chapter four
identity.digital

The headlong development that has characterized the digital world from its very inception has not been even in all its parts: some issues have been relatively neglected and have not kept up with rapid technical and market changes. Among these are questions relating to digital identity, data security, and consumer privacy. With all the expansion in progress in this domain, and the constant innovation, the risks involved are magnified and thus assume an increasing urgency. Matters such as social participation and interaction in the digital environment are equally important to consider as they ultimately provide the backdrop for developments in this field. This chapter examines the rapidly changing technological and social environment surrounding the individual (later referred to as the "digital individual"), and the blurring boundaries between the public and private spheres of existence. Detailed consideration is then given to the establishment and management of digital identity online.

4.1 The digital individual

4.1.1 From person to personae

The complexity of the interaction between technology, personal consumption and the construction of virtual identity in cyberspace has traditionally been ignored[1], but is now the subject of observation in many quarters. Users of digital technologies today have a wide scope for constructing their identity. The mostly nameless and faceless environments of cyberspace create an ideal background for developing alternate identities or digital personae. Unlike face-to-face interaction, it is much more difficult to categorize people online according to age, gender, race, country of residence, social class, body shape etc. Consequently, users may feel more inclined to interact in what seems to them a more anonymous and forgiving world.

Moreover, the internet makes it fairly easy for individuals to create multiple representations of their identities, mainly due to the lack of a generic system for identification. This fragmentation of identities can be accidental, but also intentional[2]. Creating more than one identity can even be desirable to some, depending on the context and exchanges involved. For instance, a user may wish to be aggressive and egotistical in one context (e.g. in a multiplayer game), but sensitive and sociable for virtual encounters of the romantic kind.

Alternate identities can enable the exploration of a wide variety of feelings, personalities, interests and motivations. The phenomenon of online avatars has served to make these more popular and accepted[3]: an avatar is an icon or representation of a user in a shared virtual reality space[4] (box 4.1). Although avatars were first used in online role-playing games (e.g. Everquest and Lineage) or virtual universes (e.g. Second Life and Active Worlds), their use is increasingly being extended to the non-gaming world, notably to online networking sites and forums. The avatar in this context is a picture or icon that a user of that community displays to represent his or her virtual self. In this respect, avatars may resemble a person's real or off-line self in varying degrees: wholly, partly or not at all. One of the most interesting examples of how the digital world affects the construction of identity is the phenomenon of gender switching, i.e. when users represent themselves as members of the opposite sex in social interactions online.

There are many reasons why people might take the opportunity to explore multiple identities, including:

- the ability to change character at will–this gives users the possibility of exploring other forms of existence and changing the ways in which they may be perceived by others;
- the opportunity to form relationships that may be perceived to be more difficult in the off-line world – e.g. between people from vastly different backgrounds or people who may be shy or uncomfortable with face-to-face interaction;
- the opportunity for those who are marginalised or persecuted in society to express their views freely without fear of discrimination or reprisal;
- the potential for finding groups and individuals with similar interests – identities online can bring geographically and socially disparate individuals together based on common interests, thereby stimulating dialogue and curbing loneliness;
- the possibility of sexual relations – virtual identity is important to those who seek romantic or sexual relations, particularly for those who lack confidence or have little opportunity to engage in such possibilities in the offline world.[5]

Box 4.1: Avatars and digital descents

Origins of avatar and its present use online

Avatar is a word that is commonly heard but rarely understood. It comes from the Sanskrit word *Avatara*, which means "the descent of God" or "incarnation." In English, the word originally meant "an embodiment, a bodily manifestation of the Divine." Below is the definition from the Vedas, the oldest and most comprehensive spiritual literature currently known:

> The Avatara, or incarnation of Godhead, descends from the kingdom of God for [creating and maintaining the] material manifestation.
> And the particular form of the Personality of Godhead who so descends is called an incarnation, or Avatara. Such incarnations are situated in the spiritual world, the Kingdom of God. When They descend to the material creation, They assume the name Avatara.
>
> *(Chaitanya-caritamrita* 2.20.263 -264)

The digital world has transformed the original meaning of avatar. Today, avatar most commonly refers to a graphical image of a user, for example in instant messaging applications, or, a graphical personification of a computer or a computer process. Avatars are intended to make the computing or network environment a friendlier place. An avatar can also be the virtual representation of a real participant in an activity in a virtual reality environment. For example, an avatar could represent a participant in a virtual meeting, or a tutor in a distance learning situation. To be effective, a digital avatar will need to have some basic human characteristics, such as speech and language capabilities.

Image source: insurat.com

Source: avatars.com

4.1.2 Blurring boundaries and digital interactions

An individual in today's world spends more and more time using digital means to communicate, be that sending and receiving e-mail, talking on a mobile phone, participating in a social networking site or playing an online game. As such, many aspects of daily life are increasingly mediated by technology, and this has important implications for human interaction and social behaviour.

As mentioned in Chapter 2, social networking sites like Cyworld (originally created in the Republic of Korea) provide good case studies for the changing nature of social interaction in the digital environment. Cyworld's new site, based in the United States, tells its visitors: "create and connect: record your days, keep up with friends and share what makes you special"[6]. The site has been adapted to the cultural context of the United States, but like its original version, site users can create their own avatars ("minimes") and virtual spaces ("minihomes" and "minirooms"). They can also display journal entries, photographs, and sundry virtual items (including lucky charms and miniroom furnishings). Users can reveal as little or as much as they like about themselves on the site, but the main objective is to encourage the sharing of details about personal lives that might not have been as readily shared in the offline world. An embedded "random minihome" function can transport Cyworld users to the minihomes of other users, where they can make comments, sign a guestbook, or buy gifts on a "wish list".

The rise of such social networking sites points to the increasing use of publicly shared experiences to form social bonds. Unlike the offline world, contact with strangers is not avoided, but encouraged and even expected. It is possible, and in some cases acceptable, to exaggerate, hide, alter or undermine the truth about oneself in order to encourage contact or construct more interesting and desirable online impressions or reputations. In some cases, online personalities can be vastly different from off-line personalities, and those who are well-liked and seemingly sociable in virtual spaces may not necessarily be so when engaging in social interactions off-line. Some may even forego interactions with real persons in favour of entirely virtual ones (box 4.2).

