Digital Identity Attributes Cohesion to Aceess E-services: Major Issues and Challenges in Digital Society

Ghazi Ben Ayed, Solange Ghernaouti-Hélie
Faculty of Business and Economics
University of Lausanne
CH-1015, Lausanne
Switzerland
ghazi.benayed@unil.ch,*sgh@unil.ch*

ABSTRACT: *Today, many of our daily tasks are accomplished through the use of E-services that require user's authentication based on specific number of digital identity attributes.These attributes are dependent to particular context of an E-services provider. For an end-user, different E-services may require different sets of attributes, which reside in multiple locations. More often digital identity attributes aggregation or cohesion is needed to establish trust during the authentication process when accessing E-services. In this paper, we provide a literature review of major issues and challenges related to digital identity cohesion. In the first line, we lay a particular emphasis on technical issues and in the second line we provide an overview of major economic and ethical challenges*

Keywords: Digital identity, Attributes-based cohesion, E-services grant, Cohesion issues and challenges

Received: 17 January 2011, Revised 12 March 2011, Accepted 21 March 2011

1. Introduction

Broadband Internet is diffusing rapidly and it is accelerating online activities and E-services grant such as online shopping, education, use of government services, download and playing digital content, and use of video telephony [1]. We ascribe "Out of Many, One", a Latin translation of "E Pluribus Unum" that is used in the Great Seal of the United States, to point out the idea of digital identity aggregation and cohesion. The goal of digital identity cohesion is to establish a relationship between individual's attributes in order to allow users to contract E-services.

In the offline world, anonymous transactions are conducted successfully, but in the online service-oriented world, E-services providers need to know identity information of the service recipient. Thus, building identity infrastructures is considered an attempt to establish a community of trust, which becomes a requirement for online business [2]. When E-services provider compels a combination of multiple identities residing in fragments within distributed and disparate business applications to be presented in order to fully identify the individual, identity cohesion capabilities become a requirement for E-services access control.

This article deals with major challenges and consequences of digital identity cohesion when accessing E-services. We present basic concepts of identity and digital identity in section two. In section three, we describe the importance and needs of digital identity cohesion in general and particularly in the context of E-services. In section four, we stress on technical issues of digital identity cohesion for users and E-services providers; and we provide an overview of major economic and ethical ones. We conclude in section five by providing few recommendations.

2. Identity and Digital Identity

2.1 Basic Concepts of Identity

The concept of identity is evolving over time. The term 'identity', which is firstly known used in 1570, has been used in many different ways in academic research and in popular usage [3]. The term is still of disputed origins, but its origin may derive from Middle French 'identité', from Late Latin 'identitat-, identitas', or probably from Latin 'identidem' repeatedly, a contraction of 'idem et idem' and literally 'same and same' [4]. Several decades ago, human identity was defined by geography, community, and family relationships. If an individual was born into a well-known and rich family or in a poor remote community, he or she would remain and would typically not be able to change their life pattern or economic status over time. One's geophysical space and place in society were inextricably linked and the declaration of an individual's name, sometimes accompanied by the name of their city or village, was sufficient to prove his identity. Today, individuals are having greater choice for participation in different social circles, and more possibilities and freedom of social and economic mobility. In addition, the notion of identity has been extended not only to humans, but animals, machines, organizations, devices, and other objects or resources. A machine has an identity that allows to access certain information at certain times, or be employed by some individuals, to the exclusion of specified others [5, 6].

'Identity' is defined as a collection of data about a subject that represent attributes, preferences, and traits. A 'subject' refers either to a person, a group, a software program or another entity. 'Attributes' describes a property associated with the subject such as physical trait, network address, medical record, purchasing behavior, bank balance, credit rating, dress size, and age. 'Preferences' represent desires such as preferred seating on an airline, brand of ice cream, and preferred language, and used currency. 'Traits' are like attributes but two differences are noticed between them: traits are inherent rather than acquired, and attributes may change but traits change slowly. Examples of traits are person's blue eye, hair color, company's location and date when it was incorporated. We typically use, in this article, attribute to mean all three unless there's a need to distinguish among them [2].

