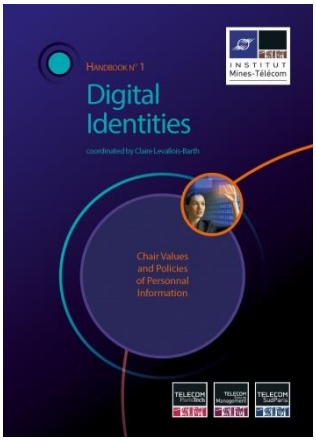


# Conclusion

*Armen Khatchatourov, Claire Levallois-Barth, Pierre-Antoine Chardel*

➢ **To cite this document, thank you for using the mention below:**

> Khatchatourov, A., Levallois-Barth, C., & Chardel, P-A. (2016). Conclusion. In *Digital Identities*. *Chair Values and Policies of Personal Information.* Paris (France)

Today we are seeing considerable growth in the use of digital identities in various forms, ranging from 'declarative' identities on online social networks to 'hard' identity initiatives, particularly at European level. While the majority of these initiatives are directed towards the public sector, they are also designed to be adopted by actors in the private sector, for uses as varied as online purchases and transport. This phenomenon reflects the fact that it seems at first sight 'more convenient' to use the same identity, with the same identification system, in different contexts.

As emphasised in this Handbook, however, the use of a unique identity in sectors of activity that are fundamentally different entails risks when it comes to ensuring respect for fundamental liberties, which the French legislator has striven to protect, for example with the adoption in 1978 of the Loi Informatique et Libertés. To reduce these risks, it is possible to make use of pseudonym-based identity management systems, or multiple identities. The pseudonymisation approach is however not always sufficiently elaborated: in this case, some

actors are able, *a posteriori*, to unify the identities of a single person without any consent on his part, and thus group together his personal information.

In view of the constant expansion in the use of digital identities, it is important to summarise the challenges that this raises, and to explore solutions that would enable the construction of systems that do not lead to global traceability of the citizen. This is in the interest of everyone, including the state (if it wishes to maintain its sovereignty) but also companies, as winning the trust of their customers is an important issue.

As far as law is concerned, existing (the Data Protection Directive 95/46/EC, transposed in France into the Loi Informatique et libertés), as well as recently adopted legislation (EU General Data Protection Regulation, adopted on April 27 2016 and coming into force on May 25, 2018) expresses a clear determination to ensure a 'high level' of personal data protection.

Hopefully this approach should correct certain weak points so as to put the user back into the heart of the technical and economic system. One of the current weaknesses is the difficulty for a person of manifesting his wishes. In practice, it is not always possible to express consent: in some cases, the user has no choice other than accepting the conditions proposed, and in others, the cognitive cost required of him is far too great.[1]

This situation may lead to an imbalance between the power of the user and that of the data owner. Will the new legal provisions resolve this imbalance? Some would argue that the legislative approaches currently used are still inadequate.[2] It is worth noting however that the upcoming regulation reinforces the definition of consent[3] and specifies the conditions of consent in more detail[4]. In particular, the controller must be able to demonstrate that the data subject did indeed give his consent, in accordance with the principle of accountability.

With regard to implementation, there are also difficulties in the application of the principle of transparency. While the advent of the digital world in which we live leads to an unprecedented amplification in the use and subsequent transfer of personal data using increasingly complex means, it is difficult for the user to be aware of or understand this phenomenon, and even more difficult for him to exercise a degree of control on the circulation of his data. It is vitally important that the controller fulfils its obligation of giving notice, as this is a prerequisite if individuals are to be able to assert their rights.

If individuals are not even aware of the existence of processing, how can they be actively involved in their own protection? How can they exercise their right of 'data portability' or their right 'to be forgotten', for example in relation to their identity provider? Even if they could, how is it possible for them to ensure that the provider is trustworthy if no reliable indicators

---

[1] See, for example, Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation*. Annenberg School of Communication.

[2] On this point, see: Koops, B.-J. (2014). *The trouble with European data protection law*, *International Data Privacy Law*, 4(4), pp. 250-261. — Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics, *Computer Law & Security Review*, 30(6), pp. 643–660. — Blume, P. (2014). The myths pertaining to the proposed General Data Protection Regulation, *International Data Privacy Law*, 4(4), pp. 269–273. For a critical discussion of "notice and consent", see Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press.

[3] Art. 4 (11) of the GDP Regulation of 27 April 2016 states that *" any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

[4] Art. 7 of the GDP Regulation of 27 April 2016. Note also Recital 25 , and Recital 42 which states that *" Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."*

are available? In this respect, the reinforcement of the obligation of giving notice.[5] and the establishment of certification and label schemes seem a positive way forward, which could increase transparency and give labelled products and services a competitive advantage.

It is also important to encourage complementary approaches, enabling the modulated application of legal principles in a contextual, operational and comprehensible way both for companies and for the general public. This process of modulated application of legal principles, which is by no means easy, needs to be introduced through public policy (e.g. by the publication of guides setting out 'best practices'), economic actors (particularly through the fostering of best practices through business associations) and users.

The solutions to be applied also have technical aspects. The principal method is the use of multiple identities by means of 'unlinkable' pseudonyms. It must be kept in mind however that the use of pseudonyms provides only a partial answer to the problem of user traceability. Furthermore, such technical solutions have two hurdles to overcome.