The growing use of mobile phones has been blurring the boundaries between the private and public spheres of existence even further. The mobile phone has become such an intimate and important aspect of a user's daily life that it has moved from being a mere technical tool to an indispensable social accompaniment. [7] Its highly personalized and emotive[8] nature has meant that its form and use have begun to represent the very personality and individuality of its user. In other words, it has in some respects become a reflection of a user's identity. Much can be gleaned about the personality of a user by looking at their mobile phone:

a) its model, shape and size;

b) the ringtone in use (e.g. traditional telephone ring, classical music, hip-hop or heavy metal music);

c) the chosen wallpaper (e.g. personal photo, cartoon, abstract or realistic landscape);

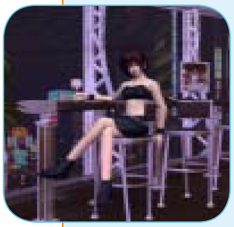
d) the messages and digital photos stored in the phone's memory (e.g. content, style, number, origin and so on).

It is little wonder that phone manufacturers and operators are capitalizing on this trend by offering an ever-increasing variety of customized and fashion-conscious handsets and services, thereby shortening the average lifecycle of their phones.

Mobile phones have transformed the way people interact in many respects. Not only can they communicate with each other anytime and anywhere, but they can also avoid contact by screening phone calls, resorting to voice mail, or limiting communication to SMS. Revealing yourself when phoning has become expected—some users might be criticized by friends when their incoming call is listed as "private" or "withheld". In traditional fixed-line phone environments, most calls were dutifully answered when possible, and the identity of the person on the other end was typically unknown, or at least unconfirmed, until the conversation was engaged. Today, many young people text each other before engaging in a voice call. There is a reticence towards voice communications until both parties are available, willing and prepared. Consequently, the spontaneity of voice communications has diminished, resulting in more controlled and predictable exchanges.

Box 4.2: You too can win her digital heart

The virtual girlfriend



For men who are tired of spending the time, trouble and expense of having a real girlfriend, the city of Hong Kong proposes a digital solution for their lonely hearts.

A creation of Hong Kong based Artificial Life, "Virtual Girlfriend" is a 3G mobile game in which users can meet, woo, date, and develop a relationship with virtual partners. The Virtual Girlfriend herself is based on intelligent animated 3-D characters existing only in the virtual world. Virtual girlfriends can be visualized and contacted using a 3G phone at any time. These virtual characters are usually involved in different activities throughout the day: for example, they could be relaxing at home, working in the office, lounging in a bar, dining in a restaurant, or shopping at the mall with a virtual friend.

Players in the game can observe their girlfriends during these various activities and interact with them via the mobile phone. The characters and the game follow a certain daily and weekly schedule which will continuously change and progress over time. The purchase of flowers and diamonds might serve to get increased attention from a character, and might develop the relationship to more advanced levels. In return, a virtual girlfriend might introduce the player to her virtual parents or friends, and unlock other aspects and details of her private life.

It is not all rosy, however. As in the real world, relationships do have their ups and downs. A virtual girlfriend can get angry and ignore a player if she does not get what she expects. And, since virtual flowers and diamonds cost real world money, players have to take care not to fall into the hands of purely money-minded digital characters. But, that as they say, is fate.

For women, the "Virtual Boyfriend" made its debut on 1 February 2005.

Image source: V-girl.com

Source: Artificial Life Inc., at **www.artificial-life.com**

On the other hand, recent fads such as "bluejacking" (communicating with Bluetooth-enabled mobile users in a given area) and "flash mobs" (the spontaneous assembly of people through targeted SMS and internet communications) have given an entirely new meaning to spontaneous communications and associations. Indeed, in the online world, spontaneous instant messages are encouraged between members of the same networking site, or even the same service (e.g. Skype through the "skype me" mode[9]). People are much more likely to contact strangers in the digital world for a query or comment about a website, a book, or a common interest in the digital world than they ever were in the off-line world (through e.g. the postal service or fixed-line phone). In some sense, therefore, everyone has become increasingly accessible. This can be desirable in some cases (e.g. a student can more easily write to her professor with a question) but undesirable in others (e.g. direct access to minors has become easier).

Yet another aspect of the digital environment is its impact on family structure and communications. In the past, a fixed line household telephone served as the gateway to all members of the family, be they parent or child. In the digital world, this has given way to individual gateways to each member of the household (e.g. father, mother, and school-going children). Families may own as many mobiles as they have family members, or even more (for instance, for business and home use). Individuals may typically own up to two or three e-mail addresses each. As such, channels for communication go up manifold, and many distinct exchanges can be carried on simultaneously. Whereas in the past, parents were aware of when their children might be interacting and with whom, today these exchanges can easily take place without the knowledge of other members of the family. In order to prolong participation in their peer group, many children engage in online chats or text messaging in their bedroom (and late into the night): this has been known to cause sleep deprivation[10], high monthly bills and parental frustration. On the one hand, this gives the benefit of allowing members to create and assert their individuality (e.g. a teenager who has an overbearing parent), but on the other hand, it can lead to disaffection from the family. Of course, the vacuum left by this disaffection may be filled, at least to some degree, by an affiliation with a chosen social network in the digital sphere.

Wireless e-mail and SMS have created another related phenomenon, that of the "permeability" of the separate contexts of social life[11]. People are frequently interacting with others present in their physical space and simultaneously messaging with other "remotely present" persons (by e-mail, SMS or MMS). This form of intrusion, or even potential intrusion, in any given social context has become commonplace. Among youths getting together for a social event, it would be unusual to expect that no one is seen using their mobile phone to interact with others. In fact, not doing so might even lead some to conclude that that person was unpopular. In this sense, much of one's digital reputation, or identity, is based on the quantity of communications received, such as the number of SMS or e-mail, the number of comments on a moblog or website, the number of visitors to a Cyworld minihome. Prospective employers may take into account the number of "hits" on Google that an applicant's name generates. Data available on the internet may also be used to verify elements contained in a curriculum vitae. Thus, it would seem that a sufficient connection between online and offline identity is required for societal purposes, especially in the face of the trend towards alternate and multiple identities.

4.2 Virtually private

The advent of the digital world implies a progressively ambient use of technology and communications. This in turn leads to an increase in the amount, quality and accuracy of data generated and collected. Not only does this increase apply to the ability to collect data, but also the ability to store, analyze and process it.[12] The sheer amount of data is alarming, but so too is its nature, which is ever more detailed and personal. The public and private spheres of existence are experiencing a progressive blurring of the boundary separating them. This creates a new set of concerns that bear serious consideration.

4.2.1 The value of privacy

The Merriam-Webster dictionary defines privacy as follows:

privacy:

- the quality of state of being apart from the company or
- isolation, seclusion or freedom from unauthorized oversight or observation;
- a place of seclusion or retreat *(archaic)*

Over the ages, privacy as a concept was not explored in much detail, and was not a popular subject of consideration. The great classical philosophers seem to have left it alone. But it is unlikely that this was a conscious omission. Perhaps it was thought to be a core aspect of existence, inherent to the very processes of life. The right to privacy has in many circles been viewed as the cornerstone of freedom and liberty.[13] Freedom lies in the ability to better understand one's position in the world and to develop opinions independent of external pressures. Indeed, a good deal of individual thought is a private matter.