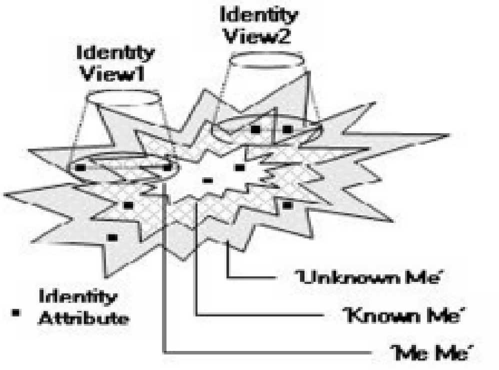

Figure 1. Identity views and attributes – Adapted from [7]

Authors [7] classifies identity information into three perceptions based on awareness of identity and control over it: 1) 'Me-Me' refers to the part of the identity information that the subject is aware of and directly controls, e.g. residence address; 2) 'Known-Me' is the part of identity information that the person is aware of and indirectly controls such as revenue data and the associated tax levels that are under the control of the department; and 3) 'Unknown-Me' is the part of identity information that the person is not aware of and over which the person has no control. This information can be controlled by known parties such as certification authority, or by unknown parties such as credit rating agencies and identity thieves. We believe that this picture of identity that comprises multiple views, perspectives, or views is derived from a multi-dimensional classification of the human world, and the definition and role of identity in social sciences.

2.2 Digital Identity Part of the Overall Identity

Digital identity is an intersection of identity and technology and represents identity in the digital world [8-11]. Wherever we go, we leave traces of fragmented information about our identity. We leave a comment in a forum, fill out a form, maintain a blog, create full profile that comprises a photo, name, phone number, and other information in a social network, and conduct a parallel existence. Educating others about who we are, what we do and especially what we think is constructing 'digital identity'. Some Internet users strive to share their digital identity with others to re-enforce their online presence and others try to hide it for security and privacy considerations.

Digital identity is defined as 'the data that uniquely describes a subject or an entity and the ones about the subject's relationships to other entities' [2]. The same author gives the car title as example of digital identity. The car title contains VIN identification number that uniquely identifies a car to which it belongs and other attributes such as year, model, color and power. The title contains also relationships such as the set of car owners from the time it was made. From technical perspective, the same author explains that digital identity is built on set of technologies that includes cryptography, authentication, authorization, identity provisioning, directories, digital rights management, identity federation, and interoperability standards. However, the author [12] does not distinguish between identity and digital identity. He provides a broad definition of identity from a computing perspective as 'a computer representation of an active entity that can be physical (such as human, a host system, or a network device) or a programming agent'. We believe that both identity and digital identity are parts of the overall identity. We borrow the words of an author, who holds two citizenships, in response to the question: how do you perceive your identity: half French and half Lebanese? 'The identity cannot be compartmentalized; it cannot be split in halves or thirds, nor have any clearly defined set of boundaries. I do not have several identities; I only have one, made of all the elements that have shaped its unique proportions" [13].

2.3 A Mutation from One YOU to Multiple YOUs

Digital identity is partial. Partial identities construction is a consequence of context-specific nature of identity. Partial identities are any subset of attributes associated with the subject who can select for interacting with other parties. For instances, a traveler.

3. Digital Identity Cochesion

Attributes are either unified into one all-encompassing digital dossier or relationships are defined between them. Digital identity attributes are rarely stored in one place but rather in diverse and various stores residing within multiple E-services providers. As a consequence, the individual is in one-to-many relationship with his identity.

3.1 Motivations for Digital Identity Cohesion

Subjects undergo a process of digital identity cohesion for several reasons:

3.1.1 Convenience of the Experience

Through the use of a single point of access and convergence services such as Universal Social Networks, and Single Sign-On, abbreviated USN and SSO. Online social networks and activities are having more visibility and gaining more accessibility through USN since it permits to facilitate access to user's feeds coming from different socials networks. We classify USNs into four categories: a) social feed aggregator e.g. MyMashable [16]; b) desktop aggregator e.g. 8hands [17]; c) people finder such as Wink [18], a people search over the user profiles of MySpace, LinkedIn and Bebo; and d) users' bookmarks aggregator such as SecondBrain [19].