First of all, as in the case of the regalian digital identity approach in Germany, technical solutions that protect individual liberties require significant investments by the public authorities, and in some cases by companies. Furthermore, technological changes constantly challenge the solutions' effectiveness. The classic example is that of the cross-linking of data with the aid of the Big Data techniques, a process which enables increasingly precise identification of the individual, even if he is using multiple digital identities. It is therefore important to establish adequate internal procedures to ensure regular checks on the effectiveness of the solutions implemented throughout the digital identity life cycle.

To encourage actors, and economic actors in particular, to adopt solutions that protect individual freedoms, it is important to stress that users are calling for pseudonym-based solutions. As it may reasonably be assumed that the consumer chooses a digital identity that is suitable for the context of the transaction, it seems probable that the choice will be guided by the possibility of remaining 'anonymous' and that the use of pseudonyms has a positive impact on adoption levels and thus on the volume of transactions. Up to now, it has proven difficult to draw conclusions, as it seems that this correlation depends on the sociotechnical context. Some research – such as that of Balgobin et al. (2015)[6] – suggests that there is a positive correlation between the level of personal data protection offered by systems and their adoption: guaranteeing anonymity during a transaction enables the acquisition of products that would not otherwise have been purchased. Other research – such as that of Khatchatourov et al. (2015)[7] – tends to suggest a lack of correlation in a context of 'hard' digital identities.

Finally, seen in a wider perspective, digital identities raise fundamental issues for society as a whole. If the possibility of users actively constructing multiple identities is not preserved, this will threaten citizens' autonomy and the conditions of possibility of their free will. This means that any tendency towards the unification of identities that could become established in a long-term perspective would threaten to reduce the possibility of heterogeneous voices, by calling into question the fragile balance between a degree of transparency and a

[5] See Art. 12 of the GDP Regulation of 27 April 2016

[6] Balgobin, Y., Bounie, D., Quinn, M., Waelbroeck, P. (2015). *Payment Instruments, Financial Privacy and Online Purchases*, working document.

[7] Khatchatourov, A., Laurent, M., Levallois-Barth, C. (2015). *Privacy in Digital Identity Systems: Models, Assessment, and User Adoption*, in *Electronic Government, Lecture Notes in Computer Science*, Springer.

possibility of dissimulation that is however necessary for each individual to fulfil himself in the public sphere.[8]

In other words, we understand that technological measures taken to encourage unique identity entail choices that are not only political, but also ethical. What vision of society do we intend to put forward through measures of this type? It will indeed be a major challenge to develop solutions that show respect for the way we construct our identities. This can only be done if there is a real determination on the part of governments and companies, whose choices will have a crucial influence on the way our society evolves, and on the possibility of stimulating (or on the contrary undermining) a sense of common purpose. To take care of the quality of living together will require not only appropriate legislative and technical initiatives, but also the mobilisation of civil society, particularly by means of 'data education' that is capable of raising the awareness of all citizens about issues of such great importance for the future of our democratic societies.

*This article has been translated from French by Peter Thomas*



[8] On this point, see: Pierre-Antoine Chardel, Brigitte Frelat-Kahn, Jan Spurk (eds.), *Espace public et reconstruction du politique,* Presses des Mines, 2015.

## ABOUT THE CHAIR VALUES AND POLICIES OF PERSONAL INFORMATION

Launched by the Institut Mines-Télécom in March 2013, the Chair has brought together a multi-disciplinary team of researchers working on the legal aspects of regulation and compliance, the technical aspects of data protection and data security, the economic aspects of sharing personal information, and the philosophical aspects of responsibility and anticipating societal consequences of digital transformation.

It is supported by six partners: the Groupe Imprimerie Nationale, BNP Paribas, Orange, LVMH (the four founding patrons), Dassault Systèmes and Deveryware (associate partners), in collaboration with the Commission nationale de l'informatique et des libertés (CNIL) and with the support of the Fondation Télécom.

The Chair is coordinated by Claire Levallois-Barth, Associate Professor of Law at Télécom ParisTech, and was co-founded with Maryline Laurent, Professor of Computer Science at Télécom SudParis, Patrick Waelbroeck, Professor of Economics at Télécom ParisTech and Pierre-Antoine Chardel, Professor of Philosophy at Télécom École de Management.

The Chair aims to help companies, citizens and the public authorities in addressing issues relating to the collection, use and sharing of personal information, that is information concerning individuals (their private lives, professional activities, digital identities and contributions to social networks, etc.), including information gathered by the communication devices around them. This information, supplied by the data subjects, and the traces of their activities and interactions, in fact raise many questions in terms of social value, economic value, control policy and regulation policy.

The Chair's research is directed towards five transdisciplinary areas: • digital identities; • personal information management; • contributions and traces; • personal information in the Internet of Things; • personal information policies.

In addition to the publication of research articles and participation in colloquia, the Chair regularly organises events that are open to everyone, to raise public awareness about these major issues affecting the digital world.

**FOUNDING SPONSORS**

GROUPE Imprimerie Nationale

BNP PARIBAS

orange

LVMH

**ASSOCIATE SPONSORS**

DASSAULT SYSTEMES

DEVERYWARE
TRUSTED LOCATION-BASED SOLUTIONS

**QUALIFIED PARTNERS**

CNIL