The ethical challenges of digital identity

November 7 2019, by Armen Khatchatourov

Credit: CC0 Public Domain

The GDPR recently came into effect, confirming Europe's role as an example in personal data protection. However, we must not let it dissuade us from examining issues of identity, which have been redefined in this digital era. This means thinking critically about major ethical and philosophical issues that go beyond the simple question of the protection of personal information and privacy.

Current data protection policy places an emphasis on the rights of the individual. But it does not assess the way in which our free will is increasingly restricted in ever more technologically complex environments, and even less the effects of the digital metamorphosis on the process of subjectification, or the individual's self-becoming. In these texts, more often than not, we consider the subject as already constituted, capable of exercising their rights, with their own free will and principles. And yet, the characteristic of digital technology, as proposed here, is that it contributes to creating a new form of subjectivity: constantly redistributing the parameters of constraints and incitation, creating the conditions for increased individual malleability. We outline this process in the work *Les identités numériques en tension* (Digital Identities in Tension), written under the Values and Policies of Personal Information Chair at IMT.

The resources established by the GDPR are clearly necessary in supporting individual initiative and autonomy in managing our digital lives. Nonetheless, the very notions of the user's consent and control over their data on which the current movement is based are problematic. This is because there are two ways of thinking, which are distinct, yet consistent with one another.

New visibility for individuals

Internet users seem to be becoming more aware of the traces they leave, willingly or not, during their online activity (connection metadata, for example). This may serve as support for the consent-based approach. However, this dynamic has its limits.

Firstly, the growing volume of information collected makes the notion of systematic user consent and control unrealistic, if only due to the cognitive overload it would induce. Also, changes in the nature of technical collection methods, as demonstrated by the advent of

connected objects, has led to the increase of sensors collecting data even without the user realizing. The example of video surveillance combined with facial recognition is no longer a mere hypothesis, along with the knowledge operators acquire from these data. This is a sort of layer of digital identity whose content and various possible uses are entirely unknown to the person it is sourced from.

What is more, there is a strong tendency for actors, both from the government and the private sector, to want to create a full, exhaustive description of the individual, to the point of reducing them to a long list of attributes. Under this new power regime, what is visible is reduced to what can be recorded as data, the provision of human beings as though they were simple objects.

The ambiguity of control

The second approach at play in our ultra-modern societies concerns the application of this paradigm based on protection and consent within the mechanisms of a neo-liberal society. Contemporary society combines two aspects of privacy: considering the individual as permanently visible, and as individually responsible for what can be seen about them. This set of social standards is reinforced each time the user gives (or opposes) consent to the use of their personal information. At each iteration, the user reinforces their vision of themselves as the author and person responsible for the circulation of their data. They also assume control over their data, even though this is no more than an illusion. They especially assume responsibility for calculating the benefits that sharing data can bring. In this sense, the increasing and strict application of the paradigm of consent may be correlated with the perception of the individual becoming more than just the object of almost total visibility. They also become a rational economic agent, capable of analysing their own actions in terms of costs and benefits.

This fundamental difficulty means that the future challenges for digital identities imply more than just providing for more explicit control or more enlightened consent. Complementary approaches are needed, likely related to users' practices (not simply their "uses"), on the condition that such practices bring about resistance strategies for circumventing the need for absolute visibility and definition of the individual as a rational economic agent.

Such digital practices should encourage us to look beyond our understanding of social exchange, whether digital or otherwise, under the regime of calculating potential benefits or external factors. In this way, the challenges of digital identities far outweigh the challenges of protecting individuals or those of "business models", instead affecting the very way in which society as a whole understands social exchange. With this outlook, we must confront the inherent ambivalence and tension of digital technologies by looking at the new forms of subjectification involved in these operations. A more responsible form of data governance may arise from such an analytical exercise.

Provided by The Conversation