United Nations
Educational, Scientific and
Cultural Organization

UNESCO Chair in Data Privacy
Catalonia

UNIVERSITAT ROVIRA I VIRGILI

ANSWERS TO QUESTIONS FOR UNESCO'S COMPREHENSIVE STUDY ON INTERNET RELATED ISSUES

Prof. Josep Domingo-Ferrer, Chairholder, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Tarragona, Catalonia
(http://unescoprivacychair.urv.cat , http://crises-deim.urv.cat/jdomingo)

November 23, 2014

DISCLAIMER. The viewpoints expressed below are Prof. Domingo-Ferrer's own and do not commit UNESCO.

A. Questions related to the field of Access to information and knowledge

1. What can be done to reinforce the right to seek and receive information in the online environment?

A problem with the current situation is that the Internet search engines are in the hands of very few companies, basically U.S. companies (Google, Yahoo!, Microsoft). Hence, the access to information is dominated by very few big players from a single country, who are able to determine whether information is easier or more difficult to find. Unfortunately, the only significant search engine not controlled by the previous companies is Baidu, controlled in turn by a non-democratic government (China).

Breaking the above oligopoly would no doubt reinforce the right to seek and receive information. Initiatives like DuckDuckGo, which is an independent and privacy-aware search engine, go in the right direction, but they still lack critical mass.

2. What mechanisms can develop policies and common standards for open-licensed educational resources and scientific repositories, and for the long-term preservation of digital heritage?

I suggest to take as a model what is probably the most successful educational resource nowadays: the Wikipedia.

Stable financial support by the international public powers (maybe UNESCO itself) to Wikipedia and other existing free and neutral knowledge repositories could enable them to cover other roles, such as long-term preservation of digital heritage. Of course, such a support should not entail any political meddling in the contents of those repositories.

3.How can greater progress be made as regards inclusive strategies for women and girls as well as marginalized and disabled people?

A necessary and essential pre-condition is to increase literacy among those groups of people. And teaching them English or another of the world's major languages would also help them to access worldwide and neutral sources of knowledge. Then comes of course facilitating access to Internet, for example, with free Wi-Fi networks in urban areas and low-cost or entirely subsidized terminal equipment (smartphones, tablets, etc.).

4.How can accessibility be facilitated through increases in locally produced and relevant content in different languages?

Encouraging content production in different languages is essential to preserve languages and cultures in the digital age. Furthermore, it facilitates the access to the digital world by those groups of population who master only their own language.

5. What can be done to institutionalize MIL effectively in national educational systems?

I suppose MIL stands for media and information literacy. Using e-books and, especially, computer-based exercises goes a long way, although it requires investment in computers for schoolchildren.

B. Questions related to the field of Freedom of Expression

6. What are the current and emerging challenges relevant to freedom of expression online?

One major challenge is the increasing number of countries that enforce censorship mechanisms on the Internet, by preventing access to certain foreign contents or applications, by punishing local people who post contents considered "unorthodox", etc.

A second, more subtle, challenge relates to the neutrality of Internet, which currently is a battle between Internet access providers (basically the telecom operators) and the large Internet content providers (Google, Facebook, Amazon, Microsoft, Apple, etc.). The former players want to be able to prioritize packets carrying certain (premium) content at the expense of packets carrying other content, while the latter players oppose this pretension. At the moment, the Internet is still neutral, in that no content is penalized or prioritized due to its nature, and neutrality should continue to be the rule. Losing

neutrality would not only be damaging for the large content providers, but also for the myriad of small content providers. It would render the digital world more undemocratic.

7.How can legislation in a diverse range of fields which impact on the Internet respect freedom of expression in line with international standards?

Clearly legislation should forbid any form of censorship by governments and also ensure the neutrality of Internet.

8. Is there a need for specific protections for freedom of expression for the Internet?

In most countries, legislation on freedom of expression is general, not specifically restricted to the Internet and this is perfectly fine. However, there is a need for legislation on more technical issues that have also an indirect impact on freedom of expression, like protecting the neutrality of Internet, fighting cartel practices by access or content providers, etc.

9. To what extent do laws protect digitally interfaced journalism and journalistic sources?

I am not a legal expert, but it seems to me that laws protecting freedom of press are general enough to be applicable regardless of whether journalism is paper-based or digitally-interfaced.

