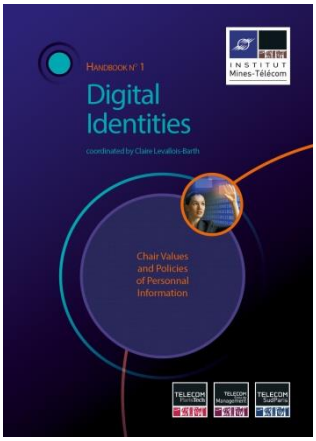

Introduction

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

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

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

From the user's viewpoint, digital identity is a means of accessing resources (to display a photo or consult your user account) and performing certain actions (to invite a friend or pay your taxes) in the digital environment by identifying oneself as a user who is registered and authorised to perform the action in question.

There are different kinds of digital identity depending on the use:
• '**hard' identity** for the holder of an electronic identity card, enabling him to access electronic administration services (taxes, civil status);
• local citizen identity to access services proposed by the neighbourhood or town, e.g. to sign children up for a daycare centre;
• '**private' identity**, e.g. for a social network account,
• **customer identity** for the user of an online sales or bank website;

- **the professional identity** assigned to a lawyer, police officer or doctor;
- **the identity of a legal person** in its relationships with companies, its customers or the state.

This spectrum is broadening day by day, and in the near future it is likely to cover every kind of everyday use. It enables us to have multiple ways of revealing ourselves to others and our ways of being, for example, by giving us the possibility of presenting ourselves under several identities, particularly on social networks.

In the process, the use of digital technologies raises questions about the way in which the individual relates to himself and to others, for we construct our subjectivity (which designates that which is personal and specific to a person) not only on the basis of stable criteria (family name, first name for example) but also of various possibilities opened up by digitisation. This is made possible by the architecture of digital networks. Because of the nature of this architecture, whose characteristics were defined when the Internet was created, it is not always possible to easily find out the identity of a person in the sense of that person's civil identity, when she sends a message or consults a website.

This lack of immediate identification can sometimes be perceived as a difficulty, for example when identification is necessary to make a bank transaction or to combat illicit content (such as child pornography or the online sale of drugs). At the same time, it constitutes a major step forward for freedom of information, action and expression in debates that are technically facilitated by the new public space that is the Web.

'Digital identity' can thus be seen from two viewpoints:
- firstly, the effects of digitisation on the construction of identity, seen as a relationship with oneself, with others and with the public sphere;
- secondly, the identification of the user and his actions.

These two complementary aspects together form the heart of the issue we are considering.

The first aspect, i.e. the influence of digital on the individual's construction of his multiple identities as a way of presenting himself to others, is a phenomenon that has already attracted interest amongst researchers in the humanities and social sciences[1].

In the epoch of the 'multitude'[2] in which the activity of billions of connected persons is captured, the effects of a reverse movement however tend to attract far less attention. This tendency is that of relating the multiple activities of a person, who presents himself under various identities depending on the context (e.g. the same individual presents himself as a 'footballer', 'father', 'music fan', 'job seeker', 'incurable disease sufferer'), to a 'unique' identifiable individual. In the course of this operation, the person is 'reduced' to his own civil identity, or to a profile composed of an almost complete set of his personal data. But this assimilation is not without consequences: it strengthens the transparency of the individual's various facets, increases risks of discrimination and reduces the richness of possible interactions.

---

[1] To limit the list to the French language literature and in non-exhaustive mlanner, one can think of works of researchers in sociology, such as Nicolas Auray, Dominique Cardon, Julie Denouël, Antonio Casilli, Fanny Georges and Fabien Granjon.

[2] See Guattari, F. (2006), Entretien avec Jacques Robin: Révolution informatique, écologie et recomposition subjective, *Multitudes,* no. 24, and Colin, N., Verdier, H. (2014), *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique,* Paris, Armand Colin.

In this Handbook we intend to raise questions about this tendency, referred to as 'unification of digital identities'. Is a unification of this kind desirable? In which cases? What are its drawbacks and its weaknesses? How could they perhaps be avoided? Using what kind of regulatory approaches?

METHOD

To throw light on the various issues raised by digital identities in contemporary societies, this Handbook is adopting an original multi-disciplinary approach. In our view, while this broad view necessarily involves information technology and law, it also raises many questions about economic mechanisms, and ethical, philosophical and societal implications of thete technologies.

In the following we develop an approach based both on fundamental theoretical issues and on the practices of actors (through interviews, participation in meetings with key actors, and comparative analyses).

The establishment of a unequivocal identification, which could take the form of a unique identifier leading to permanent identification, is today a central issue of a public debate and concerns certain states and economic actors.