It has traditionally been thought that what one thinks, believes and knows is inalienable to oneself, and may only be revealed with the voluntary consent of the thinking person. Slowly and gradually, however, this notion has begun to erode. Today, eavesdropping or monitoring by all sorts of agencies (not only governments) seems to have become regular practice. Large amounts of information can be gathered by a variety of actors, for legitimate or illegitimate purposes. The written works read by a particular community can be known, but so too can those perused by a particular individual. The early days of print media favoured one-way communications and information: by its very nature it ensured that the gap between authors and readers remained intact. The browsing and reading habits of today's digital individual, however, are subject to progressively more detailed observation and analysis. It can be argued that the current concerns surrounding privacy result from a technological shift in communications, from one-way print media to bi-directional flows of information: as such, it will become increasingly difficult to "reveal without being revealed, and to learn without being learned about"[14].

It might be rightly argued that digital technology has not been developed for the purpose of invading privacy. And in an ideal world, it is possible to conceive that the deliberate or accidental availability of data would not be detrimental to the individual. But today, with the wide and almost universal means of data acquisition, this is less and less the case. And of course, certain applications are being developed with this particular purpose in mind (e.g. profiling). Safeguards may need to be created to disable these applications from carrying out tasks indiscriminately. The universal availability of data, the ease of its accessibility, its durability over time, and the possibility of its early and infinite accumulation present us with an entirely new situation. In this context, the good news is that it is generally been accepted that data pertaining to the individual should only be propagated with the knowledge and consent of the individuals concerned. Many governments and organizations (commercial or otherwise) show an awareness of this aspect by making disclaimers at the time of the acquisition of data. But these efforts, often voluntary, are feeble in the face of the many challenges present in this field. For these reasons, the privacy of personal data, while appearing to some to be a subject of only passing interest, is actually of considerable importance, and moreover, one whose importance will grow with time.

4.2.2 Privacy and digital ubiquity

The vision of digital ubiquity is based on Gordon Moore's long term vision (known as Moore's law) of the increase in the power of microprocessors, which has held true with remarkable consistency, and also seems applicable to other parameters such as storage capacity and bandwidth. All indications are that this trend is likely to continue for some time to come, with advances in nanotechnology, RFID and sensor networks[15] further fuelling developments towards a global "internet of things"[16].

As digital innovation gathers even more speed and as the information environment becomes pervasive and intensely functional (such as in the case of smart homes), tracking and monitoring will become commonplace. As such, this "enriched" environment will differ from the more traditional information technology environment in four main ways[17]:

- Ubiquity: infrastructure and information will be everywhere and constantly on, affecting every aspect of daily life;
- Invisibility: the infrastructure will be cognitively or physically invisible to the user – as such, the user will have no idea when or where they are using a computing or communications device *per se*;
- Sensing: the network, mostly transparent to the subjects, will automatically record every activity, human and otherwise, and conscious input will be less and less necessary (such as through a keyboard);
- Memory amplification: selected activities (including private or personal ones), could be stored, processed, or retrieved.

The factors listed above, notably memory amplification, are likely to suffer further aggravation, due to expected exponential growth in digital storage capacity: thus, there will be little technical, or economic, incentive to delete anything. An information environment such as this can lead to easier and more widespread "eavesdropping" and to problems resulting from data leakage and device integrity (particularly as devices or sensors on the edges are inherently more mobile).

Furthermore, as more and more entities in the economic process (goods, vehicles, factories, equipment) are being enhanced with comprehensive methods of monitoring and information extraction (e.g. RFID), the entire lifecycle of products, beginning with their creation and ending with their complete consumption (or recycling) can be witnessed (and to some extent controlled) in real time. As such, the world "would be filled with all-knowing all-reporting things"[18]. Data collection would cross not only the boundaries of space, but also of time (with data about humans starting from pre-natal diagnostics to daily life in a retirement home). Thus, real-time ubiquitous monitoring will create new opportunities for "border crossings": natural borders, social borders, spatial borders and temporal borders.[19]

Naturally, information privacy is at the core of blurring boundaries and borders in smart and pervasive information environments. In order to ensure that border crossings are reasonable and fair, analysts and thinkers have put forth a number of information practices, notably Alan Westin in his book "Privacy and Freedom". Westin's principles include: openness and transparency, individual participation, collection limits, data quality, limits on usage, appropriateness of limits, and accountability. In multimedia environments, three main characteristics relating to the nature of information have been considered: the destination (or receiver) of the information, its use or purpose, and its level of sensitivity[20]. In a pervasive information system, awareness on the part of users must be added to this list, as invisibility of communications might hide from their view that information relating to them was being collected.

In the end, it will most likely boil down to one thing: intention. But intention can never be guaranteed. Data about an individual or a group of individuals in a digital environment can be used for beneficial as well as nefarious purposes. In this respect, digital technologies share common characteristics with many other technologies such as nuclear technology. Somehow, vigilance will have to be exercised and means found for the elimination of illegitimate uses of private data. This is doubtlessly urgent and important. At stake is human freedom itself which is recognized to be the very foundation of modern civilization. The maintenance of the privacy of designated data can be indispensable for the maintenance of a free society. This is especially true given the universal availability of computing power. A society in which every detail concerning an individual's interests and associations are recorded and easily available will result in a total freeze of movement – the equivalent of a traffic jam. The same holds good for the individual. It is on the basis of confidentiality and some minimum level of privacy that individuals are able to function. As data acquisition and accumulation proceeds apace, the equilibrium between privacy and convenience is threatened.

4.2.3 A delicate balance

The gathering, processing and analysis of information are crucial aspects of today's digital information economy. Without it, cash would be required for every purchase, there would be no licensed drivers, no health system, and no unemployment benefits. There is a balance to be struck, however, between the need to harness the power of information for economic progress, quality of life and convenience, and the need to curb potential abuses relating to its collection and distribution. The balance is a delicate one, but one to which the state and private corporations need to pay heed for the protection of individuals in an environment which has been deemed by many as a potential threat to human dignity.

The individual and the state

Many states have made attempts to manage data pertaining to their citizens, in order to provide streamlined and efficient government services. Moreover, since the number and scope of terrorist attacks continue to rise (e.g. New York in 2001, Madrid in 2004, London in 2005 and Mumbai in 2006), security concerns are increasingly at the forefront of national policy priorities. Biometric data is now being used in many cases for identification purposes, or for entry into a particular country, notably in the United States through its US-VISIT programme (under which foreign visitors are required to provide fingerprints upon entry[21]).

