providers that offer increased privacy protection are already using some e.g. for signalling the risks of privacy settings. Others propose to devise a system of 5/6 standardised symbols in analogy with those used by Creative Commons to signal author options.

49. There is a controversy about the possibility to establish and put into effect the **principle of citizens as the owners of their data** by offering users multiple choices, rather than yes or no, in personal data disclosure (in analogy to Creative Commons IPR system). In this regard new conceptualisations of ownership are being proposed, attempting to deal with the complex area of personal data, generated not only by the users themselves, but also, in some context, by the State or by automated devices.

50. Ways of increasing the **accountability** of service providers and other recipients of personal data towards the data they are entrusted with should be considered.

51. Ways of ensuring **personal data portability** should be considered.

FOCUS A9 - GAP IN THE REGULATORY AND ENFORCEMENT SYSTEM

Many discussants stressed the fact that technical developments on the Internet are so fast that it is difficult to keep pace with legislative or regulatory measures (as regards cookies for example). Also, many references were made to the fact that the whole regulatory framework for data protection and privacy is undergoing a deep revision in an interaction involving European institutions, member states and global actors. Furthermore, notions of privacy and personal data protection are changing and overlapping, creating several imbalances. Privacy was seen as a fundamental right that is protected by many different legal concepts to deal with the diverse particular interests that constitute privacy. It was also noted that privacy, or the protection thereof, is dependent on cultural aspects and on the legal systems. In this regard, a need for harmonisation was emphasized. The major substantive issues discussed were how to increase transparency as to the purpose for personal data collection and how to empower each user to decide what happens to his/her data. Furthermore, there are tensions between expressing oneself on social networks and the right to be forgotten. There is a lot of experience of regulations that have been created with the best intention and have had to be pulled back because they were impossible to execute. A major problem discussed in many focus groups was what jurisdiction applies to the Internet in different cases (to one speaker it is a "no man's land"), with profound differences, for instance, between EU and US visions, or the consistency and synchronisation of national regulations with European regulations. Among the issues discussed there were the following.

52. There is a need to **reform** the whole system of "**terms and conditions**" for accessing internet services, since it was felt that at present it serves mainly the purpose of protecting the liability of the provider, rather than the rights of the user. An increased standardisation and clarity in data security declarations was called for. One major point is to work on the user interface, providing the crucial points in a clear language and being transparent as regards the use of the data and the related risks, so that the users' consent can really be informed (see, for example: https://tosdr.org/).

53. The fact that the current system of regulating the treatment of personal data under the **principle of consent** is faulty, since the ways in which such consent is requested and collected lack transparency and is rarely truly informed. Hence the need for a better integration with the principle of fairness.

54. The question of the **accountability** of **providers** and other recipients of personal data, including a better definition of the limits and the responsibilities of governments or private companies who use and process stored information.

55. There is opacity in the legal responsibilities and **role of third parties** that happen to process personal data disclosed to a different party for a specific purpose.

56. There are problems of **enforcing personal data protection in cyberspace** because of the difficulty in keeping pace with regulator and user demands in relation to ever changing circumstances. The implementation of new legislation in this field requires a system which is able to assess actual compliance with the new norms. There are not enough experts in state administrations who are qualified and who would be able to assess, on the basis of technical information, whether there is a breach of the law or not.

57. There are **inconsistencies of jurisdiction** on privacy law (e.g. between European and National Law on data storage times). Jurisdictional issues among countries make it difficult to enforce different types of legislation. There is a need to know in which country the stored data are kept, and establish what jurisdiction applies.

58. There is the current uncertainty concerning whether **unification of legislation,** or at least a common regulation, on personal data protection at European level is forthcoming or if there will continue to be partially harmonised national legislation.

59. There is the emerging question of the **territorial regulation of global providers**, like Google on issues such as defamation law, right to be forgotten or taxation law. At present, there is a very complex system of rules, which is de facto not enforced at all.

60. Part of the jurisdiction and enforcement problems, are conditioned by US legislation and regulation. In this context, the **on-going EU-US dialogue** (e.g. on Safe Harbour principles) aimed at lining up their respective privacy frameworks appears both important and difficult. In this context, there are significant divergences between the European and the USA consideration of Convention 108 of the Council of Europe establishing general rules and standards.

61. The legal process should make sure the actually intended merit of regulation has no side effect. In fact, it has been pointed out that "contradiction of regulations and their impacts" is harmful. There is the need to assess the impacts of regulation.

FOCUS A10 - RESPONSIBILITY OF PROVIDERS AND SYSTEM DEVELOPERS

Many discussants (including representatives of business organisations) addressed the issues of sensitising services providers and developers of software and applications towards a culture of responsibility. There were in fact several business persons and developers that spoke of a felt need for some kind of code of conduct or a deontology similar to that of professional associations. The feeling is that not everything can be regulated by law and there is a need for self-regulation among the parties concerned. Some specific points were made in this regard.

62. Incentivise the concern of developers towards **built-in security** and **privacy mechanisms** when designing new applications and devices (privacy by design and privacy by default).
63. Forms of **security testing** should be ensured for newly developed applications (which at present are missing).
64. Forms of **self-regulation** and **co-regulation** should be promoted in dialogue between providers, public administration and users, to regulate sensitive areas.
65. There is a need to improve the way in which **the liability of software developers and producers** is regulated and managed. At present if the products do not comply with their descriptions only big companies can resort to litigations and settlements (especially under tort law) while small enterprises and the public are completely defenceless. Someone proposed adopting a software risk management approach and software assurance liability.
66. There is a need for **new types of actors to improve trust between users and providers, including** trust intermediaries providing neutral parties and trust anchors.

FOCUS A11 - SURVEILLANCE, SECURITY AND DEMOCRACY

Another focus of dialogue that emerged from the discussion is that of security and surveillance for the prevention and repression of criminal activities (including cyber crime) and terrorism. A field in which there has been a dramatic increase in the collection and processing of personal data and where new smart surveillance technologies are being used by law enforcement authorities and services. New *smart surveillance technologies were recognised for their contribution in preventing and combating crimes in general. However, these operations were also seen by some discussants as posing severe risks of violating the rights and fundamental freedoms of citizens. The focus groups also considered the use that organised crime and terrorists are making of the Internet (including what is called Deep Internet and Dark Internet) for their criminal activities, off-line and on-line. Thus, law enforcement authorities are also faced with the need to increase their capacity to combat the criminal use of the Internet. Furthermore, in the present environment old and new forms of surveillance co-exist, co-support and feed off each other, thus producing "mutual augmentation", which could possibly produce much greater and amplified surveillance by a wide range of actors, and not only by authorities. Thus, a relevant area of discussion revolved on how to ensure a Net where the citizens are safe from criminal activities as well as from undue surveillance from law enforcement agencies, while at the same time these same agencies are provided with sufficient capacity to effectively combat the actions of criminals and terrorists. A balance that was considered by many as difficult to strike. In this regard, the discussion was articulated around the following issues.*

67.The **surveillance activities** carried out **by governments** are considered to **pose risks** to the privacy of citizens. These include concerns about the use of collected data, the impact, pervasiveness, effectiveness and quality of surveillance activities and the various technologies adopted. Another recurring concern is about the tendency to deploy systems (like traffic control devices) for surveillance purposes different from those for which they were designed (function creep).

68.The **proportionality of surveillance activities** involves striking a difficult balance between risk, crime tolerability, measures taken and what the public is able to accept in view of a higher degree of security. In this context, it is also important to consider the tendency towards "all purpose" mass data collection, as if there were a "presumption of guilt, at least in the collection of personal data".

69.The potential and employment of ever more **invasive forms of online government surveillance** (recording and retaining citizens' web and e-mail data traffic) may lead to citizens feeling inhibited in their freedom to express legitimate forms of political dissent for fear of adverse consequences. A reduction in the spectrum of views expressed by citizens and their level of freedom of political involvement is detrimental to the quality of democracy.

70.Protection of citizens' **liberties in surveillance activities** is becoming more complex. Police use of advanced technologies – which is crucial for the success of "covert surveillance" operations – needs to be properly regulated in compliance with international standards of human rights, or citizens may lose "confidence" in the system and question its legitimacy. It is necessary to establish legislation defining norms, limits (what is allowed and what it is not) and responsibilities in surveillances activities by the state, taking into account also the de facto involvement of internet providers, private organizations and big "over the top" companies.