10. What are the optimum ways to deal with online hate speech? How can Media and Information Literacy empower users to understand and exercise freedom of expression on the Internet?

Hate speech is one of the limits of freedom of expression, so insulting comments or texts promoting hate, violence or terrorism ought to undergo some form of censorship. For example, many moderated on-line fora do not publish comments by users if they consider them inappropriate. Of course, the boundaries between “legitimate” and “undemocratic” censorship may be fuzzy on occasion. Ideally, the decision as to whether contents are appropriate or inappropriate should not be left to a single person; an ethics committee would be more suitable, although it may not be affordable in terms of speed or even financially.

I am not sure Media and Information Literacy is relevant let alone sufficient to reduce hate speech.

11. What are the optimum systems for independent self-regulation by journalistic actors and intermediaries in cyberspace?

One possible mechanism would be independent reputation systems fed by the readers, e.g. analogous to what TripAdvisor is for hotels. At present, most on-line newspapers have put in place reputation/score systems internal to the newspaper, in order to identify

the best columnists, etc. But global reputation systems are not very developed.

C. Questions related to the field of Privacy

12. What principles should ensure respect for the right to privacy?

I am not sure I get this question right. The right to privacy is listed in the Universal Declaration of Human Rights (1948), in Article 12.

13. What is the relationship between privacy, anonymity and encryption?

If privacy is understood as seclusion (Warren and Brandeis, 1890), it is hardly compatible with the information society. A more realistic notion of privacy in our time is **informational self-determination**. This right was mentioned for the first time in a German constitutional ruling dated 15 Dec. 1983 as "the capacity of the individual to determine in principle the disclosure and use of his/her personal data" and it also underlies the classical privacy definition by Westin (1967).

If privacy is defined as informational self-determination, then anonymity is a form of privacy that consists of interacting with the information society without revealing one's identity.

Encryption is a technology that allows implementing a number of privacy choices: anonymity, hiding confidential information from the public view, etc. Beyond privacy, encryption allows implementing security (authentication, access control), data integrity, etc. More importantly, it can be used to reconcile privacy, security and performance. In general, **it is not true that a trade-off between privacy, security and performance is unavoidable: thanks to encryption and other technologies on can simultaneously and fully achieve those three properties.**

14. What is the importance of transparency around limitations of privacy?

First, it is important to spread the idea that privacy cannot be understood any longer as complete seclusion. Seclusion is incompatible with participating in the information society.

Second, even if privacy is more flexibly understood as informational self-determination, it cannot be attained by either technology or law alone. Combining a suitable legal framework, clear privacy standards and privacy technologies is the best way to go. Specifically, such a combination will facilitate the deployment of privacy-by-design engineering in information technologies.

15. What kinds of arrangements can help to safeguard the exercise of privacy in relation to other rights?

Privacy **must be compatible with *security*, for one thing: it should not be possible to abuse anonymity to attain impunity in case of misdemeanor. Also, privacy-aware**

services and applications ought to offer ***functionality*** comparable to privacy-unaware alternatives (otherwise the former will not be adopted): for example, if a search engine that avoids user profiling is much slower or less comprehensive than Google, the privacy-aware engine is unlikely to be adopted.

There are several technologies that allow conciliating privacy, security and functionality: encryption, anonymization, etc.

16. How can openness and transparency of data be reconciled with privacy?

In the information society, public administrations and enterprises are increasingly collecting, exchanging and releasing large amounts of sensitive and heterogeneous information on individual subjects. The fraction of these data that is made available to the general public is known as open data, and it is meant to improve transparency, planning, business opportunities and general well-being. Other data sets are released only to scientists for research purposes, or exchanged among companies

Privacy legislation (Europe's current and forthcoming General Data Protection Directive, the U.S. HIPAA, other national laws) forbids releasing and/or exchanging data that are linkable to individual subjects (re-identification disclosure) or allow inferences on individual subjects (attribute disclosure). Hence, in order to forestall any disclosure on individual subjects, data that are intended for release and/or exchange should first undergo a process of data anonymization, sanitization, or statistical disclosure control (see Hundepool, Domingo-Ferrer et al. (2012) *Statistical Disclosure Control*, Wiley, for a comprehensive book on anonymization). In fact, anonymization is not only a legal obligation, but also a matter of pragmatism: if data collectors do not guarantee disclosure control, respondents are unlikely to provide any answer, let alone a truthful answer. When performing anonymization, there is always a trade-off between disclosure risk (which must be kept acceptably low through data modification) and data utility (which requires that analyses on the anonymized data do not yield results that are too different from those on original data).