3.1.2 Trust Establishment between Parties

Applications and services may require more attributes to authorize the subject accessing resources. In addition, online reputation systems are in use to trust parties and conduct secure online business. For instance, EBay reputation mechanism unifies member's transaction feedback history to calculate community members' reputations in the form of colored and shooting stars. The feedbacks given by users in EBay and Amazon are mechanisms that could influence online buyers but we believe that feedbacks are relatively accurate.

3.1.3 Security when Identifying Criminals and Reducing Identity Theft

There are high and urgent societies' expectations and needs for digital identity cohesion capabilities to help police investigators to identify a criminal blended in with many people. For instance, after 9/11, the American Defense Department launched a program called "Total Information Awareness" to compile and unify as many data as possible: e-mails, phone calls, web searches, shopping transactions, bank records, medical files, travel history and much more. However, DARPA researchers argued that the World Trade Center bombing of 1993 and the Oklahoma City bombing of 1995 might have been prevented if US public security services could have linked commercial databases to identify large purchases of fertilizer by non-farmers [20]. Currently, services providers are using advanced tactics, collectively known as identity scoring that allows monitoring online data mining, pattern recognition, even semantic analysis of information about a subscriber that appears on Web pages. Examples of firms that offer such services are Garlik in England and MyPublicInfo in US. Garlik offer 'data patrol' service to British residents by combing credit reports, public databases and Web sites for information about customers and presents them with a detailed profile. The profile should show whether criminals may be trying to use their personal facts to apply for credit cards, take out a loan, or register a fake driver's license or marriage certificate. MyPublicInfo pieces together a customer's public identity profile' and alert him or her to dubious changes [21]. Moreover, the subject must be able to combine selected attributes made about himself by more than one identity authority into a minimal composite set of attributes and be able to present them to relaying party, who could not be able to repudiate the original attributes [14].

3.1.4 Economy around Digital Identity

'Gold Rush' (1925), the Charlie Chaplin's movie, is a true illustration of major gold rushes that took place in the nineteenth century in Australia, Brazil, Canada, South Africa, and the United States [22]. Today's new form of 'rué-vers-l'or' is digital identity. Digital identity?is perceived as the new frm of money that would facilitate today's trade between parties as the money and precious metal did in the past and will do in the future [23]. The value of digital identity increases as much as substantial quantity of digital identity attributes has been collected and aggregated. Many people search engines such as 123People engine, Spock, Social Security Death Index (SSDI), Intelius and USsearch are evolving to better provide free and paid digital identity disclosing services based on cohesion of attributes available on the Web.

3.1.5 Subject's Digital Identity Construction

Digital identity attributes become publicly available and easy to access. Each person now leaves in cyberspace an increasingly amount of digital footprint when aggregated and unified, contributes to the definition of the subject's digital identity. Visible or invisible, left consciously or not, this set of data can be collected from various sources. The very first digital records of pre-natal scans could be shared on flicker and the obituary information on Find a Grave[24]. It happens also that other data could be available and collected through the one collected by diverse agencies and organizations on our behalf during our life, the blogs that are kept, the emails sent and the internet searches performed. Maintaining and editing personal information in learning digital portfolio or personal profile within social network is much feasible and easier than the personal profile that is carried out kept by an employer 'googling' prospective employee, tracking activities as a citizen, and possibly inferring health problems from the visible activities in self-advocacy online groups. For instance, We Feel Fine [25] is a people feeling cohesion engine that harvests automatically human feelings from a large number of blogs every ten minutes. Compiled blog data [26] comes from a variety of online sources, including LiveJournal, MSN Spaces, MySpace, Blogger, Flickr, Technorati, Feedster, Ice Rocket, and Google. The engine scans blog posts for occurrences of the text fragments 'I feel' and 'I am feeling'. The approach was inspired by techniques used in Listening Post project [27]. These digital identity fragments could have been posted by users on the net either voluntarily or involuntarily. The user could also collaborate with E-services providers to have acces to E-services without having the intention to construct his digital identity.