71.A better regulation **of time limits** for data retention was demanded, also taking into account the tendency of authorities and companies to use as much data for as long as possible, "as it could come in handy one day, one way or another".

72.**Freedom of expression** on the internet can be greatly affected by people's perception of being under surveillance in different contexts. When people become more aware of the existence of organizational surveillance of their online activities, they may choose to adopt an attitude of self-censorship in their behaviour in cyberspace and change the themes/contents and styles of their discussions.

73.The **coalescing** of **different practices in surveillance** makes it more difficult for individuals to preserve their right to intimacy and secrecy in communication, putting them at risk of being monitored by social institutions.

74.There is an extensive use of **new automated systems of smart surveillance**, together with automated systems for the acquisition, storage, and interconnection of information traceable to individuals and groups creates new areas that need to be adequately regulated at national and global level. This is particularly salient for the most recent features of surveillance (such as drones) that appear to lack a proper legislative framework.

75.There are risks of **exclusion, stigmatisation and reputation**. Individuals can be damaged, using (and abusing) statistical surveillance or other techniques of surveillance in the digital environment, when they are treated differently or are excluded from access to opportunities on the basis of the attributes of the group to which they belong.

76.**Infrastructures and network security** is considered an issue of growing importance and is related not only to the national sphere, but also to that of intergovernmental relationships, and regulations to combat crime.

77.There is a need for improved means and skilled operatives to combat the **criminal use of the Internet**, such as in financial transactions and money laundering, e-commerce of adulterated or illegal commodities (e.g. drugs or arms), the offer of criminal services, as well as forms of **cybercrime proper**, such as identity theft, hacking into data banks, etc.

FOCUS A12 - SAFEGUARDS, ENCRYPTION AND ANONYMITY

Several discussants highlighted that fast paced technical developments, besides creating new necessities for regulation, open increasing opportunities for misuse and abuse, which affect both organisations and individual citizens. In parallel to this, there is an expansion of cybercrime as a common criminal practice. This requires an expansion of possible safeguards to these hazards. Some of these safeguards are linked to the use of anonymity, encryption and the management of identity. During the discussion, the following distinctions were made. At the first level, there is ***identity****, where an authority declares things about a person that are real identifying attributes that can be verified or corroborated in some way. The next is* ***partial anonymity****, where an authority provides attributes about a person but does not disclose his/her identity. Then comes* ***pseudonymity*** *where a person may not know who the person is behind it but he/she does know that the person exists somewhere. In the case of pseudon ymity, it is possible to get repeatability, which is the most important function, like an email address, and then it is possible to be confident that the person is dealing with the same person, even if he/she doesn't know who that person is. Then there is* ***true anonymity*** *– the person knows nothing with any confidence. Also, the mechanisms that wrap around authentication in its broadest sense, including access control were discussed, with the understanding that, in the absence of authentication, there really is no notion of privacy. It was also highlighted that there is a lot of ongoing research on encryption technologies and its implementation for protecting privacy and securing communication, email exchanges and data on the internet. Some discussants quoted the on-going debate in some European countries about the use of encryption, revolving around the question of individual privacy and safety vs. collective safety. The following specific concerns were formulated.*

78.**There are limits to anonymity**. Generally speaking, most of the users think they surf the web anonymously but this does not correspond to the reality. Thus, it could be necessary to debunk the concept of anonymity. So far, people that think they are anonymous by using usernames and passwords have "leaked" so much information about themselves on the Internet that the sheer volume of data will enable them to be identified. It is important to note, for instance, that the IP addresses used for surfing on the net play an important role in identification. Furthermore, the "Internet of Everything" and the various interconnected devices represent a kind of "barrier" against anonymity. The very system of password protection appears obsolete. True anonymity is certainly possible but very difficult to achieve and beyond the capabilities of the average user.

79.**There is the issue of anonymisation / de-anonymisation**. Data analytics do not require the use of personal data. Various types of software allow data to be anonymised, as a first step to processing them for producing statistics, forecasting, etc. Nevertheless, there are technical means to relink anonymised data to individuals (de-anonymisation) – i.e. restoring the individual-relation in the long term with statistical methods. Therefore, in many cases, anonymisation is not a definitive step or at least this cannot be ruled out.

80.The relationship of **statistics (anonymised data)** with **individual-related data** is problematic and risky. Among the risky uses there is automated decision-making based on anonymised data statistics that can produce risks of exclusion. In fact, statistical analysis making use of big data allows groups of people with certain characteristics to single out, or even individuals that match some attributes. There are also many portals, which calculate a person's career opportunities according to their data (allegedly anonymised). But they can also prognosticate a user's professional career, or whether he/she is at risk of committing suicide or becoming ill. Information that can be exploited by insurance companies. Anonymised data are also used for diagnosis in Telemedicine.

81.**There is the issue of pseudonymisation, fake identity, anonymous search and anonymity**. In order to protect and hide their identity and personal data there are citizens who use fake identities and search the internet anonymously. Others access the web through free software for online anonymity, like Tor, or access the Deep web directly. This is particularly important in authoritarian regimes countries in which there is no freedom of expression. Nonetheless, anonymity and fake identity are also used for committing crimes on the Internet (also by using Deep and Dark web) like trade in drugs, weapons, child pornography, terrorism, etc. It can also cause uncertainty and mistrust in individual exchanges and transactions.

82.There are several **opportunities and problems** in the use of **cryptography**. The use of encryption combats the occurrence of fraud and crimes on the Internet, as well as the loss of data and is largely used by enterprises, organisations and the public administration to protect their own data and communications. Nevertheless, the use of encryption poses other problems. One is the limited interoperability of data sets using different encryption technologies, which can obstruct its use by the public administration, where data sets have to be linked to each other. That is why only auditable (i.e. susceptible to public scrutiny) encryption technologies need to be employed. A second problem is that the use of encryption (end-to-end) technologies prevents the state and law enforcement authorities to carry out surveillance activities and lawful interceptions against crime and terrorism.

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

Area B - **Internet Governance**

As indicated in the introduction, the focus groups manifested a general perception that the Internet environment is undergoing a process of overall change. Internet Governance is seen as a complex and multi-layered process which was seen as the product of choices, negotiations, conflicts, and power relations between numerous and diverse (public, private, non-profit) actors, with often different or even conflicting interests. The issue of providing guidance to this process and the remedies for the main problems encountered in the current use of the Internet occurred again and again in the discussion, thus making Internet Governance a discussion area in its own right, with specific *foci* of dialogue. In this regard, it is interesting to note that while all discussants had ideas and points of views on several issues and problems in need of overall guidance, not all were familiar with the concept of Internet Governance as such, and manifested much more divergent opinions than in the previous area of privacy. In fact, the various focus groups expressed different views on what one should mean by Internet Governance, its constituent elements, its fields of application and its very benefits and effectiveness. Different opinions were expressed also on governance actors, their interests, their respective roles and their democratic legitimacy. Views on two specific themes proposed in the discussion, the usefulness of an international multilateral treaty or other legal instruments and the prospect of parallel internets, produced the greatest divergence compared to other areas of the debate. What follow are the 5 main points of focus where dialogue can be articulated as they resulted from the discussion.

FOCUS B1 - DIVERGENCES ON HOW TO UNDERSTAND INTERNET GOVERNANCE

There were divergences in the terminology used, including the definition of "internet governance" itself. In a way, this provides an illustration of what some authors have maintained: i.e. that Internet Governance has been, and is being practised, long before such a term gained currency. This shows that even among people somehow involved in issues related to the current management of the Internet, there is a lack of consensus on what is meant by 'governance', hence the need to engage in dialogue on the subject. The different views presented in the discussion can be grouped into a number of categories.

83.**Restricted conception** of Internet governance, as pertaining mostly to the management of the technical functionality of the Net (such as infrastructures, rules, standards, IP addresses, protocols, etc.) with a special reference to names and domains. In some cases, ICANN was actually quoted as the main governance agency.