17. What may be the impact of issues relating to big data on respect for privacy?

Indeed, big data are based on the ability to link data coming from several sources, and this is a clear threat to privacy (via profiling) *when data are related to persons*. There are no privacy issues in other types of big data, e.g. those related to meteorology or finance.

As mentioned above, personal data must be anonymized before release. Then the question is how to anonymize data to prevent re-identification while still allowing some amount of linkage of data coming from several sources. This is currently a hot area of research in data anonymization.

18. How can security of personal data be enhanced?

A first principle to be observed by individuals is data minimization: they should avoid giving data on themselves unless strictly needed.

Second, organizations managing personal data should avoid releasing and/or exchanging those data without proper anonymization.

Third, whenever storing personal data in clouds managed by untrusted service providers, these data should be stored in a privacy-preserving format (e.g. anonymized, encrypted, redacted). In this line, I am co-ordinating the European H2020 project "CLARUS", to be started on Jan. 1, 2015 for a period of three years; CLARUS seeks to enable using untrusted software-as-a-service clouds for storage and (limited) processing of sensitive data.

19. How can Media and Information Literacy be developed to assist individuals to protect their privacy?

Media and Information Literacy is extremely important for privacy preservation. Everyone should be aware that, whenever some personal information is published, it will probably stay public forever. It should be clear to everyone that Internet is a global village where we do not know who is observing us. Also, people should be aware that to take care of their privacy is fundamental to preserve their freedom.

Awareness is key for consumers to opt for privacy-preserving information technology solutions. This will in turn act as a driving force for privacy technology and even privacy legislation development.

D. Questions related to the field of Ethics

20.How can ethical principles based on international human rights advance accessibility, openness, and multi-stakeholder participation on the Internet?

The Universal Declaration of Human Rights contains several articles that can be construed as supporting accessibility, openness, and multi-stakeholder participation on the Internet:

- Article 19. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
- Article 26 (1). Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.
- Article 27(1). Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.

In our days, the freedom of receiving and imparting information or ideas (Article 19) is hard to understand without an accessible and open Internet. The accessibility of education

set forth in Article 26(1) can be best implemented by making all educational materials on the Internet (Wikipedia, MOOCs, etc.) freely accessible to everyone in the world. Participation in the cultural life and sharing the scientific advancement and its benefits (Article 27(1)) is hardly possible today without an accessible, open and multi-stakeholder-ruled Internet.

21.What conceptual frameworks or processes of inquiry could serve to analyse, assess, and thereby inform the choices that confront stakeholders in the new social uses and applications of information and knowledge?

A first process of inquiry would be to analyze the terms of use that users must accept to access the various Web services offered to them (social networks, e-mail, etc.). Other inputs to this analysis should be the views of the users (represented by Civil Liberties associations and similar NGOs), the views of Internet companies (which also have their legitimate interests, especially when they offer free access services) and the views of governments (represented by privacy commissioners).

A task force of ethics experts appointed by some international organization (e.g. UNESCO) would be in the best position to conduct the above analysis.

22. How does ethical consideration relate to gender dimensions of the Internet?

In my opinion, the Internet is a new medium for communication, so in itself it does not raise new ethical issues related to gender. If there are gender differences in Media and Information Literacy in certain countries, this has to do with gender differences in education. Also, there may be gender differences in the access to new professions related to the technical aspects of Internet; but such differences can be explained by women being less prone to take engineering education (this is a statistical truth in most Western countries).

A different issue is gender discrimination related to the contents distributed over the Internet. Indeed, easier access to certain content (such as pornography) may encourage sexist discrimination. Also, the fact that an increasing number of decisions are based on automated analysis of large amounts of data may also result in discrimination if the underlying training data are gender-biased. To counter this latter danger, a new discipline called discrimination-aware data mining has been developed. We at the UNESCO Chair in Data Privacy have been particularly active in this area; see for example:

Sara Hajian, *Simultaneous Discrimination Prevention and Privacy Protection in Data Publishing and Mining*. Ph.D. Thesis, Universitat Rovira i Virgili, Doctoral Programme in Computer Engineering and Mathematics of Security. Date submitted: April 12, 2013.