The United States government has been criticised for various measures introduced since 2001 that are seen to violate the protection of privacy, in the name of national security. In late 2005, for instance, an article in the New York Times revealed that in the months following the September 11th attacks, the United States President authorized the National Security Agency (NSA) to spy on citizens without a warrant or court order[22]. Since then, the NSA has been monitoring international phone calls and intercepting international e-mails between residents of the United States and people in certain foreign countries. Two opposing positions regarding the legality of such measures have emerged: the United States Department of Justice claims that the President acted at the "zenith of his powers in authorizing NSA activities", whereas the American Civil Liberties Union believes that the NSA programme "seriously violates the first and fourth amendments and is contrary to the limits imposed by Congress"[23].

The European Union (EU) attempted to harmonize its data protection legislation across its member states through Directive 95/46/EC on the protection of personal data[24] (hereafter referred to as the Data Protection Directive), which defines minimal requirements applicable at the national and European level in this regard, notably the sharing of databases using identifiers and the use of these identifiers by private bodies and citizens. Case law under the directive includes the 2006 annulment of a Council Decision[25] which concluded an agreement between the European Community and the United States on the processing and transfer of passenger data by air carriers to the US Department of Homeland Security, Bureau of Customs and Border Protection[26].

A single multi-purpose state identifier, also known as a single identification number (SIN), is under consideration in a number of countries. In the special administrative region of Hong Kong, an e-citizen card is already in use, with biometric data and preferences (box 4.3). The problem, however, is that despite a progressively borderless digital world, the application of the SIN is not globally harmonized, even within groups of countries that are otherwise

Box 4.3: All about who you are—on a tiny card

Residents in Hong Kong SAR see their identity go digital

It contains your name, address and birthday. It carries a template bearing your photo and fingerprint. It reveals your favourite books and travel records. It keeps track of your tax returns – all on a small card. And this is only the beginning.

The government of Hong Kong SAR launched an ambitious and innovative identity card replacement scheme in August 2003. In the course of the four-year programme, 6.9 million Hong Kong residents over the age of 11 were issued with a "Smart ID card". The objective was to introduce multiple value-added applications onto the identity card.

The card itself is made of polycarbonate and anti-forgery laser-engraving technology is used for printing personal data, and a digital photo. A duplicate of the data with digital thumbprint templates is stored in a chip embedded on the card, and authentication is required every time the data in the chip is retrieved. This prevents unauthorized access. If the chip is tampered with mechanically, electrically or electronically, there is a self-erasing mechanism, which denies an intruder access to the data.

Cardholders have the choice to decide whether to make use of the value-added applications of their Smart IDs. At the same time, the Hong Kong government continues to broaden the range of applications. By the end of 2004, for instance, card-holders were able to use their cards for immigration clearance through self-service control points. This facilitates the immigration control process notably at the border crossing between Hong Kong's SAR and mainland China, which handles nearly 300'000 people and 31'000 vehicles every day. If cardholders are not permanent residents of Hong Kong, their condition of stay and limit of stay are also stored on the chip. By the end of 2006, the Smart ID could also double as a driving license. The e-Cert, a free optional digital certificate issued by Hong Kong Post, allows various online transactions such as e-banking, stock trading and online payments. It is widely acknowledged that e-Cert will boost e-business development in Hong Kong in the immediate future. The Hong Kong SAR government is also hoping to encourage citizens to file tax returns online using the Smart ID-based credentials for identification and authentication.

To cater for the increasing number of Smart ID Cards and digital certificate holders, self-service kiosks have been installed at all Immigration Department offices to enable citizens to check the data on their ID cards. In addition, more than 600 public kiosks and computers in public transport stations, shopping centres, post offices, public libraries, and community centres throughout Hong Kong have already been equipped with smart card readers.

Image Source: sxc.hu

Source: Hong Kong S.A.R. Immigration Department and m**ultos.com**

closely associated, such as the member states of the EU. A recent study points to the increasing use of single identifiers across Europe: in 2001, 60 per cent of Member States had a national SIN and in 2005, that proportion rose to 78 per cent. Two countries have thus far been against the notion of a SIN due to data protection concerns: Germany and Hungary[27]. The study found that a minority of countries (three out of the fourteen studied) have constituted their respective SINs from purely random figures. The other eleven countries use meaningful data such as sex or date of birth. In terms of the data used, there is also a wide variety across countries. Some countries limit the data to those items that are absolutely necessary for reliable identification (such as family name, first name, sex, and date/place of birth). Many others, however, have identified a wider array of data points (over twenty in Bulgaria and Cyprus). In all, some thirty possible attributes were found, ranging from main domicile and marital status to photographs and academic titles (figure 4.1). The study concluded that while the use of SINs is widely prevalent in the EU, there are a number of different systems to constitute them: the number of data attributes, documents comprising the identifying numbers, the legislative and organizational framework set up to regulate the use of the SINs, and the role of the designated supervisory authority.

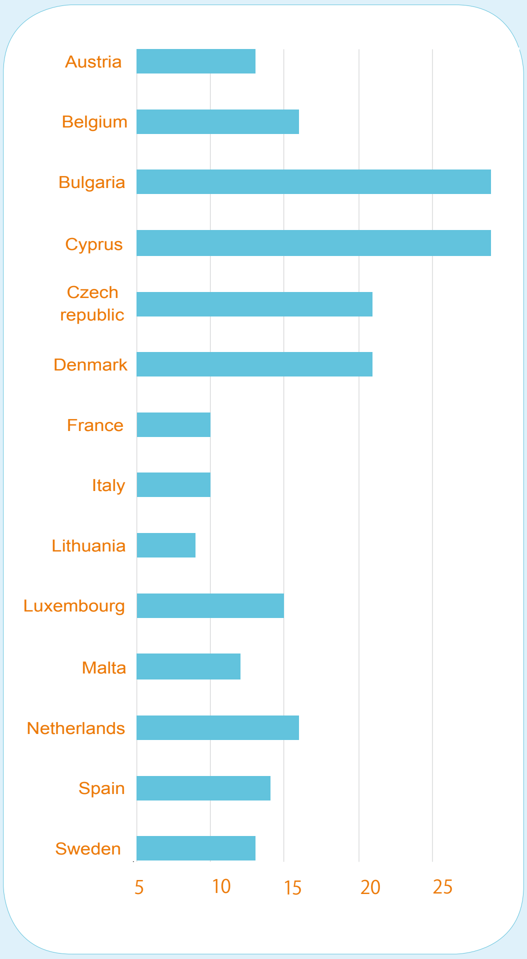
In light of the new technologies available to governments, the need for streamlined government processes and the growing concerns for national security, governments are studying and implementing new ways of using the vast databases of personal information that they have at their disposal, and those collected by companies and data aggregators. As such, some analysts warn that civil liberties advocates should not rely on protracted or inefficient government processes in the use of information and communication technologies (ICTs), and that to the contrary, inefficiency may itself pose a threat to civil liberties[28].