84.**More comprehensive definitions**, with reference made to the IGF formulation[7], considering governance as an overall function, encompassing legal, economic, social, cultural, developmental and technical interlinked issues and provided by a plurality of actors in their respective roles.

85.**Reductionist interpretations**, seeing governance as the mere exercise of a political rhetoric with no actual impact on real life situations: "It's only talk"; "The problem with Internet Governance is that everybody is heard equally and nobody does anything".

FOCUS B2 - DIFFERENT VIEWS ON THE CURRENT PERFORMANCE OF INTERNET GOVERNANCE AND THE AREAS TO BE GOVERNED

The divergence on conceptualisation presented above, reflected on the different views expressed regarding the way in which legal and policy responses of the many issues related to the Internet are provided. Such differences were sometimes traced back to the conflicting interests of the actors themselves (states, private business,

[7] "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".

civil rights advocates) and their divergent visions of what governance should be provided to the Internet. Several areas were named as calling for better governance: geographical denominations for domains and brands; harmonisation of user access to websites; better regulation of payment systems, including cryptocurrencies; cloud computing and its jurisdiction; monopolies in the web and the need for competition law; regulation of the deep web and dark web; combating "criminal" websites (child pornography, terrorist, jihadist, return fighters, etc.); universal protection of freedom of expression on the Net; regulating the use of encryption. Discussants saw Internet governance as a multi-faceted, multi-layered phenomenon involving multiple and sometimes contradictory interactions among numerous stakeholders at many different levels. Also, some very different ideas on which areas might need better governance were expressed. The different positions could be grouped as follows.

86.Current governance works fairly well at the level of **technical rules for** infrastructure, protocols and standards that ensure Internet operation in that they are governed by **independent organisation**s, such as ICANN, without much influence from governments. There is an attempt by governments and global lobbies to enter the process more decisively and control regulation.

87.Besides this technical level, when looking at **what is exchanged** on the Internet – content, data protection, privacy, IPRs, security – **conflicts** and **differences** in views **are much greater**. In this regard, there are doubts about the capacity of governments to find agreements.

88.The governance of the Internet is **not hierarchical** but is more similar to a horizontal mesh of rules, decisions, powers.

89.Cyberspace can be seen as a "**global commons**" and the Internet as a "**public good**", which, as a common infrastructure, cannot be managed by a single actor ("Internet is something belonging to mankind and, therefore, needs to be controlled jointly by mankind").

90.The current approach is considered **insufficient**, especially in light of the need for better **balance** between the **technical** and **legal protection of rights,** such as privacy or intellectual property rights.

91.The principle of **Net neutrality**, typical of the current management of the web, is being challenged, but its preservation remains crucial.

Focus B3 - Divergence concerning the governance models and the legitimate actors

There was divergence about the relative roles of the main Internet Governance actors, for instance state and non-state actors, which reflected ongoing discussions even in recent international meetings, where the division between multi-stakeholder and multilateral models was not reconciled. In fact, several discussants made more or less explicit reference to the multi-stakeholder model, as the only one really attuned to the multi-layered governance of the Internet. Others saw states as striving to exercise or reaffirm in cyberspace some of their sovereignty prerogatives (multilateral model). Others still were distrustful of the United Nations or ITU playing a major role, because of the eminent influence of states (including authoritarian states) and their bureaucratic apparatus. The Internet Governance Forum (even if it is a UN initiative) was seen by some as playing a positive role in defining the Internet Governance mechanisms from a multi-stakeholder perspective. But IGF was also object to criticism for its difficulties in reaching concrete results. Some mentioned also the NetMundial initiative. The need for a stronger European role and the position of infrastructure management has also been stressed. The various, differing views are summarized below.

92. The **major actors** are, in any case, **states** and global businesses such as Google, while an international institution for Internet Governance does not appear to be a realistic solution.

93. There is a need for an equal tripartite "**governance table**": states, industry/private sector and civil society (three domains equal vote). However, the feeling was that states are not at ease with the current governance system and oppose the equal participation of the other actors and are striving to exercise more power. It is necessary to avoid states playing the main role in Internet Governance.

94. A common **European position** on Internet Governance and on the web in general is missing, so that Europe appears at odds in the global debate on emerging issues such as that of security and the protection of citizens' rights. But the participation of the European Union, with a unitary point of view in the debate of Internet Governance, would be necessary. The EU initiative on the European cloud was greeted positively.

95. There seems to be no strategy for the over one billion of additional people from **developing countries** that are expected to **soon be on-line** and who might conceivably demand to have a bigger role in controlling and governing the Internet at the level of content and technological codes. This might require policies for an inclusive and multilingual approach.

96.There is the need to **improve the level of participation of the various stakeholders** and in particular the participation and the involvement of users as such (now they are included in the civil society organizations). The point of view of users is still lacking.

FOCUS B4 - PROS AND CONS OF A MULTILATERAL LEGAL INSTRUMENT OR DECLARATION OF PRINCIPLES FOR THE INTERNET

An important focus of the dialogue is whether there is a need for a general legal instrument such as an international treaty or a generally agreed framework convention to provide some order to the current "mesh" of heterogeneous provisions. The fields in need of regulation by means of an international instrument included: the general rules of Internet Governance; protection of citizens' rights in relation to surveillance and intelligence activities, especially as regards mass surveillance; cyber security; personal dignity and defamation; management of the physical infrastructure of the Internet; data protection, with a need for an International regulation of data traffic; harmonisation of the legal frameworks for e-commerce; "cyber warfare". Again, the views on the subject tended to diverge. Some discussants thought that some sort of legal framework, "Magna Carta" or "bill of rights" could help different regulators to respond to the diverse problems that originate from the developments of digital transition. Others were of the opposite view, preferring loose governance mechanisms that, according to some, can spontaneously "coalesce" to propose remedies whenever a new problem rises. Most of the discussants, regardless their position, were at any rate convinced that any effort to reach any kind of framework agreement would meet several obstacles and difficulties. Finally, a different point of view was manifested by some participants who declared themselves in favour of alternative forms of "soft" regulation. The different views could be grouped into some significant points of contention as listed below.

97.Some form of **treaty is needed** because, given the **transnational character** of the Net, it is not possible to deal with many emerging issues only by means of national legislation.

98.Internet Governance **cannot depend on self-regulation only** and some **juridical rules are necessary** in order to protect less resourced parties and to avoid them being marginalised. It could also help in achieving a better balance between users and service providers.

99.An emerging risk in the Net is that of **informational anarchy**, hence a better **internationally agreed typification** of certain behaviours as illegal or illegitimate is necessary.

100.There is a **general tendency towards some form of agreement** and this eventually will be reached for better or for worse.

101.Some **positive examples** were presented: the Budapest Convention on Cybercrime, promoted by the Council of Europe, undersigned by 40 countries worldwide, but which includes a sort of benchmark also for the countries who have not subscribed to it; the United Nations Convention on organised crime of the year 2000.

102.A controversial issue was whether the area of **Privacy** can be an object of a treaty; for some there is a need to have an international framework on Privacy, besides the various provisions in international conventions regarding the right to privacy. For others privacy cannot be the object of a treaty because there are too many definitions and divergences about privacy issues.

103.An alternative to a treaty could be some kind of Internet "**Bill of Rights**" or **declaration of principles** related to the Internet and addressed to citizens/users as bearers of entitlements and obligations, as a form of awareness building. The idea of citizens' security in the internet as a human right could be considered.

104.The main **objection to a treaty** was that the **self-regulatory capacity** of the relevant actors in the Net was to be relied on and preserved. There are also doubts about the capacity to obtain significant consensus on the issue, considering the divergence and irreconcilability of the positions of different states and other actors, which might lead to such downward compromises as to become virtually useless.

105.Legal instruments require a **long time to be agreed upon** and to come to effect. In the case of the Internet, this means that they would be dramatically out of sync with the pace in which changes occur. Hence, a treaty would be too static and lack the flexibility required by Internet Governance.

106.There is **no need of a Magna Carta** or a specific **Internet Bill of Rights,** which would be redundant since there is already the existing United Nations universal declarations of human rights. Much of extant Internet activity can in fact **be covered by the rules of "*netiquette*"** or **codes of conduct**.