3.2 Digital Identity Cohesion and E-services

Access control and policies are different within different applications. Each application or E-service provider requires a specific set of attributes to let the subject consuming the E-service. This is reflected in the real-life, various forms of identity are required to various contexts in which, the identity is to be presented in a suitable way and within suitable information to get access to service's assets. For instance, a customer is asked to provide a credit card and fidelity saving card in a movie store to take advantage of DVD prices rebates, and a visitor is asked to provide more than one than one identity proof comprising different identity information such as ID cards to get into some mistrusted or restrictive environments, such as national security organizations. The digital identity cohesion is considered as one of the current challenges and a critical step to authenticate the subject and controlling access to E-services [2, 12].

4. Digital Identity Cohesion Issues And Challenges

The author of the Economist magazine article [28] explains the current situation of digital identity aggregation and cohesion by pointing out that despite years of large-scale efforts, law-enforcement and intelligence agencies' databases are still not effectively linked yet. He gives the examples of health care industry in which computerizing health records tend to run into bureaucratic, technical and ethical problems. The digitization of health records could have been helpful to spot and monitor health trends and evaluate the effectiveness of different treatments. We explain in the following sections that mashing digital identity attributes, from credit-card bills to cell phone logs, poses technical, economic, legal and ethical problems.

4.1 Technical Issues

The author [20] explains that digital identity cohesion is hard because we are drowning in data from a multitude of sources, all with different levels of detail and uncertainty. He points that John Marlan Poindexter, a career naval officer, bridged complexity of data cohesion technical issue as finding a submarine enemy in the vastness of the ocean. Poindexter says that identifying the signatures of terrorist preparations in an ocean of data is much harder than finding subs in an ocean of water.

In addition, Poindexter argues that oceans may be huge but every spot can be uniquely identified by a latitude, longitude and depth. However, data oceans are not so easily to be categorized. Much of information are spread across millions of computer systems. In addition, oceans are not doubling in size every few years like data oceans. Major issues for aggregators are:

4.1.1 Data Quality

Much of the personal data in databases may not be accurate and they are riddled with errors and meaningless coincidences. For example, a Scientific American editor ordered an US$ 80 report from an online identity consolidator, including criminal, real-estate and bankruptcy records. It was riddled with errors such as misspellings and confusion with namesakes. The report showed no signs of identity theft! Currently, algorithms overcome only some of these hurdles but not all of them [20].

4.1.2 Semantics of Aggregated Digital Identity

Companies are increasingly linking isolated databases together into one data scheme could infect a person's entire digital identity and reputation either by stealing data scheme or through attributes cohesion bias, particularly decontextualization of digital identity by data mining algorithms. The author [12] stresses that managing and maintaining identity repository separately would inhibit scalability and multiply attributes inconsistencies. More dramatically, he adds that attributes that are stored in heterogeneous stores within different formats and schemes (e.g., databases, directories, HR repository, and Web application server) would increase management difficulties. For instance, adopting a unique data cohesion schema may yield to attributes deconteactualization issue.

4.1.3 Identity Resolution

It consists of matching up the various names and account numbers with the right individual by taking into account cultural variation in names and other business-related rules [20, 29]. Idetntity resolution issue is consequance of the two data quality ans semantics issues. In online world there may be dozens of people sharing the same name and dozens of names used by the same person, thus the issue deals with ontology and syntax of attributes. Person's first name may be listed in one database as Robert, in another as Rob and in a third as Bob. Attributes semantics, ontology, syntax and interoperability issues arise whenever digital identity attributes are to be aggregated. For example, when Attributes Fusion Engine (figure 2) aggregates attributes, how E-services could recognize that the short names 'G. Ben Ayed' and 'Ghazi B. Ayed' are referring to the same person with a full name 'Ghazi Ben Ayed'? In addition, names written with typo errors such as 'Gazi Benayed' and 'Ghasi Bennayed', the ones written in other languages and following cultural semantics such as Hispanic, Japanese, Chinese and Arabic, or Arab names written with Latin font could be automatically recognized as being part of the same subject's identity?