Although governments must work with market mechanisms to ensure security and raise awareness[29], they have a duty not to neglect or minimize their more general social responsibilities (ethical and social) relating to data use and protection[30]. Defining the limits of data collection relating to human individuals and the safeguarding of authorized data are matters of too great an importance to be left solely in the hands of private agencies. It is integral to the role of governments to be deeply conscious of human and privacy rights in the handling of data pertaining to citizens.

The individual and the corporation

Although a number of countries have taken steps to safeguard personal data gathered by their governments, this has not been equally true so far as the private sector is concerned. Legislation

Figure 4.1: A variety of SIN in Europe
Number of data attributes linked to single identification numbers (SIN) in selected member states of the European Union



Source: B. Otjacques, P. Hitzelberger & F. Feltz, "Identity management and data sharing in the European Union", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006

Box 4.4: Trashing data

What happened to eGroups user data after its purchase by Yahoo!

Yahoo! purchased eGroups in the Summer of 2000. At the time, eGroup users were not given permission to access their data unless they provided Yahoo! with a complete profile and agreed to entirely new terms of service. If users declined to provide a complete profile or agree to the new terms, Yahoo! maintained ownership of their data and the archives of their correspondence. In October 2001, a number of listserv owners had all of their archives and data deleted. They were given no explanation at the time, nor were they given any recourse. Their attempts to contact Yahoo! were in vain, and resulted in silence. In 2002, a Washington Post article was published on the subject, which finally gave the reason for the deletion. Apparently, Yahoo! had declared those users to be terrorists in the month following the 9/11 attacks on New York.

Image source: sxc.hu

Source: D. Boyd, MIT Media Lab

regarding access to information may go some way in keeping the public sector and credit agencies in check, but little has been done to make the private sector accountable in a similar fashion. Ubiquitous networks and technologies are creating a socio-economic paradigm, in what has been termed the “ambient economy” or “real-time economy”, and in which enterprises monitor their environment in real-time in order to be in a position to react instantly to changes affecting their business.[31]

Despite the recognition of the evolving socio-economic and technical context, there is limited recourse for individuals wishing to challenge the collection of data about their behaviour by private companies, or by those who have suffered damages as a result. If an individual attempts to block cookies from a certain website, for instance, the result may simply be exclusion from the website altogether. In such cases, it would seem that the monitoring of behaviour or user preferences becomes a prerequisite for accessing a particular service. By contrast, in the off-line world, loyalty cards offered by supermarkets or department stores remain optional, where shoppers may exercise discretion.

Moreover, online, the use of data about users can easily change hands, thus shifting contractual obligations. When Google purchased the Usenet archives owned by the company Deja in 2001, they were able to purchase all of the content that Usenet had collected, including statements made public by individuals. Google gave no guarantees about removing those statements from its data repositories. Thus, it would seem that any website or service that collects data on users can sell that data without the permission of the users. The purchaser of the data does not have to abide by the terms of the contract as understood by the users when they first signed up with the original service. A similar problem arose following the sale of eGroups to Yahoo![32] (box 4.4). Criticism over Microsoft’s Passport platform also points to the importance of creating services that do not give a single service provider complete control over a user’s identity and data (box 4.5).

There remains significant ambiguity about social and corporate responsibility relating to personal data (e.g. shopping habits, location, information accessed and so on). Not surprisingly, many observers are calling for a shift from self-regulatory mechanisms and a mere awareness of ethical principles to concrete and tangible legal measures. If corporate responsibility is to be expanded to include issues such as information privacy—an expansion that is wholly desirable—there remains much work to be done in order to identify mechanisms for its elaboration, application and enforcement.

4.2.4 Current solutions for enhancing privacy

The rise of PETs

Though much has been done since the 1970s for developing legal principles and provisions for the

Box 4.5: Passport to privacy?

Microsoft's Passport platform

Microsoft launched Passport as its "platform service" in 1999, providing an easy single sign-on mechanism for an individual's everyday online tasks, including access to e-mail (hotmail) and other online content.

To merchants and other partners, it promoted the service as a convenient and safe means of determining whether individuals browsing a site were who they claimed to be. Passport operates on a "federation" model, which is meant to allow other authentication vendors to create systems that interoperate with it.

However, in order to use Passport, users are prompted to enter all kinds of information, that are not wholly necessary for the purpose of its Passport service, e.g. full name, e-mail, sex, address, postal code, occupation and income. And since Passport includes a wallet system that speeds shoppers' checkout at designated sites, Microsoft can also maintain encrypted credit card information. Given the need for users to accurately represent themselves at payment sites, this mechanism ensures that users are not able to lie about who they are or where they live (lest a book is sent to a wrong address). The system therefore excludes the possibility of anonymity online and goes against the principle that only a minimum of a user's personal information is to be disclosed. It is also impossible to establish two different identities for two different contexts, as users can only be logged into one passport at a time.

Users initializing Windows XP are actively encouraged to create a passport account. Microsoft maintains most of the personal data, as most of the sites that participate with Passport are owned by Microsoft.

Passport, of course, only works if a user enables cookies allowing the tracking of their surfing behaviour. If cookies are disabled, users receive the all-too-familiar message: "Your browser is currently set to block cookies. Your browser must allow cookies before you can use the Passport Network."

In order to address some of these criticisms and the security failures of Passport, Microsoft has been phasing out Passport to make room for its new identity metasystem, known as "InfoCard".

Image source: flickr.com (ahhyeah)

Sources: Wired News, internetnews.com, D. Boyd (MIT Media Lab), Microsoft

protection of privacy, many argue that legislating for a digital world is essential but that it is as yet insufficient, and especially so in the absence of the necessary technical measures deployed in this area, both at the network and application layers. This has led to the growth of a number of so-called privacy-enhancing technologies (PETs) with the aim of giving users greater control over their personal data. These can be thought of as falling into three categories:[33]

- Proxy: protecting privacy through proxy is the most common approach to PETs. It prevents the receiver of a message from identifying a sender, e.g. it may remove the sender's information from the header of an e-mail before forwarding it. The main disadvantage of this system is that the anonymity is uni-directional, that is to say the perpetrators of harassing or harmful messages can remain anonymous. Furthermore, the solution is onerous, as all communications need to be mediated via a central hub.
- Informed consent: protecting privacy through informed consent includes the popular

Platform for Privacy Preferences (P3P). P3P is an open standard that a given website can use to describe how it uses personal data collected during any session: this is done through a set of multiple choice answers which are made available in a machine-readable format. P3P-enabled browsers can then interpret this description, providing users a way of making decisions about how they use the site by reference to their own set of "privacy preferences". Of course, the use of P3P is dependent on the availability and willingness of sites and service providers to share information about their privacy policies[34]. These privacy policies can also be certified by trusted third parties (e.g. TRUSTe). Although this encourages users to seek out companies with better privacy protection, there may not always be alternate services available, resulting in a lack of choice for users. If the number of such sites is to be reduced, P3P will certainly need the support of legislative measures.