107.An alternative could take the form of "**soft regulation**", with the creation of an "Inspirational environment", aiming at higher objectives and a process with the traction of nucleuses of dedicated actors to attract an ever-increasing number of willing participants with forms of "osmotic P2P dialogue". In this view, it should be possible to achieve that basic rules agreed in the offline world might also be applied in cyber space. This approach allegedly might be supported also by the commercial and industrial sector (examples of such approach: the Commonwealth Cyber Crime Initiative or the Ghana Cyber City initiative).

FOCUS B5 - DIVERGENT VIEWS ON "PARALLEL INTERNETS" AND THEIR FEASIBILITY/SUSTAINABILITY

A greatest degree of contentiousness concerned the notion of "parallel internets", meaning a part of the net with a number of built-in technical safeguards, aspiring to attract citizens worldwide to use an area of the Internet which is open to all but which adheres to certain ethical, technical and legal standards. It is to be noted that for some the expression "parallel internet" in itself was considered problematic or misleading. In fact in several cases it raised a rather negative response, being even assimilated to the praxis of authoritarian regimes, in which governments strive to control their society in cyberspace and apply censorship over content and strictly control and block the activity of their citizens online (goes against freedom of speech). Others interpreted it as a segregation control at the lower network layers. A completely different objection was based on scepticism of getting shared values and legal frameworks in the European Union to be the basis for a "Euronet" / "Schengen Net", subject to European jurisdiction and adhering to European standards. Other objections concerned more specific allegations and technical difficulties. On the other hand, a minority of the discussants found the notion interesting and gave examples of its feasibility. It has also been suggested that the concept of a network on top of the IP net and the integrative concept of "federated identity management" might be more acceptable and productive. The main doubts and objections are reported below, followed by more positive responses.

108.A "Euronet" would be **illusory** in that it would be at **odds with the global character** of the Internet and unfeasible for enterprises that strive for a global market. It could be identified with a desire to create new forms of protectionism in the cyberspace.

109.It is unclear who could decide and how to **access** the **parallel Internet,** what would be the criteria for admission, who should manage it, what infrastructures should be used. In particular, states might play much too strong a role and dictate rules of access.

110.It is **doubtful** whether a parallel Internet could grant **better protection** and safety to users, because attacks on content producers cannot really be blocked from the inside or from the outside.

111. With the present state of development of the Internet, it seems **unfeasible to attract a critical mass of users** that would be sufficient to ensure the sustainability of a parallel Internet. In the context of the switch from IPV4 to IPV6, it does not appear possible to develop a European technological area. This was in direct contrast with the view shown by other discussants (see below).

112. In contrast with the position presented above, the **switch from IPV4 to IPV6** appears to offer the possibility of an interoperable, but separate Internet.

113. Parallel Internets are **technically feasible**, for instance having an Internet in which two different kinds of packets would travel: those which would be "Euro tested" and those not.

114. Parallel Internets can be assimilated to an **extranet** like those created in the nineties, which in turn gave rise to trust federations. It could work as **more extended "walled garden"**, and as such possibly useful, albeit somehow limited and difficult to control. It is also akin to networks like GNUnet which are already working and gaining traction and that respect European standards. GNUnet's key differentiator is that it employs peer-routing instead of fencing off networks, thus strictly localizing any surveillance activities. Newer approaches such as HORNET that allow fast onion-routing should also be kept on the radar.

115. A network that would **make encryption** to protect the data of the users **the standard** could be desirable, but it should also take into account the legitimate needs of law enforcement agencies for crime prevention and security. Such an approach would require a rethinking of all related rules, including those for data retention, law enforcement and the like. It should also take into account the opposition of some countries.

116. The Internet is currently also **a network of networks**. Therefore, it is possible to use a separate network for certain matters (for instance for protecting the user privacy or to protect the web from attacks or mass surveillance interception by cable). According to some discussants, physical or logical separation of this network is not the solution. Because users want a net as big as Europe and more, very small networks would not be interesting for them. An interesting alternative could be that of a truly decentralised Internet, consisting only of mesh network connections, avoiding tunnels where everything comes together. And this, therefore, would also make it harder to attack anything.

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

Area C - **Intellectual Property Rights**

The third area that was discussed concerned the challenges posed by the development of the Internet – with all the new ways of providing, creating and distributing content and of generating value – for the traditional concepts and principles of Intellectual Property Rights.

In this field, we found significant convergence as well as divergence of views. Some discussants focused on the risk that authors, creative industries and other rights holders lose control over a work of art or an invention, making it more difficult to enforce forms of protection offered by current regulatory systems, whose basic principles were developed (and function fairly well) to protect the IPRs off-line. Several participants pointed to the problems related to the territorial fragmentation of the protection system. An issue that was felt to be particularly salient in Europe. Some discussants highlighted the disproportionate weight of monopolies and big corporations in the debate, with other voices being much less represented.

Other speakers were more intent on discussing how the Internet and the unprecedented opportunities it offers for creative collaboration, are challenging the conventional IPR regime. In their view this goes as far as questioning the underlying idea that exclusive rights promote the progress of science and useful arts under all circumstances and that the protection of IPRs should be considered an end in itself. While some maintained the basic principles of intellectual property retained their full functionality also in the on-line world, others advocated the necessity to find a new balance between the protection of property rights and the free movement of knowledge, taking full advantage of the unique opportunities created by the Internet as an open medium. In this regard some pointed to a tendency towards a "sharing economy" in the society. Reported below are the 5 *foci* of dialogue that could be gleaned from this part of the discussion.

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

FOCUS C1 - COMMON PRACTICES PUTTING AT RISKS AUTHORS AND CREATIVE INDUSTRIES

By and large, many examples were given of how the particular conditions of the new digital environment, offering huge opportunities to share content, makes it all the more difficult to enforce the forms of protection offered by the current regulatory system. In the arts and entertainment industry, the fruition of a copyrighted artistic product is increasingly independent of the possession of a specific physical medium (a record, a book, a CD). In this regard, several discussants pointed out how technical solutions made more or less legitimately available on the Internet, coupled with a widespread social practice, which downplays or utterly disregards issues of copyrights for certain products or certain forms of fruition, are greatly impacting the commercial environment, which might need to undergo a profound transformation. Also, the results of invention and scientific discovery are more exposed to the risk of being seized from their legitimate owners by means of cyber espionage, piracy and counterfeiting. Among the different problems highlighted, the following were the most recurrent.

117.**Streaming technologies**, coupled with different forms of **social networking** and peer-to-peer exchange, make it easy to exchange copyrighted content, greatly affecting the music, movie and television industry.

118.Apart from the more or less spontaneous initiatives of P2P exchanges of copyrighted content, there is a **proliferation of web sites that offer such pirated or counterfeit content** in exchange for personal data for borderline commercial purposes, thus also challenging user privacy. One publishing sector that is particularly challenged is that of text-books.

119.Challenges to IP protection are also coming from **new emerging forms of artistic production** typical of the so called "remix culture". In fact, practices like co-creation are blurring the distinction between the private/amateur sphere and the professional sphere in the production of content. This calls for new forms of regulation, such as for innovative musical expressions, which do not fit well in the standard protection regime.

120.The increased availability of authored intellectual content online magnifies the **problem of plagiarism, also on the mass media**. In this regard it can be noted that authors seem to have only limited knowledge of their rights and options about the protection of their IP, hence the necessity to promote their "self-determination", enabling them to make informed choices. There is an ongoing discussion whether it would be necessary to change from the current "opt-out" to an "opt-in" regime.

121.**There are difficulties** faced by **associations** also the protection **of authors' rights** to adjust to the on-line environment, where some of the traditional forms of protection are difficult to apply.

122.There are further technological developments in the near future, such as **3D printing**, that will pose a whole new set of challenges having a virtually disruptive effect on several manufacturing industries.

123.Increasing difficulties have been encountered by enterprises in **protecting their innovations and their patents** from theft, violation of industrial data and security.

Focus C2 - Rethinking IPRs vis-à-vis technology, social behaviour and legal rules

In connection with the challenges highlighted in the previous point, an important focus of dialogue concerns the question of whether the new scenario produced by on-line technology requires a profound reshaping of the IPR system or just a few fixes. In the focus groups, both points of view were presented, with various qualifications. One important discussion verged on the fact that while the copyright in itself, might become obsolete and requires deep revision, authors' rights (droit d'auteur) as human rights might not. The discussants made also various references to the fact the social perception of the acceptability of various forms of copyrighted artistic content on the Internet is a factor to be thoroughly considered in the development of the protection system. The major contentious points in this regard are listed below.

