Let me start asking you a question: "Would you accept that your personal communications were broadcasted instead of being routed to your recipient?". If your answer is no, as I imagine, you can easily understand the importance of confidentiality of communications: it has to do with the most intimate sphere of our lives, but it has also a social value, as precondition for trust between users and providers, which is necessary for the development of services and technologies. This is why we need special rules, beyond GDPR: we need to protect confidentiality in order to build trust in electronic communications.

Why a Regulation? Technology is the key for the answer. Transmitting, storing and processing data are becoming "commodities", and this trend is bringing the processing of data far from Europe and far from persons, towards a limited number of very efficient global players, with the effect that people use a number of voice, video, and messaging applications in a seamless way, and they expect the same level of confidentiality whether they use these services or traditional ones. A Regulation embracing telco operators and OTTs seems to me the best available legal instrument to rebalance the effects of this "commoditization".

How does this Proposal aim at protecting confidentiality? With a general prohibition on the processing of data, unless specific derogations apply: 1) the necessity of the data to accomplish the electronic communication; 2) the consent expressed by the users involved and 3) the anonymization of data. In my view, this pattern is adequate to build trust and it should be harmonized as much as possible, and applied to all types of data and to all types of communication.

Let me deal briefly with the issue of anonymized data. Anonymization was an option already introduced in the Directive as an alternative to data deletion, at the end of data lifecycle. Remarkably, the Proposal poses anonymization at the beginning of data lifecycle, offering data a twofold life: one as "traditional" personal data, and another life as anonymized data, which will still offer controllers huge opportunities for many applications in the area of Big Data and Internet of Things. In future electronic communications, the implementation of anonymization will require, in my view, three big commitments from controllers: 1) transparency, on the scope and on the applied anonymization methodology; 2) a preliminary privacy impact assessment with mandatory consultation of the DPAs, and 3) easy opt-out for users from even the anonymization itself. In this manner, I think that anonymization can become a real privacy friendly opportunity for data controllers, allowing a more rigorous interpretation of consent for the processing of personal data.

As to consent, in the Proposal cases are envisaged where the consent of a single party involved in the communication is needed. I believe that this rule can be applied for the provision of services, beyond "transmission", specifically requested by the user, and if the processing does not affect the other parties involved in the communication. Consent by all the parties involved can be applied to the accomplishment of a purpose that is in the interest of data controllers. But in order to foster the implementation of mutual consent, new technical standards, especially in environments with many interconnected parties, need to be promoted.

Consent is not envisaged for wifi tracking, and the current Proposal allocates very weak transparency and security obligations to controllers, leaving it to the data subjects to minimize the data or opt out by switching off their wifi interfaces (and therefore preventing all kinds of communication on this interface). I would like to stress that the area of "emitted data" is the one where a stronger commitment by controllers is needed, because this is where asymmetry with data subjects is highest: "emitted data" can be collected at any time by controllers with very limited margins of intervention for the data subject. The current proposals are not sufficient to build trust. At the very minimum, the technology-intensive task of data minimization (I would say data anonymization) and the implementation of opt-out solutions should be allocated to controllers and device manufacturers.

Regarding the use of data stored in users' terminals, such as cookies used to track web navigation, publishers normally interact with a multitude of other parties for various purposes, making our navigations less than confidential. Users are not aware of these complex interactions and any take-it-or-leave-it solutions (like cookie walls) are not fair; besides, they do not meet the requirements of consent. Trust in the web environment would benefit a lot from introducing a transparency obligation on the existence of these interactions. Also, the promotion of clear technical standards for the classification of cookies per purpose (for instance, tracking cookies, web measurement cookies, and so on) would help in enforcing the rule and strengthen the accountability of controllers.

According to the Proposal, consent in internet can be expressed using functionalities made available in the browsers or similar software. The underlying idea here is to centralize consent in commonly used tools. There are still two main technological issues: first, in order for consent to be valid, it is not enough to offer options, but also the initial conditions are important, and browser default configurations should be set in the most privacy friendly mode; second, the preferences expressed by data subjects on the use of cookies and configuration data, such as device fingerprinting, should be binding on controllers.

Let me conclude with a few words on data integrity and availability, which are equally important components of security. If information is used to control the devices that we use every day (think of connected cars, for instance, or other machine-to-machine applications) a general obligation on information integrity and availability, together with the protection of confidentiality, might provide safeguards against threats such as identity theft or data manipulation, which could trigger even vital consequences for data subjects, promoting at the same time accountability and facilitating enforcement.

All these gaps have to be properly addressed if we don't want to create a divisive internet. Technologies are of primary importance here: the protection of confidentiality of electronic communications in future Big Data and in the Internet of Things will require new generation technologies. Old tools will not be sufficient.

I would like to thank the LIBE Committee for offering me the opportunity to express my views on the Proposal for the e-privacy Regulation. Now it is up to you. You have the responsibility to decide how the way we communicate will look like in the next decade, and maybe more. This is not a minor, or a different, "separate" dimension of our lives, since this infosphere where we live is becoming more and more the main dimension of our being "digital human beings": will we communicate "trustingly", opening up the path to prosperity, or will we communicate "conflictingly", paving the way to an erosion of wealth? This is the question. I wish you the wisdom that is needed for this delicate task.

Thank you very much