- Untraceability: protecting privacy through the absence of traceability (i.e. through "untraceability") is yet another category of PETs. Not being able to link persons to their representations and expressions of identity online lies at the heart of fundamental rights such as the freedom of expression. The Freenet Project[35] falls into this category. This project, having begun as part of a research project at the University of Edinburgh in 1999, had as its main objectives, *inter alia*: to incorporate anonymity for producers and receivers of information, to create dynamic routing, and to decentralize network functions. More specifically, Freenet eliminates the link between a document's origin and its place of storage. One of the main criticisms of the project is that though it is designed to protect free speech, it has the undesirable consequence of stifling measures to curb the free circulation of material. Thus, Freenet seems to question the very need for protecting intellectual property rights in a digital world.

Cryptography for enhanced security

In addition to the privacy-enhancing systems as described above, improvements in cryptography have been contributing to the growing security of data. Although privacy and security are often related, there is an important difference: security refers primarily to the ability to protect certain information from unauthorized access by third parties, whereas privacy refers to the ability to keep that information private: a system can be secure without necessary being private[36]. Cryptography does not ensure the absolute protection of privacy, but the denial of it to unauthorized parties. As such, it plays an important role in authentication, i.e. checking the identification of those seeking access, but cannot guarantee that privacy is protected.

Cryptography is not a new concept: literally, it means "secret writing". Secret codes (or ciphers) have been in use for centuries, and cryptography has a long tradition in religious writing. Scholars argue that Egyptian Hieroglyphs themselves (used in ancient documents or monuments) are actually early examples of cryptography[37]. Today, information flowing through and stored by the computer is an increasingly rich field for the application of cryptography. In the digital world, most cryptography is based on the use of keys. A popular example is Pretty Good Privacy (PGP)[38], a program which can be downloaded by users to encrypt and decrypt e-mail messages. SSL (Secure Socket Layer) and TSL (Transport Layer Security), communication protocols in daily use for hiding sensitive information (like credit card details online) are also based on cryptography.

Due to its ability to conceal information from those unauthorized to view it, cryptography can be a useful support mechanism for digital identities. It is seen as a core component of a coherent and secure identity management scheme. It may be useful at this stage to outline in brief some of the basic principles behind cryptography, and in particular the most common form of cryptography in use today: public key encryption.

There are two forms of cryptography (figure 4.2): symmetric (or private key cryptography) and asymmetric (public key cryptography). Symmetric encryption is the less complex form of key-based cryptography. It uses the same key to encrypt and to decrypt messages, and parties are required to ensure that the key remains private. A simple example of a private key is a password, e.g. an alphanumeric code used to open a document. The main disadvantages of symmetric encryption is that it is difficult to ensure that the private key stays private, and anyone who intercepts the key can later have access to all messages encrypted with that key, without the knowledge of the owner. Moreover, this form of encryption can be burdensome and does not scale very effectively (imagine all the passwords and private keys that would need to be in circulation). The second form of encryption is asymmetric. It differs from the symmetric form in that it uses two separate keys: one public and one private. Information encrypted by the public key can be decrypted by a private key. The main disadvantage of this system is that encryption and decryption can be very slow, given the increased complexity of the system.

The basics of public key cryptography were first set out in a paper by W. Diffie and M. Hellman in 1976[39], and are the foundation of PKI or public key infrastructure. In public key encryption, symmetric keys (that are encrypted by a public key) encrypt the data. Public key and symmetric key cryptography are complementary. A public key infrastructure refers to the entire set of processes, technologies and policies that aim to ensure secure online transaction environment. In PKI, the use of keys is complemented by the use of "digital certificates", which separate the signing and lookup of identity by allowing a certification authority (CA) to bind a name to a key through the use of a "digital signature" and then store the resulting certificate in a database[40]. The use of a CA is central to PKI, and introduces an added level of security.

Today, PKI is one of the main online tools for trusted transactions, but also for ensuring that new identity mechanisms such as biometric passports are secure[41]. But it does suffer from a number of shortcomings. For instance, it does not address the problem of linking a digital identity with a network, an e-mail, an account or a role. Moreover, its digital certifications do not provide sufficient information for authorization, e.g. access permissions for whom and in what context. Though it is one of the most popular forms of security online, it is not universally deployed and does not offer a uniform security and identity platform.