Amongst the economic players, GAFA (Google, Apple, Facebook, Amazon) have introduced so-called 'private' digital identities. A user's Facebook identity, for example, is used on the social network itself, but also increasingly in other contexts. The Facebook Connect button thus means that this identity can be used in discussion forums or in an online purchase. It is worth noting that GAFA have repeatedly tried to introduce a 'real ID' policy which consists of compelling their users to provide a 'hard' credential for their civil identity. Is this tendency desirable? Should it be subject to conditions?

In the case of states, as shown by the Snowden affair, the cross-linking and grouping together of the various personal data of the same person increase the risk of surveillance across the whole population. It is worth noting that states do not necessarily have recourse to a unique identifier (in the form of an identification number, such as a social security number) but may still have technical ability to uniquely identity the user.

In view of this, we wish to ask questions in particular about the tendency towards the institutionalisation of the digital identities of individuals. By institutionalisation we mean the very processes of formation of the institutions that provide the framework for social relations, participate in the organisation of society or of the state, and ultimately impose values and behavioural norms (like in the institution of marriage). In the case of digital identities, this process of institutionalisation is connected to the introduction of special technical devices and the adoption of legal provisions whose implementation then in turn influences social relations as a whole.

In France, this process is rapidly progressing. 'Sectorial' identities are growing in number – the most striking example being the identity of the person insured for medical care via his

'Carte Vitale' – but it is worth noting that no 'hard' digital identity has been introduced and become recognised that is comparable with the civil identity certified by the state in the 'real' world. However other countries have introduced — or are working towards the introduction of — digital identities that can be established on various media (electronic national identity card, mobile phone, social security card, bank card, USB memory stick, etc.).

The current trends at state level raise the following questions:

- If digital identity covers the whole population, what are the effects of this scaling up, e.g. in terms of public policy?
- If the use of digital identity is made compulsory, how this would affect citizens' behaviour? What could be the possible coercive and disciplinary consequences on each citizen when a large proportion of his online actions become more easily traceable?
- More generally, to what extent should the user be held responsible?
- How can the use of "hard" identities be regulated in the private sector?

Furthermore, it seems that the public authorities is most cases see the use of 'hard' digital identity management systems by private concerns as a driving force encouraging the adoption of the systems they are offering. It is supposed indeed that users are more inclined to use these systems on a daily basis, and that the costs can be shared between the public and private sectors.

This Handbook thus examines the way in which certain states —France and the countries of the European Union — intend to set up identity management systems covering the whole of a society, and how the European Union is intervening in this area. It also contributes to the study of the potential consequences of this 'systemisation' on social and democratic balances. Over the last few years, it has been noticeable that states have been pursuing several objectives in this field:

- improving the security levels of the means of identification used by citizens;
- simplifying citizens' formalities;
- making the use of such means commonplace, so that they can be used in increasingly varied contexts, to expand the number of applications and enable economies of scale.

But this strong tendency towards increasingly widespread use carries with it risks that need to be highlighted, particularly if one of the consequences is to group together all the different 'identities' that a human being can have ('hard' identity, citizen identity, private identity, customer identity and professional identity) in a 'unique' identity. More specifically, while this heightened visibility may provide a strong degree of assurance in the context of electronic transactions, it may also be seen as exponentially increasing the possibilities of surveillance, both by the state and by the private sector. The creation of a 'unique' identity thus raises questions in terms of preserving public freedoms. The question of this preservation seems to be more acute today than in the earlier days of information technology, for example in 1978 when the Loi Informatique et libertés was adopted in France.

It is far from easy to strike the right balance between the various objectives. Technical and political decisions can have many implications that go far beyond merely managing data flows. One of these issues arises when an individual takes on the role of a whistle blower. We are referring here to the possibility of a person revealing to the public in good faith either a danger or a risk that could constitute a threat to people (e.g. informing the media about a serious problem inside a company that could have damaging consequences for the environment).

More generally, the question may be asked whether a certain form of opacity of the individual is not required to enable him to formulate an expression of opposition. How can this opacity be guaranteed so as to preserve freedom of expression, and more broadly the very workings of our democratic societies? How is it possible to ensure that the citizen does not find himself immediately enmeshed in technical networks of identification that are by their very nature indifferent and insensitive to the singularity of the contexts in which he expresses himself?

There is also a need to ensure that the citizen as a subject of law can continue to affect the way in which he wishes to present himself to other people, by preserving his autonomy as far as possible. What effects will the rationales of identification and cross-linking between contexts have on his autonomy? Questions may be asked about the consequences of systematically comparing the different actions of a person (e.g. comparing a record of the books a person consults in a library with his applications for benefits or allowances). Is it not advisable to strengthen the way such practices are regulated and encourage the granting of new rights?