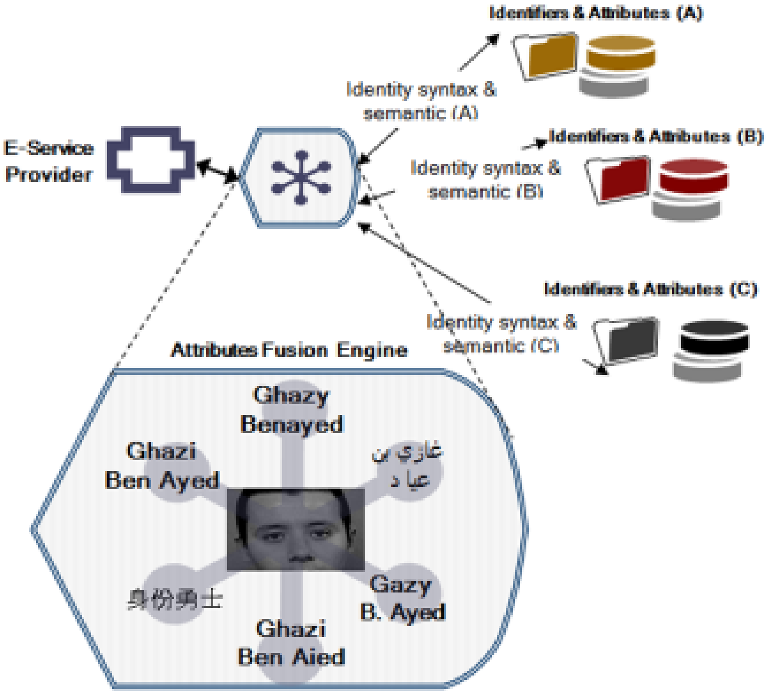
Identifiers & Attributes (A)
Identity syntax & semantic (A)
E-Service Provider
Identifiers & Attributes (B)
Identity syntax & semantic (B)
Identifiers & Attributes (C)
Identity syntax & semantic (C)
Attributes Fusion Engine
Ghazy Benayed
Ghazi Ben Ayed
غازي بن عياد
身份勇士
Gazy B. Ayed
Ghazi Ben Aied

Figure 2. Identity resolution issue

The authors [11] explain that digital identity cohesion operation must support vocabulary definitions of digital identity attributes. All parties concerned with digital identity services share a common ontology and semantic web metadata formats could throgh Resource Description Format (RDF) and RDF Schema usage could an interesting clue to resolve this issue.

4.1.4 Digital identity cohesion algorithms adjustments

Data cohesion algorithms can trace its heritage back to the computerized matching programs of 1970s. US government authorized the creation of the Federal Parent Locator Service that denies a wide range of federal benefits to parents who are behind on their child support. Those data are aggregated with digital identity of recently employed parents who are not up to date on their payments so that their wages can be garnished. For instance, casinos have funded development of a technique called NOnobvious Relationship Analysis (NORA), which combines identity cohesion and resolution with databases of credit companies, public records and hotel stays. The program works by building hypotheses based on existing profiles and then revising these hypotheses as other digital identity attributes become available.