Sara Hajian, Josep Domingo-Ferrer, Anna Monreale, Dino Pedreschi and Fosca Giannotti, "Discrimination- and privacy-aware patterns", Data Mining and Knowledge Discovery (to appear, 2014).

23. How can ethics, - i.e. the simultaneous affirmation of human rights, peace, equity, and justice - inform law and regulation about the Internet?

The ethical analysis proposed in my answer to Question 21 above should serve as input to promote new law and regulation about the Internet.

In fact, the elaboration of the new General Data Protection Regulation (GDPR) of the European Union has followed this process, albeit in an imperfect form (lobbies have been pushing for changes in the drafts behind closed doors, whereas an explicit inquiry including them would have been more transparent).

E. Broader issues

24. What international, regional and national frameworks, normative guidelines and accountability mechanisms exist of relevance to one or more fields of the study?

Privacy is considered as a fundamental human right. This is acknowledged by Article 8 of the European Convention on Human Rights, which provides a right to respect for one's "private and family life, his home and his correspondence". Similarly, the Charter of Fundamental Rights of the European Union defines the "respect for private and family life" (Article 7) and adds a specific article on "protection of personal data" (Article 8). Moreover, on an even wider scope, Article 12 of the Universal Declaration of Human Rights protects an individual from "interference with his privacy, family, home or correspondence, [and] attacks upon his honour and reputation." Thus, as a fundamental human right, privacy protection is not only regarded as a value that is important for an individual, but also as an essential element in the functioning of democratic societies.

Regarding European legislation, I copy below the legal section of the following report: G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Métayer, R. Tirtea and S. Schiffner, *Engineering Privacy by Design*, ENISA-European Network and Information Security Agency, Draft for peer review, Oct. 2014.

> "The main principles from the European legal data protection context are summarised and briefly discussed. Thereby, references to the European Data Protection Directive 95/46/EC (in short: DPD), to Opinions of the Article 29 Data Protection Working Party (based on Art. 29 DPD) and to the proposed European General Data Protection Regulation (in short: GDPR) are given.
>
> **Lawfulness.**
> Lawfulness in European data protection law boils down to two cases; processing of personal data is lawful only if a statutory provision permits it or if the individual whose personal data are being processed (in the European legal framework called "data subject") has consented. "Personal data" means any information relating to an identified or identifiable natural person. This is related to the term personally identifiable information (PII), as e.g. used in the privacy framework standardised by ISO/IEC.
> This very basic principle of lawfulness is not internationally harmonised, i.e., while in several countries outside Europe processing of personal data is permitted unless it is explicitly forbidden, in the EU processing is usually forbidden unless an explicit permission by the individual's consent or by law is necessary.

Note that for legally compliant data processing regulatory norms other than such concerning privacy need to be considered. Some of them contain requirements colliding with well-known privacy and data protection principles, e.g. legally demanded data retention overruling data minimisation considerations.

References to European data protection law

- Art. 7 DPD which contains more lawful grounds, e.g. if the processing is necessary in order to protect the vital interests of the data subject,
- Art. 29 Data Protection Working Party: “Opinion on the concept of personal data”,
- Art. 29 Data Protection Working Party: “Opinion on the notion of legitimate interests of the data controller”,
- Art. 5(1) point(a) GDPR principles “lawfulness, fairness and transparency”, and
- Art. 6 GDPR “lawfulness of processing”.

Consent

The term consent is further specified in the legal framework. To enable lawful data processing of individuals’ personal identifiable information, individuals need to give specific, informed and explicit indication of their intentions with respect to the processing of their data. The consent is invalid if not all these requirements are met. Hence, transparency is a prerequisite for consent. Furthermore, consent can be withdrawn with effect for the future. Consent is related to the right to informational self-determination and by this an expression of the individuals’ freedoms in general. However, in practice many individuals are not sufficiently informed, or the consent is not freely given. In the opinion of the authors, this deplorable situation occurs due to two issues, namely the way consent is asked is too complex, and the individuals’ focus is on another topic, at the moment consent is asked. This observation has been made not only in the field of privacy and data protection with “take it or leave it” apps or contracts in legalese, but also when signing consent forms for medical measures or bank statements. This has discredited the concept of consent.