HOW DOES A DIGITAL IDENTITY WORK?

To perform some actions in a digital environment, it is necessary for the user to obtain authorisation. The identity management system is used to manage the authorisations through means of authentication, such as the login/password pair or dedicated equipment (e.g. a smart card or fingerprint reader). Once authenticated, the user is defined by a set of attributes (name, age, employer) and rights (access to certain documents, modification of the files). Two aspects need to be stressed: firstly, any given natural person can have several digital identities, even in some cases inside the same management system; secondly, the set of attributes and rights can be defined by the user himself or by an authority that manages identity, and the set may be non-modifiable or evolving. Everything depends on the choices of architecture made in the design of the identity management system.

The role of the bodies that initially issue digital identity is crucial here, both in terms of identity life cycle management and of the level of credit that is given to the identity: the same value is not granted to a national identity card issued by a state and to a card attesting to membership of a particular profession. Choices of architecture are not therefore merely technical choices. They constitute strategic choices, which may be societal choices, that must be performed in a way that depends on the context of use of the digital identity.

With these questions in mind, the Handbook proposes an interdisciplinary approach in a set of Chapters that can be read, not necessarily in order, and independently of each other.

Chapter 1 shows how the question of identity is linked to that of a person's autonomy, and how autonomy determines the construction of the individual and his ability to act in society. The major issue is that of the very possibility of democracy, in the sense that preserving one's autonomous capacity for action is a prerequisite for living together. It is important here to highlight the idea that constructing identity depends on the possibility of having recourse to multiple identities, and the risks arising from a unique identification of the individual.

Chapter 2 considers the way in which this personal autonomy is set up, focusing on the European and French context. Traditionally, law considers identity from two viewpoints: that of the state, which has set up a system of establishing civil status so as to individualise one person in relation to others; and that of the person who has a right to personal fulfilment whereby he can establish for himself the components of his identity as a human being. The digitisation of our lives on a massive scale makes it essential to find a new balance between the process of mass identification of people by administrative bodies and the possibility for an individual of acting freely and autonomously.

Chapter 3 focuses on technical means. After drawing a distinction between the concepts of identification and authentication, it considers the changing use of digital identities in information systems and possibilities of tracking the activities of a user. It sets out the argument concerning the limitations of the anonymity and pseudonymity solutions currently in use.

Chapter 4 looks at economic issues. Given that most business models today use targeted advertising and price discrimination based on knowledge of the user's preferences, it is important to understand the ways in which the pseudonymous status of the user influences his ability to pay. Another question is whether it is possible to design business models that are not based on the direct monetisation of personal data.

The big question then is how to set up digital identity systems while achieving an optimum balance between personal autonomy, respect for people's fundamental rights, particularly personal data protection, and the interests of economic players. With this in mind, this Handbook concentrates on the spectrum of digital identities that can be used by an individual in the European context. It thus considers the following questions from the personal data protection viewpoint:

- What are the fundamental issues raised by digital identity management systems?
- How have management systems of this kind been rolled out in France and Europe, or how are they now being rolled out?
- What are the limitations of the current systems?

While Chapter 5 provides the basics for an understanding of existing systems, Chapter 6 explains how to implement the key principles of personal data protection so that the systems collect and use the attributes of individuals in a lawful way. This legal perspective must necessarily go hand in hand with a technical approach. Accordingly, Chapter 7 sets out the solutions that can be implemented in designing a digital identity management system, and then throughout its life span, by use of the "Data protection by design" approach.

Chapter 8 provides a comparative analysis of the systems in use in four European countries. Particular emphasis is placed on "hard" digital identities whose deployment is today a major political issue, dealing as it does with the practical administrative and technical ways in which citizens are recognised by their own state and by the other European states.

Chapters 9 and 10 are concerned with the situation in the near future; they respectively describe the regulatory framework currently put in place in the European Union via regulation (EU) no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and the various forms this trend is taking in the French context.

Lastly Chapter 11 starts out from the observation that conventional digital identity management systems are inadequate to guarantee multi-identity and protect personal data. It sets out an alternative based on the exchange of identity or attribute credentials. These credentials have the advantage of attesting certain characteristics of the individual without in the process revealing his personal data.

This Handbook is designed to be a practical tool for any person, citizen, business leader, professional or teacher for whom the question of digital identities is an important issue.

The reader can explore the subject further thanks to the many bibliographical references, the recommended reading and the conferences organised by the Chair Values and Policies of Personal Information.

This article has been translated from French by Peter Thomas

For further information: www.personal-information.org

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