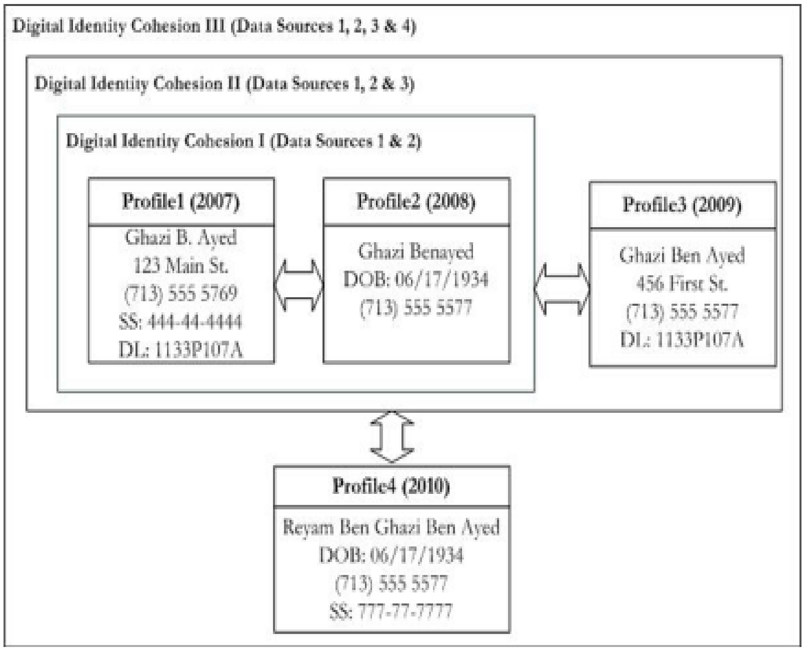

Figure 3. Matching names algorithm

In the 1990s software engineer Jeff Jonas developed a system that could match the names in a casino's computers with other sources of information. Figure 3 shows that four of the profiles reside in different locations and have been collected in different periods of time. Digital identity cohesion I combines profile1 and profile2 and each of them holds different attributes, so the system provisionally assumes they represent different individuals. In cohesion II, the system infers that profile3 holds attributes common to both previous profiles: the driver's license number from one and phone number from the other. So the system reassigns all three to the same individual. Finally, digital identity cohesion III shows that profile4 includes a birth date matching with profile2, thus, the system deduces that the four profiles actually represent two individuals. The program guesses that the two may be father and son since they share the same surname and phone number. In 2005, Jonas sold the system and his company to IBM, which has added a feature called anonymous resolution. Two organizations can determine whether they share the digital identity of an individual in their databases without revealing digital identities of all people who do not match. The technique works by comparing cryptographic hashes instead of digital identity attributes. Currently, most algorithms of data cohesion have some kind of sensitivity adjustment. Tipping the scale to the right, and the system fails to find genuine matches; tipping it to the left, the system turns out to be wrong because too many predictions are achieved. Another important issue raised by data cohesion is to find an algorithm that it never confuses original data with a conclusion inferred from those data [20].

4.1.4 Digital Identity Cohesion Technical Models

Models are to be chosen in response to well-defined cohesion requirements. Many authors are stressing that a closer look should given to digital identity cohesion models, called technical models of digital identity systems, identity management models [12], or identity cohesion conceptual models [31]. The OECD report provides a comparison between siloed, centralized,federated and user-centric technical models. Supremacy has been given to user-centric technical model for privacy and user control over identity considerations [30]. Two of the centralized models are particularly specified meta- and virtual- centralization, which are compared to identity federation models based on a set of criteria [12, 31].

In the next section, we do not intend to cover all the economic and ethical issues but the major ones.

4.2 Economic Issues

The value of digital identity increases as much as substantial quantity of attributes' attributes has been collected and aggregated. This could encourage fraud e.g. identity theft, loss of identity, and misuse of personal information, therefore economic losses could be sought. For instance, in response to such risk, Naymz [32] offers identity aggregator feature, reputation assessment tool, and reputation score 'RepScore' in order to build trust-based professional community.

Economic gains should justify cohesion costs. In 1994, the author [20] studied computerized matching programs maintained by federal and state governments in the U.S. and Australia. These systems scanned millions of records and flagged thousands of potential "hits." But most of them turned out to be false positives. The benefits did not justify the costs of collecting data, training personnel and chasing down the false positives. However, the same author points that many people feel that if a data-cohesion program could anticipate and stop a major terrorist attack; it would be worth whatever it costs.