124.It was noted that a certain number of behaviours that **involve micro infringements of copyright laws,** such as downloading or streaming movies, exchanging music on a P2P basis, creatively remixing artistic content or using it for amateurish self-productions, are not perceived as socially censurable by a vast portion of the population worldwide, including Europe.

125.There is a **legal uncertainty**, paradoxically **produced by the rigidity** itself of the current system, which is considered to be too comprehensive in labelling as criminal so many forms of socially established behaviours. Hence there is a demand for more flexibility in better nuancing what can be considered lawful use and what is not, and drawing new boundaries between commercial and non-commercial use – e.g. in streaming – and revising the notion of piracy itself.

126.There is a need for **redefining the conditions of "fair-use"** for non-commercial exchanges of creative content on the Internet, making it more attuned to the current established behaviours of the users, striking a balance between IPR and the right of expression. The Creative commons system could be a positive model.

127.There also appears to be a need to **redefine the creative product from the legal point of view** to adjust it to present forms of on-line fruition. For instance, with respect to the notion of "private copy", which in the analogic environment is identified by a physical object while in the digital environment is identified by a digital entity, with completely different limits and possibilities of fruition[8].

128.The standard instruments for **Digital Rights Management** (commonly utilised to combat digital piracy) are undergoing a process to make them simpler and more responsive to new necessities and to achieve a better user interface. As a matter of fact DRM is considered of controversial nature[9].

129.Forms of **co-regulation between industry and government** can generate really effective regulatory systems to overcome the shortcomings of the current system.

130.There is a need for a **broader portfolio of instruments**, especially **of a conciliatory nature**, in order to overcome the difficulties of enforcing existing legislation. An important role can be played by case law in attuning the juridical rules and balancing rights.

131.The possibility of **generalising the use of symbols and pictograms** to inform users of what they can and cannot do with the rights associated to the contents they are dealing with needs to be considered.

[8] Consider the following statement of Bruce Schneier: "Digital files cannot be made uncopyable, any more than water can be made not wet", https://www.schneier.com/crypto-gram/archives/2001/0515.html

[9] See for example: https://defectivebydesign.org/ and also point 42 in this text.

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

FOCUS C3 - NEW BUSINESS MODELS FOR CREATIVE INDUSTRIES

A focus of dialogue related to the above revolved around the new business models being experimented by the creative industries in order to respond to the challenges of a market in which the enjoyment of artistic products is more and more independent from the possession of a physical object (see above). That is, models that mark the transition from the acquisition of a "private copy" to the fruition of a service or of a reproduction right. In this framework, discussants proposed examples of remuneration of artistic creation based not so much on the product as such (e.g. a new song album), which could even be offered for free, but to its collaterals, such as live concerts, merchandising, advertising. Some discussants, on the other hand, pointed out that there are also significant forms of resistance to transformations based on purely repressive practices and aggressive litigation, which, however do not always prove to be really effective. The main examples of emerging business practices were the following.

132.New business models for the fruition of mass culture are being promoted by big companies that make use of technological and commercial innovation in order to **offer "legal"** (and safe) **fruition of artistic copyrighted content** in ways (such as subscriptions) that make it easier and more convenient (iTunes, Spotify, NetFlix, etc.).

133.While these new models of fruition and marketing multiply and develop, they **coexist with the traditional models** of big entertainment industry (which now is also present on-line). This is giving rise to a complex process of adaptation and redefinition of relationships.

134.**Intermediaries** are, in fact, **changing and increasing** in number. Together with traditional publisher and recording companies, there are new actors such as search engines, social networks, streaming providers. This is also leading to a change in the behaviour of authors that have to deal with a plurality of intermediaries, such as publishers and their platforms, marketing companies, other providers, etc.

135.The **publishing sector** is **undergoing profound changes** with companies such as O'Reilly ed., which digitalise and distribute books and manuals using a new Digital Rights Management in which books can be legitimately downloaded for free or at a very reduced cost.

FOCUS C4 - HARMONISING IPRS IN EUROPE AND WORLD-WIDE

An important focus of dialogue that emerged from the discussion is related to the fact that the protection of intellectual property is further complicated by the global character of the Internet so that violators may reside, and be subject, to the rules of a different jurisdiction than that of the place in which the violation occurs. Several discussants pointed out that in Europe the issue of territoriality is further complicated by the fact that IPR protection regimes are fragmented by national boundaries, putting European actors at a disadvantage with respect to other continental markets. Several references were made to the need for a harmonisation of IPR national legislation, especially as regards copyright regulation and the current debate accompanying the ongoing process of revision of the EU copyright legislative framework. The following are the contentious points that emerged from the discussion.

136.The **fragmentation of copyright regimes at European level** is a major factor limiting the capability of European enterprises to emerge in the entertainment industry, putting them at a disadvantage with competitors from USA, since a provider of content (e.g. movies) has to negotiate broadcasting rights country by country.

137.The **need for harmonisation** of IPR regimes does not entail only copyright, but also other areas, like brand or names and domains, where some advancements are taking place. Hence the necessity to reach a **unique IP title valid for all the European Union**. There is also the need to make more expedite the patent process, which currently is considered too slow with particular regard to digital technologies.

138.There is support for ongoing the "**Unitary Patent**" project, aimed at centralising the judicial courts at European level to reach a consistent ruling system on patent infringements.

139.There is the need to negotiate a **reciprocity principle** between the different IPR systems in various countries – a difficult negotiation because of the many differences and the interests of pressure groups from the current intermediaries that profit from the current fragmentation

FOCUS C5 - EVOLUTION OF THE CURRENT IPR REGIMES AND THEIR EFFECTS ON INNOVATION

A last focus for dialogue concerns the debate on whether the particular features of the Internet and the unprecedented opportunities for creative collaboration it offers, are the underlying idea of current IPR regimes that exclusive rights promote the progress of science and useful arts under all circumstances. On this issue, views were rather polarised, with some discussants reaffirming that the current "property logic" remains the key factor to protect and remunerate intellectual creation, discovery and innovation. Other participants, instead, maintained that an exceedingly rigid and standardised understanding of IPR can lead to prohibitive practices and chilling effects on the economy and innovation. The experience of Open Source Software and of other "open innovation" initiatives were mentioned, to show that innovation can be triggered and value produced also by a logic other than that of property. While some reference was also made, beyond the Open Source Software, on the debate on the more radical "free software" perspective. While coexistence with diverse approaches was generally considered appropriate, some difficulties in making the different systems compatible were presented. What follow are the more salient contentious points that were raised during the dialogue.

140.There is a growing recognition that – at least in some fields, such as the field of software production – it is possible to have **innovation based on open, collaborative research and developmen**t. Also important global actors, such as ICANN support the principle of the so-called "permissionless innovation".

141.There are **problems in adjusting the current patent system to software development**, which is often co-produced in an "open source" regime. There are frictions in integrating the open source approach with the standard patent regime, for instance when big companies try to apply proprietary rights on software that was originally developed as "open source", as opposed to the "free software" approach.

142.A different kind of paradox is produced by the **European rule on open access to academic papers** in that the author is not remunerated but the publisher which makes the article available limits access in order to be remunerated from it.

143.Current **patent management can lead to conglomerates slowing down innovation** (like in the case of the "patent wars" on smartphone between major companies). There is also the case of leading industries that buy patents and do not implement them in order to block the innovation of their competitors. Another "chilling" practice is that of big companies that register some patents without either exploiting nor revealing them, making it difficult for small enterprises and researchers even to know if they are producing innovation or not.