References to European data protection law

- Art. 2 point (h) DPD,
- Art. 29 Data Protection Working Party “Opinion on the definition of consent”,
- Art. 4(8) GDPR definition of the “data subject’s consent”, and
- Art. 7 GDPR “conditions for consent”.

Purpose binding

Personal data obtained for one purpose must not be processed for other purposes. The purpose has to be legitimate, and it has to be specified and made explicit before collecting personal data.
In many countries outside Europe, the principle of purpose limitation or purpose binding is unknown. Instead, it is encouraged to use data for multiple purposes. Big Data is one of the big trends that incorporates multi-purpose linkage and analysis of data instead of leaving them in separated domains.

References to European data protection law.

- Art. 6(1) points (b)-(e) DPD,
- Art. 29 Data Protection Working Party: “Opinion on purpose limitation”,
- Art. 29 Data Protection Working Party: “Opinion on personal data”,
- Art. 5(1) point (b) GDPR principle “purpose limitation”, also
- Art. 5(1) points (c)-(e) GDPR, and
- Art. 21(2a) GDPR.

Necessity and data minimisation

Only personal data necessary for the respective purpose may be processed, i.e. in the collection stage and in the following processing stage, personal data has to be fully

avoided or minimised as far as possible. Consequently, personal data must be erased or effectively anonymised as soon as it is not anymore needed for the given purpose. Although data minimisation at the earliest stage of processing is a core concept of privacy-enhancing technologies, and it has been mentioned explicitly in the Global Privacy Standard of 2006, it has not been well enforced, yet.

References to European data protection law

- Art. 7 DPD,
- Art. 29 Data Protection Working Party: “Opinion on anonymisation techniques”,
- Art. 29 Data Protection Working Party: “Opinion on the application of necessity and proportionality concepts and data protection within the law enforcement sector”,
- Art. 5(1) point (c) GDPR principle “data minimisation”,
- Art. 5(1) point (e) GDPR principle “storage minimisation”, and
- Art. 23 GDPR “data protection by design and by default”.

Transparency and openness

Transparency and openness mean that the relevant stakeholders get sufficient information about the collection and use of their personal data. Furthermore, it needs to be ensured that they understand possible risks induced by the processing and actions they can take to control the processing.

Transparency is a necessary requirement for fair data processing. Since (1) individuals need information to exercise their rights, (2) data controllers need to evaluate their processors, and (3) Data Protection Authorities need to monitor according to their responsibilities. Currently, the transparency level is entirely inadequate whereas the complexity of data processing and system interaction is further increasing. However, full transparency might not be possible (nor desirable) due to law enforcement requirements and business secrets.

References to European data protection law

- Art. 10 DPD, Art. 11 DPD and Art. 14 DPD (obligations to inform the data subject),
- Art. 12 (a) (“right of access”),
- Art. 29 Data Protection Working Party: “Opinion on more harmonised information provisions”,
- Art. 5(1) point (a) GDPR (principles “lawfulness, fairness and transparency”),
- Art. 10a GDPR (“general principles for data subject rights”),
- Art. 11 GDPR (“concise, transparent, clear and easily accessible policies”),
- Art. 13a GDPR (“standardised information policies”),
- Art. 14 GDPR (“information to the data subject”),
- Art. 15 (“right to access and to obtain data for the data subject”), and
- Art. 12 (for defining the conditions for exercising data subject rights).

Rights of the individual

Individuals have right to access and rectify as well as (constrained) to block and erase their personal data. Further they have the right to withdraw given consent with effect for the future. These rights should be supported in a way that individuals can effectively and conveniently exercise their rights.

The implementation, or at least support, of these rights is promoted by the privacy by design principle that demands considering the user and the one that stipulates privacy by default.