Life beyond PETs

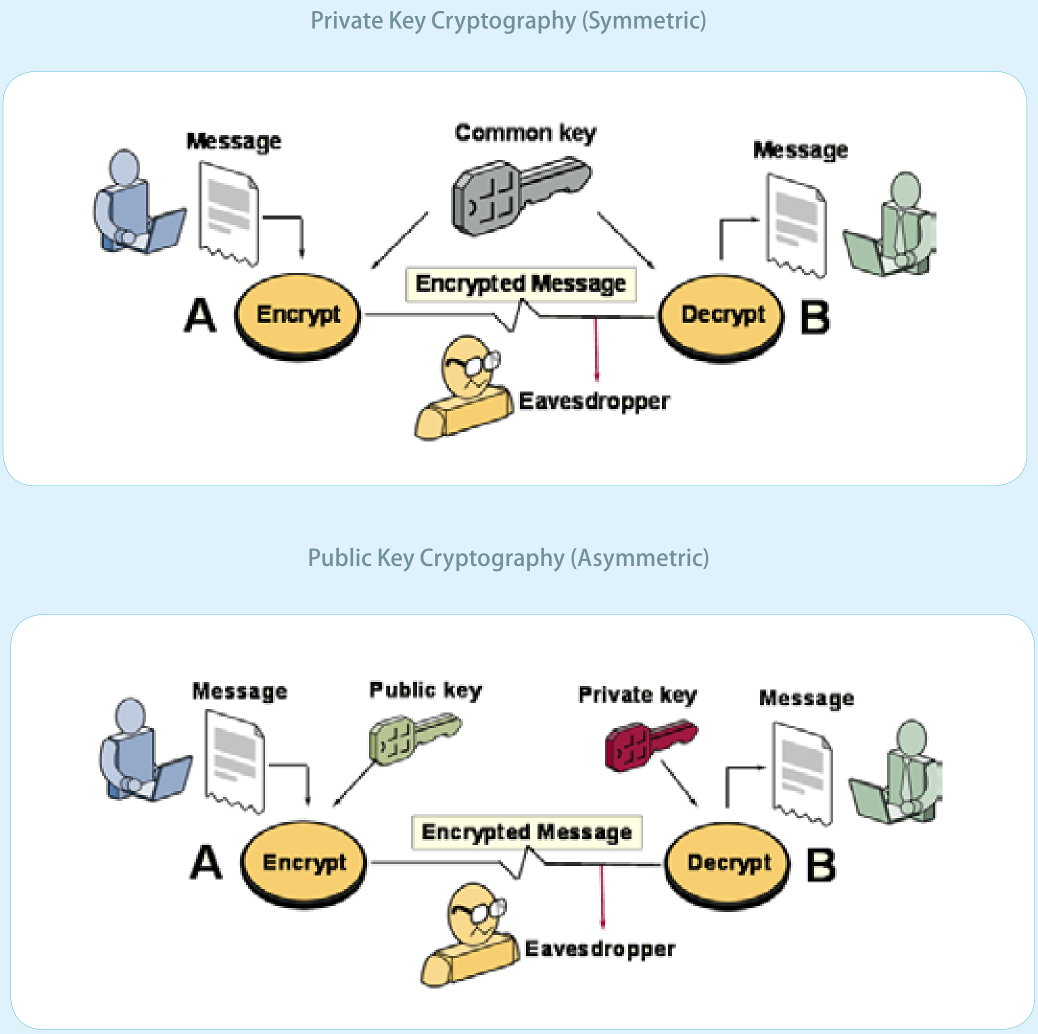
The main reason that the use of PETs for the provision of privacy has been limited in the digital world is that the market for privacy is still relatively small. Besides, most consumers find that the available systems are too complex or burdensome to apply properly. Others lack information and awareness relating to the possibility of privacy violations. Furthermore, there is a "significant disconnect between action and negative effect, but connection between action and positive effect"[42]. When access to information is required, gratification is instantaneous (e.g. if you accept cookies). On the other hand, the tracking and compiling of information about a user can take several months or more, and so it does not affect a user consciously in the short term. In this respect, tools for enhancing privacy should be made part and parcel of the digital world, and not just a rag-tag assortment of software left to the user to use or not use. Indeed, a consistent and coherent digital identity management framework should contain the necessary mechanisms for protecting user privacy. One of the main developments in this area is the emergence of federated identity, discussed in section 4.3 below.

4.3 Managing identity in a digital world

From the foregoing considerations, it emerges that the notion of identity is complex. It incorporates not only philosophical considerations but also legal and practical ones. Identity is what makes individuals the same today as they were yesterday (sameness), but it is also what makes them different from one another (uniqueness). Underlying identity is the distinction between the private and the public spheres of human existence, and as such identity and privacy are forcibly linked[43]. In practical terms, identity can include parameters such as a social security number, a date of birth, a job title, a bank account or a credit card number. And some of these parameters are used both online and offline.

As the boundary between the private and the public in the digital age becomes increasingly blurred, the creation and maintenance of secure identities online has emerged as an important priority for businesses

Figure 4.2: Have you got the keys or have I?
Symmetric versus asymmetric key cryptography



Private Key Cryptography (Symmetric)

Public Key Cryptography (Asymmetric)

Source: Verisign

and consumers alike. Governments, too, are looking for ways to effectively streamline their procedures, offer e-government services, and reduce criminal activity. The confirmation (or in technical terms, authentication) of identity in the online world is much more difficult than it is in the everyday "real world", and comes with its own set of challenges. As such, there is a progressively important role to be played by digital systems that can simply and accurately identify, to the extent required, persons, machines or even things[44], while minimizing the risk of access by unauthorized third parties. This goes beyond assuring the security of networks or of transactions (e.g. through PKI or SSL), to developing a coherent system for managing identity online.

The next sections examine further the rationale behind digital identity management, and outline its key principles. After considering the relevant vulnerabilities of the digital age, they explore design principles for maximizing trust and predictability online.

4.2.1 The changing nature of identity

In the Merriam-Webster dictionary, identity is defined as follows:

identity:

1. Sameness:

- sameness of essential or generic character in different instances
- sameness in all that constitutes the objective reality of a thing
- the condition of being the same with something described or asserted

2. Individuality:

- the distinguishing character or personality of an individual
- the relation established by psychological identification

The reference to sameness in this definition points to the continuity and permanence of the identity of the human self. The notions of uniqueness and individuality contained therein are what differentiates one human being from another, and are the basis of self-awareness, social interaction and decision-making.

Though these fundamental concepts have remained the same over time, changes in economic and social structures have affected the determination and perception of identity. In the past (pre-modern times), human identity was defined by geography, community, and family relationships. If an individual was born into a well-known and rich family in London, that is typically the environment in which he or she would remain. If an individual began life in a poor remote community in India, they would typically not be able to change their life pattern or economic status over time. One's geophysical space and one's place in society were inextricably linked, the possibility of freedom of movement being severely limited. With modern times there arrived a greater choice for participation in different social circles, and the possibility of social and economic mobility.

In today's (post-modern) world, the individual has even more choices, covering even more aspects of life, and is at the centre of an increasing number of social networks (that are often quite distinct)[45]. Sociologists have been arguing for some time now that human relationships are increasingly short-term and fleeting. The widespread and constant availability of information and communications in the surrounding environment have made constant change and unpredictability the rule. Change in the perception of identity is a direct consequence of this phenomenon.

Today, most people carry some form of identification on them at all times, but this practice is relatively recent in human history. In the past, the declaration of an individual's name, sometimes accompanied by the name of their city or village, was sufficient to prove their identity. This is no longer the case. Further, the notion of identity today can refer not only to humans, but also to animals, machines, and other objects or resources. A machine may have an identity which would allow it to access certain information at certain times, or be employed by some individuals, to the exclusion of specified others. This possibility complicates an already complex issue.

4.3.2 Vulnerabilities and rationale

The consumer perspective

The internet was developed without a coherent mechanism for determining to whom and to what a user might be connecting. Like the network itself, which was founded on ad-hoc principles of information dissemination, online identities, too, exist in the form of a "patchwork of one-offs"[46]. Although most sites require some form of identification or registration, many of these are fairly basic (e.g. requiring a simple password and username) and do not communicate any form of centralized registration system on other sites. Even e-commerce or payment sites, which typically have at least one identity mechanism in common

Box 4.6: Stolen selves

The growing problem of identity theft

A personal identity is an asset that everybody owns but most people neglect. However, if one loses it, one does risk losing everything.

