Generally, and up to a point, laws reflect the ethical principles of every society, and such beliefs and principles may also be strongly related to geographical, religious and other factors. During the last decades, legal systems have been globalized to a point, while at the cyber level geographic borders seem quite vague, and ICT Technologies have also played their part into affecting the ethical and moral values of a worldwide, overlay community, which I could call as “the citizens of the WWW community”, towards a more liberal and progressive orientation. In a matter of fact, even new ethical rules and principles specifically concerning the Internet Society have emerged, some of them being still investigated from legal, philosophical and technological points of view, under the name of Cyber Ethics.

On the other hand, conventional legal systems are more representative of the heterogeneities inherent in national societies. Their salient features are inherently conservative to a point, since they typically express a historical continuity of principles and mentalities that have been evolved for the last thousand years of human history and which even in our times, evolve in a relatively slow pace, compared to the exponential rates of cyber-ethical evolution. Of course, conventional societies are also affected by the Internet society, and I would say that such an ethical flow between the two societies should be investigated.

While at a first glance the Computers and the Internet strengthen freedom, foster communication and bring people together, this comes with a trade-off. As you also describe in your paper, new technologies create the capabilities for generating and maintaining a bulk of personal and sensitive information for citizens. This can either come as a by-product of using an augmented reality service, or as a pre-condition for enjoying it. Especially with the advent of data mining technologies, the risk of massive privacy violation is quite high. Specifically, Service Providers, possibly in cooperation with network providers may be capable of supporting monitoring users’ behavior, targeting users with personalized spam, or making intrusive inferences about their lifestyle, political or religious views, state of health and so forth.

To give a dramatic tone to that, one could say that in the hands of a total regime, such information could lead to a scenario whose most appropriate analogy to a physical world is the world envisaged by G. Orwell. In a matter of fact though, even

democratic regimes nowadays pass big-brother-like laws and anti-privacy has been rejuvenated, more or less, as a new moral value, from a sociological aspect.

Another ethical issue that worries me, and which is also interesting from both psychological and sociological points of view, is that people in electronic Social Networks increasingly consider as a virtue or just "cool", to disclose even to strange people a bulk of personal and sensitive information. In exchange, they are able to look at other people's lives through a keyhole offered to them for free. What are the economics of this state of affairs? Is there any possibility that people may just ignore the privacy and security risks? Is this acceptable?

From a technological point of view I believe that privacy by design, if drawn carefully, could also increase people's trust in mixed reality services, and thus increase acceptance and participation of privacy-aware people to such services. For example, suppose I do not use Facebook because I may have privacy concerns. Secondly, I would like to use a Buddy Finder social networking service which would alert me when any friend from a pre-selected list of friends would be in the same area where I am, but I would not subscribe for privacy reasons. Now, this same service would be cool for me as a privacy aware person if: a) my friends would only learn 1 bit of information, whether I am in their vicinity or not (and not my exact location) and b) the SP would also not have to know my exact position. Would that be possible? Technologically yes, for example using cryptographic mechanisms. My late research specifically concerns the use of cryptographic technologies to establish privacy-preserving Location-Based Services (LBS).

A particular goal in privacy-preserving architectures in general is not to avoid collection of information but to control it. Examples are destroying the link between user information and the identity of the user, or between user information and the exact context of the user (for example, cloaking the exact user's location in an LBS service). For example, there are some LBS services such as "*Show me some restaurants nearby*" or "*When I pass a gas station, alert me with gas price*", which could be executed anonymously or pseudonymously, or where the LBS Provider does not have to know the user's exact location (since the exact location could be my home, or in a hospital treating sexual diseases). Or, it could be just fine to send as part

of my query a location where k other users are around the same place at the same time, in order to establish what is known as k-anonymity protection. Current research in information security focuses towards efficient and usable solutions that allow customers to customize & enforce different levels of privacy, depending on their context. I agree though that privacy-preserving technology needs to be designed and implemented in a way that is effective, efficient and usable, that does hinder the very goals of a mixed reality service. These goals may be inherently contradicting each other.

To summarize, I can see the following issues for discussion, but also for future research and, why not, synergies among our institutions.

a) A series of the Sociological, Ethical and Psychological issues.
b) The Technological issue: Namely assessing the threats, the threat factors, likelihood and consequences of threat realization, and the overall risk for each threat. Also, to propose ways to mitigate them in an affordable way.
c) The Policy related issue: Namely, which are the strategies, policies and regulatory frameworks that should be designed and enforced in order to mitigate those risks. As I see it, the main challenges here are a) the pace of technological advances which create 0-day threats and privacy risks, b) the lack of security/privacy awareness and education in our society.

I believe that a minimum privacy-by design level for everyone, also supported by a regulatory reform and combined with strategies to increase the information security awareness would be a noble cause.

Personally, I think that at the end we will have to look at the mirror and ask our selves: what kind of society we and our children will spend our lives in. Thank you.