Foci of Dialogue Chart

Area A - **Privacy and Integrity**	
Focus A1 - Risky user behaviours	**Focus A7** - Personal identity management
Focus A2 - Security problems of enterprises in protecting digital data assets	**Focus A8** - Informational self-determination/data sovereignty
Focus A3 - Security risks concerning personal data legitimately managed by public or private organizations	**Focus A9** - Gap in the regulatory and enforcement system
Focus A4 - Education and awareness raising	**Focus A10** - Responsibility of providers and system developers
Focus A5 - Legitimacy/Opaqueness of current business models based on personal data	**Focus A11** - Surveillance, security and democracy
Focus A6 - Emerging "privacy friendly" business models	**Focus A12** - Safeguards, encryption and anonymity
Area B - **Internet Governance**	
Focus B1 - Divergences on how to understand Internet governance	**Focus B4** - Pros and cons of a multilateral legal instrument or declaration of principles for the internet
Focus B2 - Different views on the current performance of Internet governance and the areas to be governed	**Focus B5** - Divergent views on "parallel internets" and their feasibility/sustainability
Focus B3 - Divergence concerning the governance models and the legitimate actors	
Area C - **Intellectual Property Rights**	
Focus C1 - Common practices putting at risks authors and creative industries	**Focus C4** - Harmonising IPRs in Europe and world-wide
Focus C2 - Rethinking IPRs vis-à-vis technology, social behaviour and legal rules	**Focus C5** - Evolution of the current IPR regimes and their effects on innovation
Focus C3 - New business models for creative industries	

PART II
Guidance for engagement: operational suggestions and criteria

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

As indicated in MAPPING Deliverable D2.1, Dialogue and Participation Plan (DPP), the MAPPING project aims to provide a variety of fora in which a wide spectrum of relevant actors are engaged to be confronted, in a multi-disciplinary and polycentric environment, with the many problematic aspects of the digital transition. The challenge is to foster a constructive and informed dialogue between diverse actors, in order to maximise exchange of knowledge and collegial cooperation. A major outcome of this dialogue will be the formulation of a Road Map on the governance of the digital transition, through a participatory process during the life-span of the project[10].

Such dialogue is conducted mainly with the initiatives of the substantive Work Packages that are dealing with Internet Governance (WP4), Privacy (WP5) and Intellectual Property Rights (WP6), each with their own cluster of activities with specific themes. The common framework of the Dialogue and Participation Plan is meant to add value to the project as a whole by promoting exchanges between the different threads of dialogue, which are considered to be interrelated. Thanks to the focus groups we received the contribution of a vast array of stakeholders, which provided both inputs on the content of forthcoming dialogue initiatives (PART I) and inputs on the way in which such initiatives can be better implemented (PART II).

These operational suggestions to monitor the progress of the MAPPING dialogue are dealt with in this Second Part of the Guidelines in which we reconsider the assumptions of the DPP against the results of the focus groups discussion and the way in which it was carried out.

1. Facilitating engagement through a transformational approach to dialogue and participation

In the DPP, **participation** was conceptualised according to the definition formulated in a 2010 study for the Council of Europe, as:

> *"the **opportunity** which is made available for **those who wish to do** so to contribute to a **decision-making process** which (they believe) affects them (or in which they believe they should be heard), and to **the mechanisms** which enable them to make a contribution"* (Souter, COE, 2010).

[10] See MAPPING D2.3, "Road Map – First draft" September 2015.

According to this view participation can take multiple forms, with different degrees of involvement of the relevant actors in the decision-making process. In MAPPING the main form of participation was meant to be that of the (policy) **dialogue**. That is:

> *"a **structured deliberative process**, based on the **exchange of knowledge** between a **plurality of actors** on issues that are at the same time **politically controversial** and **technically complex**"* (UNRISD 1997; Cuppen 2010; Adler 2003).

Accordingly, the dialogue in the project is seen as a transformational exercise**,** concerned with restructuring the problem areas confronted, empowering the relevant actors and forming networks and coalitions to support the agreed solutions.

The experience of the focus groups provided some indications to support and better qualify the approach chosen and described in the DPP.

In this paragraph we make a few general considerations, while in the following paragraphs we present more specific suggestions, according to the engagement strategies as they are proposed in the DPP.

The first consideration is related to the "transformational" approach to dialogue as such. First of all, in the focus groups we could witness the interaction of various stakeholders (scientists, technologists, professionals, practitioners, industrialists, activists, public decision-makers, etc.) as representatives of diverse epistemic communities. They appeared to be in fact bearers not only of interests, but also of their own visions and interpretations on the salient aspects of the digital transition. Given these characteristics, during the dialogue there were occasions of redefining and restructuring the issues proposed through negotiations about the meanings and the issues proposed. In fact most of the participants perceived the issues discussed as an area where there is not yet a consolidated knowledge and in which much is still to be explored and qualified.

Secondly, an inclination towards a transformational approach was shown by the general interest towards finding ways to deepen the debate, to be kept in "the loop" of the dialogue process, with a demand for action oriented follow-up of the exercise.

On the basis of the outcomes of the focus groups and of the attitudes of the participants, we have reconsidered a set of components that should allow us to operationalise the transformational approach proposed with which we deal in the following paragraphs.

"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. Operational suggestions for the three MAPPING dialogue strategies

The dialogue and participation activities, which are an integral part of the MAPPING project, should be understood as a change oriented process of negotiation between different interpretations. Structured as a spiralling pathway, such process is meant to progressively broaden its target along three strategies of engagement, involving wider and wider categories of interlocutors, from partners to stakeholders, to the wider public and "Netizens". As it was mentioned earlier, a fundamental outcome of this process will be the participatory formulation of a Road Map, including policy guidelines.

The first dialogue strategy, **mutual learning among partners**, is the one that is occurring among the 13 MAPPING project partners themselves. This was kicked off with a first round of discussions (WP2 Task 2.1) held in month 1 of the project. In fact the partners themselves represent a vast spectrum of actors engaged with Internet related issues, such as digital rights NGOs, law enforcement agencies, business federations, regional policy makers, training specialists, technologists, academics and researchers of various disciplines (law, social sciences, etc.).

The second strategy, **stakeholders' involvement**, is ongoing as well, having started with the MAPPING Extraordinary General Assembly (EGA), which extended the dialogue to a broader audience by engaging relevant stakeholders in the domains of Internet Governance, Privacy and Intellectual Property Rights to jointly identify issues and challenges related to the digital transition. From then on stakeholders have been engaged in several dialogue initiatives (in different formats), relating to the three thematic drives of the project. An important milestone in this regard is the First General Assembly of September 2015 in Hannover.

The third strategy, **public engagement**, is meant to be launched at a more advanced stage of the project and is geared at engaging the wider public. It is at this point that the key issue will be tackled of how European citizens can be enabled to effectively participate in the governance of the Internet, as well as how they can be empowered to fully exercise their personality rights on the web.

The focus groups exercise has allowed us to provide suggestions on how to better adjust the dialogue tools and procedures to the typology of actors involved and the level of engagement. In the following paragraphs these suggestions are reported for each of the three strategies.

2.1. Mutual learning among partners

The first dialogue strategy is meant to make the most of the fact that the MAPPING consortium brings together all types of stakeholders by encouraging initiatives of mutual learning and the exchange and optimisation of the intelligence and knowledge acquired in the substantive WPs (WP4, WP5 and WP6). This should bring a shared and more comprehensive understanding of the features and directionality of the overarching process of the digital transition, which could inform the final Road Map and the "Heritage" initiatives (WP7), geared towards ensuring the continuity of the MAPPING process after the project conclusion.

In this regard, the implementation of the focus groups by the partners can be considered an important passage of such learning experience in that almost all of them participated into a dialogue exercise, which simultaneously dealt with the three thematic areas of the project, irrespective of their specific expertise.