References to European data protection law

- Art. 12 point (b) and (c) DPD (“right of access”, in point (b) in particular: the rectification, erasure or blocking of data if appropriate),
- Art. 14 DPD (“right to object”),
- Art. 5 No. 1 (ea) GDPR (principle “effectiveness”),

- Art. 7(3) GDPR (right to withdraw consent at any time),
- Art. 10a GDPR (“general principles for data subject rights”),
- Art. 13 GDPR (“notification requirement in the event of rectification and erasure”),
- Art. 17 GDPR (“right to erasure”),
- Art. 19 GDPR (“right to object”), and
- Art. 12 (for defining the conditions for exercising data subject rights).

Information security

Information security addresses the protection goals confidentiality, integrity, availability. All of these goals can be important also from a privacy and data protection perspective that specifically requires that unauthorised access and processing, manipulation, loss, destruction and damage are prevented. Further, the data have to be accurate. Moreover, the organisational and technical processes for appropriately handling the data and providing the possibility for individuals to exercise their rights have to be available whenever necessary. This principle calls for appropriate technical and organisational safeguards.

References to European data protection law.

- Art. 16 DPD “Confidentiality of processing”,
- Art. 17 DPD “Security of processing”,
- Art. 5 No. 1 (d) GDPR (principle “accuracy”),
- Art. 5 No. 1 (ea) GDPR (principle “integrity”),
- Art. 30 GDPR “Security of processing”, and
- Art. 50 GDPR (“Professional secrecy”).

Accountability

Accountability means to ensure and to be able to demonstrate the compliance with privacy and data protection principles (or legal requirements). This requires clear responsibilities, internal and external auditing and controlling of all data processing. In some organisations, Data Protection Officers are installed to perform internal audits and handle complaints. A means for demonstrating compliance can be a data protection impact assessment.
On a national level, accountability is supported by independent Data Protection Authorities for monitoring and checking as supervisory bodies.

References to European data protection law.

- In the DPD, accountability is not directly stated, but aspects of the principle can be seen, among others, in Art. 17 DPD (Security of processing) or by mentioning the possibility of appointing a “personal data protection official” in Art. 18 DPD who should be responsible for ensuring the application of data protection law.
- Art. 29 Data Protection Working Party: “The Future of Privacy”,
- Art. 29 Data Protection Working Party: “Opinion on the principle of accountability”,
- Art. 5(1) point (f) GDPR and Art. 22 GDPR (“Responsibility and accountability of the controller”),
- Art. 33 GDPR (“Data protection impact assessment”), and
- Art. 35 GDPR (“Designation of the data protection officer”).

Data protection by design and by default

The principle “Privacy/data protection by design” is based on the insight that building in privacy features from the beginning of the design process is preferable over the attempt to adapt a product or service at a later stage. The involvement in the design process supports the consideration of the full lifecycle of the data and its usage.
The principle “Privacy/data protection by default” means that in the default setting the user is already protected against privacy risks. This affects the choice of the designer which parts are wired-in and which are configurable. In many cases, a privacy-respecting default

would not allow an extended functionality of the product, unless the user explicitly chooses it.

References to European data protection law

• In the DPD, data protection by design is rather indirectly addressed, e.g. in Art. 17 DPD (Security of processing) where appropriate safeguards are demanded, even if this provision was mainly directed to security instead of privacy guarantees.
• Art. 29 Data Protection Working Party: "The Future of Privacy", and
• Art. 23 GDPR ("Data protection by design and by default")."

25. How do cross-jurisdictional issues operate with regard to freedom of expression and privacy?

I am not a legal expert, but normally the terms of use of Internet services establish the national jurisdiction under which any disputes should be resolved. By default, the jurisdiction to be used is the one of the country hosting the servers containing the data.

One problem here is that nearly all large Internet companies have their headquarters in the United States, where most of their data centers also reside. This gives the United States a disproportionate legal control on the Internet which, coupled with U.S. regulations like the Patriot Act and other laws arising from 9-11, certainly weakens the privacy of all Internet users worldwide. After the NSA scandals and also for performance reasons, there is a trend to open new data centers in other countries, mostly in Western Europe and the Far East. This will give more weight to the regional and national jurisdictions of these areas.

26. What are the intersections between the fields of study: for example, between access and freedom of expression; ethics and privacy; privacy and freedom of expression; and between all four elements? Responses may wish to distinguish between normative and empirical dimensions to these questions.