4.3 Ethical Issues

From the ethical and legal perspectives, linking together attributes into a single profile through the process of data cohesion is still the bête noire of privacy advocates. They advocates still considering that digital identity aggregators use personal information for purposes other than the ones for which it was originally acquired [20]. But, if identity linking is deemed necessary, safeguards that ensure privacy limits respect should be implemented because attributes linking and data sharing should be under the sole control and consent of the subject. Thus, benefits of attributes-based digital identity cohesion should be weighed against the risks to privacy [8]. In most countries, privacy is linked to personal data protection laws. The legal approach is to be taken into consideration when dealing with privacy issues. Moreover, the concept of privacy is part of fundamental human rights and it is a prerequisite of real freedom of expression.

5. Conclusion and Outlook

Today, in our digital society is based on knowing more details about digital identity of subjects. In such context, attributes-based digital identity cohesion is considered as an urgent requirement for identifying subjects to access E-services. In this article we identified and detailed in the first line main issues related to attributes-based digital identity cohesion and give an overview of some relevant economic and ethical related issues that are faced by individuals, private and public institutions. Our primary objective was to analyze technical issues without forgetting to take into consideration the importance of economic, legal and ethical challenges. We are convinced that non-technical issues are as important as technical ones, but it was not the scope of the article to focus on non-technical ones, which will be analyzed and detailed in further publications. The benefits of attributes-based digital identity cohesion should be weighed against its consequence.

Digital identity allows subjects accessing e-services and for this reason it becomes a valuable asset. Protecting and securing digital identity cohesion would reduce identity theft and increase trust. In addition, we need not only just a cohesion but an effective attributes' attributes management because a poor administration and maintenance of duplicated, out-of-date, and low-quality attributes' attributes may expose enterprise assets and resources at a high risk.

Dealing with digital identity is a complex problem with several facets and for this reason it should be apprehended in a global perspective through a coherent, integrated and interdisciplinary approach. The digital society has had an important impact on our lives and common society's yardsticks have changed including the concept of identity. In fact, digital identity is much more than a sequence of binary digits of personal information and attributes.

References

[1] Organization for Economic Co-operation and Development (OECD) (2008). OECD Information Technology Outlook 2008 Highlights, ed.

[2] Windley, P, J. (2005). Digital Identity: Unmasking identity management architecture (IMA). O'Reilly Media.

[3] Akerlof, G. E. A., Kranton, R, E. (2010). Identity Economics: How our identities shape our work, wages, and well-being: Princeton University Press.

[4] Merriam-Webster Online Dictionary. (2010). Definition of Identity. Available: http://www.merriam-webster.com/dictionary/identity.

[5] Olson, E. T. (2008). Personal Identity," in Standford Encyclopedia of Philosophy, ed.

[6] Noonan, H. (2009). Identity, *In*: Stanford Encyclopedia of Philosophy, ed.

[7] De Clercq, J., Rouault, J., (2004). An Introduction to Identity Management. Available: http://devresource.hp.com/drc/resources/idmgt_intro/idmgt_intro.pdf.

[8]. Center for Democracy & Technology. (2007). Privacy Principles for Identity in the Digital Age [Draft for Comment - Version 1.4]. Available: http://www.cdt.org/files/pdfs/20071201_IDPrivacyPrinciples.pdf.

[9] International Telecommunication Union. (2006). Digital Life. ITU Internet Report Available: http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf.

[10] Cameron, K., (2005). The Laws of Identity, ed: Microsoft Corporation.

[11] Damiani, E. (2003). Managing Multiple and Dependable Identities, *IEEE Internet Computing* - IEEE Computer Society, p. 29-37.

[12] Benantar, M.(2006). Access Control Systems: Security, Identity Management and Trust Models: Springer Science + Business Media.

[13] Facing History and Ourselves Foundation, (2008). Stories of Identity: Religion, Migration, and Belonging in a Changing World, ed.

[14] Organization for Economic Co-operation and Development (OECD). (2008), At Crossroads: Personhood and Digital Identity in the Information Society. The Working Paper series of the OECD Directorate for Science, Technology and Industry. Available: http://www.oecd.org/LongAbstract/0,3425,en_2649_34223_40204774_119684_1_1_1,00.html.