On the other hand, the partners mobilised their specific competences and interests to adjust the exercise to their national context in order to effectively select, approach and involve the participants, as representatives of relevant stakeholder groups. In this regard, they also made use of their contacts and social capital. Below we present some operational suggestions to improve the mutual learning strategy.

a. **Cross-fertilisation among partners**. In order to enhance the exchanges that are at the basis of mutual learning, besides incentivising the, already ongoing, presence of partners to the substantive dialogue initiatives promoted by each thematic WP, we suggest to devote a specific space on the overall lessons learned in the dialogue process during the forthcoming (interim) Steering Committee Meetings. Furthermore, ad hoc Skype meetings for exchanging lessons learned could be organised, after a significant set of thematic initiatives have been conducted. The main lessons could be recorded and used to inform the Road Map.

b. **Self monitoring of dialogue initiatives**. In connection with the point above, it seems important to foster a shared awareness and understanding by all partners of the overall progress of MAPPING process, as one of ever expanding concentric circles of dialogue and engagement. In this regard it is appropriate to monitor and exchange views on four interrelated aspects: 1) the incremental (provisional) outcomes of the thematic drives, including the progress of the Road Map formulation; 2) the kind and quality of the actors engaged; 3) the political nodes leading to policy formulation; 4) the obstacles and facilitating factors encountered. To this effect a specific discussion on these items could be held each semester, either in connection with a general meeting such as a (interim) Steering Committee Meeting or with an ad hoc remote meeting. This exercise should also improve the synchronisation of the partners' efforts with the comprehensive thrust of the project.

c.**Contextualisation**. As they did for the implementation of the focus groups, the partners can play an important role in contributing to make the MAPPING substantive activities more context specific. In this, they can bring in their particular expertise, their knowledge of the characteristics of their country and the perspectives and demands of the social and professional groups with which they are connected.

d.**Discussion on stakeholders' engagement**. Through the effort of all partners, diverse groups and networks of stakeholders were contacted and participated in the focus groups. In doing so, different kinds of approaches were experimented and different interests and concerns were registered. It would be useful to have a discussion ad-hoc on the kind of actors better suited to actively participate in MAPPING initiatives and the best ways to engage them.

2.2. Stakeholders' involvement

The second strategy concerns the extension of the dialogue to a broader audience by engaging relevant stakeholders in the various MAPPING clusters of activities.

In the DPP the stakeholders have been operationally defined as bearers not only of interests and risks, but also of diverse and original perspectives and visions on Internet Governance, Privacy and Intellectual Property Rights able to bring crucial insights to the interpretation of the main challenges of the digital transition. Stakeholders' involvement is thus understood as a complex endeavour starting with the identification and categorisation of stakeholders followed by their involvement and engagement in further activities. In this regard, the results of the focus groups have provided important insights into understanding their expectations, interests and agendas in relation to the MAPPING project[11].

[11] See Introduction, paragraph 2.

In the first part of this document we have presented the major focuses of interest manifested by the participants, while discussing the substantive issues proposed in the outline. Here we make some considerations on the attitudes and concerns shown by the participants during the process.

First of all we note that most of the stakeholders involved (including those with an academic background) showed a hands-on experience of the problems at stake and were interested in discussing solutions or alternative ways of addressing the issues.

We also recorded a good response, with very few exceptions, on the interactive, multilateral and multidisciplinary approach chosen. Most of the participants were interested in interacting with bearers of different perspectives, expertise and professional or disciplinary background. They considered equally stimulating to discuss in an interrelated way the three thematic areas, and so addressing both the issues of which they were fully cognisant and those that pertained to fields outside their direct experiences. In this regard it was also possible to recognize many intersections between privacy, Internet Governance and Intellectual Property Rights.

As described more extensively in Part I, we registered both convergence (especially in the field of privacy) and divergence (on some issues of Internet Governance and Intellectual Property Rights) of views. In any case the discussion was never confrontational and a constructive spirit prevailed, with an orientation to reach a shared understanding of the issues. Some discussants (especially representatives of Public Administration and enterprises) made reference to the fact that the anonymity allowed them to speak more freely and candidly.

Most of the stakeholders shared an orientation towards change, grounded on the feeling of living in a transitional moment for what regards the impact of digital technologies on society. This came together with a certain degree of skepticism on the capacity of the current governance system to provide an adequate guidance to such transformations.

Finally a majority of the stakeholders involved in the focus groups declared to be interested in the exercise and in being updated about its outcomes. They were also interested in taking part in focused action-oriented follow up activities.

In fact, the focus groups, together with other dialogue initiatives carried out in the three thematic work packages, provided evidence that there are good opportunities for stakeholders' involvement in the MAPPING process.

The participants themselves in some cases declared their interest to be reconvened in other ad hoc meetings to better address some topical issues touched in the discussion. They also showed their willingness to be integrated into the dialogue initiatives already scheduled in the DPP for the three thematic areas. On the other hand, this willingness is not unconditioned and requires an attention to respond to their expectations, interests and concerns, including requests for visible outcomes.

Some suggestions to make the most of the stakeholders' engagement are presented below.

e.**Solidifying and routinising participation**. Up to this point stakeholders relevant to MAPPING have been mostly convened to specific events and initiatives (including the focus groups). Some groups have also expressed the interest to meet again on a semi-regular basis to update or deepen the issues discussed. What seems to be needed is to develop viable and "light" instruments and procedures to channel their energy towards the MAPPING plan in its entirety and to keep the momentum in-between initiatives. In other words, to turn groups of contacts into communities. This would require keeping both at the central coordination and at the national level an active memory of the people involved in order to continue to appraise them on the progresses of the project, to collect their feed-back and to orient them to the new initiatives that can better respond to their interests.

f.**Action oriented follow-up**. The focus groups discussions have highlighted deep concerns on many problematic aspects of the digital transition and the need for viable solutions in terms of policies and legislation. These concerns could not be answered within the limited scope of the exercise, but significant follow up was requested. This opens the way to an active participation in the initiatives of the thematic drives in which policy solutions are going to be sought and proposed. One important outlet could be the process for the formulation of MAPPING Road Map, mentioned also below (see point i.). To this end, the future activities of the thematic drives should take into account the concerns of the stakeholders as documented in the Part I of this document and the topical issues at national level.

g.**Preserve and enhance the diversity of relevant stakeholders**. The focus groups have confirmed the fruitfulness of the interaction of stakeholders from very different backgrounds and affiliations. This diversity should be preserved and increased (for instance representatives of civil society organisations and law enforcement agencies, which were less represented). To this purpose specific engagement strategies addressed to different categories of stakeholders should be devised, also making use of and integrating the social capital and commitment of the various partners, who in their national context have sometimes been able to reach certain categories more than others. The map of stakeholders (CSOs, governments, science foundations, SMEs, local authorities, universities and research centres, etc.) already created by EPMA could be integrated and used proactively for the elaboration of a detailed contact list of actors, based on existing partners' databases and contacts.

h.**Improving multidisciplinary debate: negotiations on meanings and values**. The focus groups were an occasion for an interdisciplinary as well as a transdisciplinary debate (in a broad sense) integrating not only different disciplines, but also knowledge, values and interests outside the academic domain. In order to be productive, such interaction among different "epistemic communities" should cope with terminological misunderstanding and avoid conceptual oversimplification in reaching a common ground of discussion. On the basis of this experience, we suggest that further occasions of dialogue should create an enabling environment for the full expression and negotiation of different visions, positions and interests to foster the production of new ideas and meanings, develop a common understanding of the issues at stake and leading to shared, realistic and viable solutions to inform policymaking.

i.**Stakeholders' empowerment**. The participants in the focus groups as well as the other stakeholders mobilised in the MAPPING process are already engaged in various ways in diverse problem areas of the digital transition. They also take part in several networks and communities of practices. As the project progresses, the challenge is to turn this network of networks into one or more robust coalitions to provide inputs to and to advance the policy instruments, such as the Road Map and the Heritage plan, that should provide solutions and remedies to some of the issues that are being singled out in the thematic drives of Privacy, Internet Governance and Intellectual Property Rights. Eventually a consistent number of stakeholders should be integrated into this process. An important role in this regard can be played by the general Assemblies that year after year offers a space for the most active stakeholders in the three thematic areas to come together and coalesce their efforts into the overall MAPPING strategy.

j.**Globalising stakeholders' engagement**. The inclusiveness and diversity of stakeholders should apply also to geographical criteria. In the focus groups discussion several references were made in support of the ongoing efforts to extend MAPPING "constituency" to stakeholders outside Europe in order to bring in perspectives and interests typical of other geopolitical areas. In this regard initiatives of dialogue were already experimented with for instance in the United States and the overture to a greater engagement of China

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

appears certainly appropriate. Some discussants put a special emphasis to find ways to include more and more the voice of developing countries that are likely to massively enter the cyberspace in the near future.

k.**Participating in the broader dialogue arena**. The MAPPING project is not occurring in a vacuum, but in a world context in which a large number of initiatives, at different degrees of institutionalization, are occurring to provide guidance to the digital transition. Thus the terrain for the engagement of stakeholders will be not only that of MAPPING initiatives, but the broader context in which our project is meant to play a role, in connection with fora such as the Internet Governance Forum, the initiatives of the Council of Europe or other Governmental or multilateral bodies, including the European Union. As our activities progress, relevant stakeholders could interact with MAPPING partners in bringing our outcomes and perspectives in the broader context of global Internet Governance.