As I mentioned in my answer to Question 20, without access, freedom of expression as set forth in Art. 19 of the Universal Declarations of Human Rights remains a theoretical right.

Privacy having been classified as a basic human right (Art. 12 of the Universal Declaration of Human Rights), ethics should take care that privacy is respected in any new paradigm, such as the Internet.

Privacy is key to freedom of expression. If you do not know who is listening to what you say, self-censorship will naturally ensue.

27. What pertinent information materials exist that cut across or are relevant to the four fields of the study?

Among other materials, the legal references given in my answer to Question 24, as well as the ENISA report mentioned therein.

F. Questions related to options

28.What might be the options for the role of UNESCO within the wider UN system in regard to the distinct issues of online access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society?

To the extent that UNESCO is in charge of education, science and culture, it seems to be the UN agency whose mandate is most suited to deal with the regulation of fundamental rights in the information society and the Internet.

In fact, I contend that **UNESCO would be the ideal organization for taking care of Internet governance at the global level**. See my answer to Question 29 below.

29.What might be options for the role of UNESCO in relation to stakeholders outside the UN system such as individual governments, Internet companies, civil society and individual users, in regard to the distinct issues of online Access to information and knowledge, Freedom of Expression, Privacy and Ethical dimensions of the information society.

There is often a debate as to whether the big Internet companies behave ethically or not. In my view, this is the wrong debate. The real discussion should be on whether it is normal and desirable that companies managing information on a lot of people worldwide be under the jurisdiction of a single country, the U.S.

In fact, some voices from the same Internet companies have requested a global framework for data privacy. In 2007, Peter Fleischer, Google's Privacy Counsel, gave a speech in this sense at UNESCO ("The Need for Global Privacy Standards", Sep. 14, 2007), which he reproduced later in his blog ("We need global privacy standards… now more than ever", July 15, 2013, http://peterfleischer.blogspot.com). What Fleischer demands is certainly not an international control on Internet companies, but a global privacy standard that makes their job easier: they want to know which is the minimum privacy that they must guarantee to any citizen in the world to avoid trouble. The same idea of a global standard would also apply to freedom of speech, access, ethics and other moral values associated to the information society. Fleischer mentions UNESCO, the International Conference of Privacy and Data Protection Commissioners, OCDE, the Council of Europe, the International Chamber of Commerce or the World Economic Forum as possible organizations that could lead the elaboration of such global standards.

Global standardization has indeed advantages and the UNESCO Chair in Data Privacy that I lead would be delighted to collaborate in this task. Unfortunately, this would not fix everything for at least two reasons:

- Internet companies usually try to relax any international regulation on privacy. In this sense, just notice the current lobbying by these companies aimed at watering down the new General Data Protection Regulation under preparation by the European Union. Such lobbying has prompted the reaction of 100+ European

academics (including myself), who have published the manifesto ""Data Protection in Europe" (http://www.dataprotectioneu.eu), in which we require the European institutions to hold their ground.

- The prescription of a global standard must be accompanied by a supervision of its enforcement. Not much progress would have been made if, in reality, Internet companies continued to be answerable to U.S. law alone and found themselves forced by the Patriot Act or suchlike to disregard the international standard and, worse yet, to do it covertly.

Who could conduct this global supervision and how? **Among the institutions mentioned above, a UN agency like UNESCO would appear as the most legitimate option, because the UN represent all countries in the world**. As to the governance of such a supervision, it would seem natural for each country to have a weighed vote on the legal control of each Internet company reflecting at each moment the fraction of company users that are citizens from that country. Obviously, mechanisms would be needed to prevent countries or coalitions of countries not respecting human rights from acquiring a dominant or a blocking position in the supervision of Internet companies (otherwise, the proposed N/UNESCO governance might end up being worse than the current U.S. *de facto* governance).

30.For each study field, what specific options might UNESCO Member States consider, including for the Organization's Global Priorities of Africa and Gender Equality, shaping the post-2015 development agenda, supporting the goals of Small Island Developing States and taking forward the Decade for the Rapprochement of Cultures?

I think that setting up a governance scheme such as the one sketched in my answer to the previous question 29 would go a long way towards making the information society more democratic, fairer and closer to the needs of the less favoured social, ethnic and gender groups.