[15] Caroll, J., Murphy, J., Who am I? I am Me! Identity Management in a Networked World, *In*: Proceedings of the 4th International We-B Conference.

[16] Mashable: The social media guide. Available: http://my.mashable.com/.

[17] 8hands Intelligent Social Network Aggregator. Available: http://www.logiagroup.com/socialNetworks.html.

[18] Wink: People search engine. Available: http://wink.com/.

[19] Secondbrain: Save, share & discover great bookmarks. Available: http://secondbrain.com/.

[20] Garfinkel, S, L., (2008). Information of the World, UNITE! Scientific American Magazine. 82-87.

[21] Fischetti, M., (2007). Scoring Your Identity: New tactics root out the false use of personal data Scientific American 27-28.

[22] Wikipedia. (2010). Gold Rush. Available: http://en.wikipedia.org/wiki/Gold_rush.

[23] Crosby, J., (2008). Challenges and Opportunities in Identity Assurance.

[24] Find a Grave. Available: http://www.findagrave.com/

[25] Harris, J., Kamvar, S., We Feel Fine Project: An exploration of human emotions, in six movements Available: http://wefeelfine.org/ [Accessed: May 15th, 2010].

[26] Harris, J., Kamvar, S., We Feel Fine Project: Blogs Data [Online]. Available: http://www.wefeelfine.org/data/files/feelings.txt.

[27] Hansen, M., Rubin, B., Listening Post Project. Available: http://www.earstudio.com/projects/listeningpost.htm.

[28] Cukier, K. (2010) The Data Deluge: Businesses, governments and society are only starting to tap its vast potential. The Economist (February 23rd-March 5th). Available: http://www.economist.com/opinion/displaystory.cfm?story_id=15579717.

[29] McCallum-Bayliss, H. (2004). Identity Resolution in a Global Environment: Fishing for people in a sea of names IEEE IT Pro. 21-26.

[30] Organisation for Economic Co-operation and Development. (2009). The Role of Digital Identity Management in the

Internet Economy: A primer for policy makers Available: http://www.oecd.org/dataoecd/55/48/43091476.pdf

[31] G. Ben Ayed, "Consolidating Fragmented Identity: Attributes Aggregation to Secure Information Systems," IADIS International Journal on Computer Science and Information Systems, vol. 4, pp. 1-12, 2009.

[32] Naymz Features. Available: http://www.naymz.com/about.action?section=compare.

Author Biography

Ghazi Ben Ayed is currently a researcher in Information Systems research Institute. He holds a Ph.D. degree in information systems from business and economy HEC Faculty, University of Lausanne, Switzerland. He received a M.Sc. degree in E-commerce from HEC Montreal & University of Montreal, Canada; Leadership graduate certificate from McGill University, Montreal, Canada. He played consulting key roles in several projects in Canada and USA as an IT solution/ERP integrator and R&D developer. G. Ben Ayed's current research interests include privacy and security engineering, service-oriented analysis and design, digital identity management, digital reputation, trust and digital identity hiding.

Professor S. Ghernaouti–Hélie has been a member of the Faculty of Business and Economics at the University of Lausanne since 1987. She was previously a network architect, an ISO standardization expert, and a marketing product manager for international IT companies. Currently, she is president of the Social Commission and president of the Equal Opportunities Commission of the University of Lausanne. She is an international expert on cyber-security and cybercrime related issues. She is active as an ICT security analyst, possessing extensive experience of security governance, security strategies and the evaluation of security policies. She is a cyber-security expert for the ITU, and was a member of the High Level Expert Group for the ITU – Global Cyber-security Agenda. In this context she was co-leader of the working groups on "Capacity Building" and "Organizational Structures" and one of the co-authors of the Global Cyber-security Agenda's Strategic Report (2008). She is a prolific writer and speaker and the author of more than twenty books including the ITU reference guide "Cyber-security for developing countries", presented at the World Telecommunication Development Conference, Doha, in March 2006 and subsequently translated into Chinese, Russian, Arabic, Spanish and French.