2.3. Public engagement

The third strategy indicated in the DPP concerns the engagement of the public. It is at this point that one of the key issues of the project is going to be tackled, i.e. how European citizens can be enabled to effectively participate in the governance of the Internet, as well as how they can be empowered to fully exercise their personality rights on the web.

It is widely recognised that the notion of public engagement is controversial in terms of approaches and evaluation of results. In fact, the very concept of "public" must be nuanced. Because of the above mentioned reasons, the DPP, in accordance with the MAPPING Description of Work (DoW), foresees that the major efforts to foster public engagement are to be initiated **in the second half of the project**, i.e. at a more advanced stage in the production of content and in the refinement of effective participatory instruments. This notion was further reinforced in the Steering Committee Meeting that was held in Geneva on 17-18 March 2015, where it was reiterated that public engagement initiatives should be carefully considered and implemented.

As mentioned in Part I of this document, the focus groups discussions provided some inputs that could be taken into account when formulating the public engagement strategy.

First of all, we can recall that a lack of competence, understanding and awareness in large sectors of habitual Internet users was considered as a major problem by a large majority of the discussants, which suggested different kinds of educational or awareness raising initiatives (see Part I, Focus A4). On the other hand, the notion that the public of users should be considered as multi-layered and differentiated was also reinforced. Especially differences in understanding and familiarity with the technical means were highlighted for age groups (children, youth and elderly people) and social strata.

Hence there is the need to devise policies and approaches differentiated by the different groups and their peculiarities and needs. Among those were considered also more advanced groups of "Netizens", who have a better than average familiarity with and understanding of the medium (see Part I, Focus A1). In this regard it is also worth stressing that this segment of "public" must be understood as having their own perspectives, concerns and demands. Thus strategies of engagement need also to take into account the active role and the coping strategies of users that – albeit varying strongly in skills and awareness – are nevertheless full of agency for what concerns their presence in the Internet.

On the basis of the observations formulated above, we suggest that in view of devising effective strategies for public engagement, the following items could be considered.

l.**Users education**. Different approaches to the possibility of educating different categories of users to a more informed and safer use of the Internet, their feasibility and impact should be considered in designing the public engagement strategy. To this end we could reflect on how to make the most of the already planned MOOC program. Furthermore different educational policies and initiatives addressed to different targets, with a special regard to children, youth and elderly people could be suggested as an item of the Policy Observatory (MAPPING WP3).

m.**Awareness raising**. Similarly, how to achieve a better awareness of different groups of users on the risks and opportunities, should be part of the formulation of the public engagement strategy. Also in this case the Policy Observatory could record and provide examples of different approaches and policies of awareness raising.

n.**Digital self-help**. An important contribution to formulate a public engagement strategy could come from the consideration of the coping strategies, self-organisation and self-help devised and practiced by certain segments of Internet users – especially, but not exclusively, "digital natives" – that were reported in Part I of the document (see Part I, Focus A4, point 27).

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

o. **Ad-hoc approaches for different categories of users**. The fact that the public of "Netizens" ranges from Netizens with an almost total lack of awareness and understanding of the underlying architecture of the Net to Netizens that are fully aware and skilled activists of privacy protection, should be operationalized when formulating engagement strategies in order to be able to differentiate the approaches accordingly.

p. **Active digital citizenship**. Planning public engagement could receive significant inputs by the attention that will be devoted in forthcoming planned activities focused on bottom-up participation within national and European-wide debates, as well as in international Internet governance fora. The efficacy of on-line mechanisms for increasing citizen participation should receive special attention, including participation via novel and "smart" approaches to capacity and confidence-building. At the same time obstacles to meaningful participation of individuals in the development of Internet Governance processes should receive due attention, starting from the indications in this regard provided by focus groups discussion.

OPERATIONAL SUGGESTIONS CHART

Mutual learning among partners	
a. Cross-fertilisation among partners	c. Contextualisation
b. Self monitoring of dialogue initiatives	d. Discussion on stakeholders engagement
Stakeholders' involvement	
e. Solidifying and routinising participation	i. Stakeholders' empowerment
f. Action oriented follow-up	j. Globalising stakeholders' engagement
g. Preserve and enhance the diversity of relevant stakeholders	k. Participating in the broader dialogue arena
h. Negotiations on meanings and values	
Public engagement	
l. Users education	o. Ad-hoc approaches for different categories of users
m. Awareness raising	p. Active digital citizenship
n. Digital self-help	

SUMMARY

The focus groups exercise has provided important inputs to upgrade MAPPING's dialogue and participation strategies formulated in the DPP, both in terms of content (see PART I) and in terms of operational suggestions on how to conduct the dialogue initiatives in themselves (see PART II).

In PART I we have presented the views on the major issues of the digital transition of more than 150 experts and stakeholders from 11 European countries and organised them in a number of salient *foci* for the informed dialogue on Privacy, Internet Governance and intellectual Property Rights that the project aims to foster.

In PART II we have taken advantage of the lessons learned in carrying out the focus groups to formulate some practical suggestions on how better manage the dialogue initiatives in tune with the attitudes and concerns of the participants. Such suggestions were organised according to the three dialogue strategies of the project: mutual learning among partners, stakeholders' involvement and public engagement.

Both the *foci* of dialogue and the operational suggestions have also provided inputs to the draft document to launch the process for the formulation of the Road Map that will be one of MAPPING major outcomes[12].

Here below we present together the charts summarising the *foci* of dialogue discussed in PART I and the operational suggestions formulated in PART II.

FOCI OF DIALOGUE CHART

Area A - **Privacy and Integrity**	
Focus A1 - Risky user behaviours	**Focus A7** - Personal identity management
Focus A2 - Security problems of enterprises in protecting digital data assets	**Focus A8** - Informational self-determination/data sovereignty
Focus A3 - Security risks concerning personal data legitimately managed by public or private organizations	**Focus A9** - Gap in the regulatory and enforcement system
Focus A4 - Education and awareness raising	**Focus A10** - Responsibility of providers and system developers
Focus A5 - Legitimacy/Opaqueness of current business models based on personal data	**Focus A11** - Surveillance, security and democracy
Focus A6 - Emerging "privacy friendly" business models	**Focus A12** - Safeguards, encryption and anonymity

[12] See MAPPING D2.3, "Road Map – First draft", September 2015

Area B - **Internet Governance**	
Focus B1 - Divergences on how to understand Internet governance	**Focus B4** - Pros and cons of a multilateral legal instrument or declaration of principles for the internet
Focus B2 - Different views on the current performance of Internet governance and the areas to be governed	**Focus B5** - Divergent views on "parallel internets" and their feasibility/sustainability
Focus B3 - Divergence concerning the governance models and the legitimate actors	

Area C - **Intellectual Property Rights**	
Focus C1 - Common practices putting at risks authors and creative industries	**Focus C4** - Harmonising IPRs in Europe and world-wide
Focus C2 - Rethinking IPRs vis-à-vis technology, social behaviour and legal rules	**Focus C5** - Evolution of the current IPR regimes and their effects on innovation
Focus C3 - New business models for creative industries	

OPERATIONAL SUGGESTIONS CHART

Mutual learning among partners	
a. Cross-fertilisation among partners	c. Contextualisation
b. Self monitoring of dialogue initiatives	d. Discussion on stakeholders' engagement
Stakeholders' involvement	
e. Solidifying and routinising participation	i. Stakeholders' empowerment
f. Action oriented follow-up	j. Globalising stakeholders' engagement
g. Preserve and enhance the diversity of relevant stakeholders	k. Participating in the broader dialogue arena
h. Negotiations on meanings and values	
Public engagement	
l. Users education	o. Ad-hoc approaches for different categories of users
m. Awareness raising	p. Active digital citizenship
n. Digital self-help	