People whose identities have been stolen can spend months or even years – and large sums of money – cleaning up the mess that thieves have made of a good name and credit record. In the meantime, victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they did not commit. Humiliation, anger, and frustration are among the feelings victims experience as they navigate the process of rescuing their identity.

Identity theft, while not new, has quickly gained the attention of consumers, businesses, and legislators around the world. As internet use continues to grow rapidly, thieves have found it more direct channel for identity theft, posing a considerable threat to consumers and to the expansion of electronic commerce. Once thieves gain access to sensitive identity information, they can change profile information and preferences, and make or change transactions (e.g. move sums of money). New reports of identity theft or misuse seem to appear every week, and from every corner of the globe.

A September 2003 survey by the United States' Federal Trade Commission (FTC) estimated that 10 million US citizens have been victims of one kind of identity fraud or another. The survey found that:

- Only 15% of victims find out about the theft due to a proactive action taken by a business;
- The average time spent by victims resolving the problem is about 600 hours;
- 73% of respondents indicated the crime involved the thief acquiring a credit card;
- The emotional impact is similar to that of victims of violent crime.

The FTC has carried out a series of campaigns to educate the public on the importance of self-identity and how to prevent it from being abused. FTC is also urging citizens to report to the authorities immediately after discovering that their identities have been stolen.

In the United Kingdom, personal data is protected by the country's Data Protection Act which covers all personal data that an organisation may hold, including names, birthday and anniversary dates, addresses and telephone numbers. The Home Office has now set up a website explaining the danger of identity fraud and provides details on how UK residents can prevent or report cases of identity fraud.

Image source: University of Exeter

Sources: U.S. Federal Trade Commission website, "Fighting Back Against Identity Theft" at **www.ftc.gov**; United Kingdom Home Office Identity Fraud Steering Committee at **www.identitytheft.org.uk**

(i.e. credit card payments systems or systems like Paypal), offer no less of a patchwork. Users may still use different passwords for different sites. For instance, a user may enter the same credit card number to pay for travel on easyjet.com as to buy a book on Amazon.com, but with different usernames and passwords in each case. Users are often obliged to form or select usernames and passwords that are mnemonically difficult to remember; their username of choice being already in use. This has led to an every-increasing burden of usernames and passwords for the user to carry, each associated with different websites. This is in addition to banking (PIN) numbers and such that are already used in the offline world. Many users feel obliged to resort to unsafe practices, like using the same password for different services. This may cause security breaches, and leave them vulnerable to the machinations of identity thieves ever increasing in number and inventiveness (box 4.6). Thus, the lack of coordination in identification systems is a source of growing inconvenience to users and needs to be addressed rapidly.

Today, consumer privacy has become an equally important concern. A dramatic recent example has been the well-publicized boycott of Benetton following the announcement of their plans to integrate radio-frequency identification tags (RFID) in some products. Privacy violations are taking place without the knowledge of consumers, and in some cases, consumers are left with little choice if they are to adopt new services. From an ethical perspective, an environment in which citizens are obliged to disclose more and more personal data, simply in exchange for convenience, or for lower prices, must be discouraged and eventually eliminated. For example, on the internet today, most are obliged (usually by default) to accept cookies that track online behaviour—a phenomenon that just a few years ago was considered to be a serious invasion of privacy. Many sites are now effectively unusable to those who do not wish to be tracked. Although privacy is a concept that is under constant evaluation and definition, it must always remain an important consideration. The issue of privacy is magnified today because citizens' actions and interactions are perceived and recorded in greater and growing detail.

Identity management systems can empower users to regulate their activities online, and serve to instil trust in information networks that are seen to be increasingly vulnerable to misuse and attack. A clear and transparent approach to identity management will mean that users can interact with each other in a more meaningful and confident manner, i.e. to benefit from online opportunities without the fear of being monitored or intercepted. User-centric identity management will enable users to create their own impressions and representations in the digital world, rather than have these created for them through mechanisms that lie outside their control. Often, representations of identity are formed through historical data interpreted out of context which may thus result in a negative repercussion on the reputation of an identity. Without the ability to control identity (and personal information) in multiple and often disparate online contexts, the only option left for some users may indeed be absolute anonymity.[47] This may not necessarily be desirable for certain services and may affect the possibility of participating fully in a digital life.

The business perspective

For businesses, identity management can confer a number of benefits. It can, for instance, reduce the complexity of multiple users managing, entering and using their premises. For instance, physical or electronic e-mail aliases can continue to exist even after an employee's departure, due to time constraints and systems not initially designed to deal with identity management (e.g. the inability to delete identity parameters like e-mail addresses securely without compromising overall system integrity). With the availability of digital identity systems, businesses might better manage the growing array of web-based applications through a single sign-on mechanism. This would also facilitate the management of changing roles (and permissions) of users in the organization, be they employees, machines or resources (e.g. computer systems, parking garages or board rooms). More importantly, a good identity management system can protect an enterprise from unauthorized access to corporate information. Finally, for ICT service providers, digital identity management can help promote new value-added services (such as location-based services) that may otherwise be a hard-sell for consumers concerned about invasions of privacy.

Important limitations

As mentioned earlier, today's systems are insufficiently equipped to deal with the rising number of interactions occurring in the digital space. Although it is currently possible to identify machines (e.g. servers) in most cases, it is not as easy to accurately identify human parties in a virtual transaction. The inconvenience of having to register multiple accounts and passwords has already been mentioned. There are also many different types of login or registration systems in existence, and their functionality varies greatly: some allow the deletion of access permissions entirely, and others do not allow passwords to be easily reset. Moreover, current login systems are fairly primitive and typically rely on browser technologies. Identities cannot be effectively transferred from one account or context to another, even if a user would wish to create such a "meta-identity". And in spite of the continuing availability of information, identities may expire after a length of time. This may not be considered serious in some instances (perusal of online newspapers), but in other cases, the consequences may be grave (such as the deletion of user accounts after a fixed period of time, e.g. Hotmail).

Yet another source of concern is that the current network infrastructure suffers from security problems, due to persistent difficulties, with viruses, worms, and spyware. Serious information leaks have been known to occur, compromising entire data systems (box 4.7). Security and trust in critical network infrastructure is an indispensable requirement, and must be addressed in parallel with data protection initiatives. Thus far, an approach favoured by governments and industry has been to secure the affected network only after a security violation or leak has occurred. This amounts to locking the stable doors after the horses have fled. A more astute policy would require security to be built into technical design, thus preferring prevention over cure.

Human identity receives protection from many sources – constitutional and other legislation, international conventions and protocols and so on. Freedom of speech and self-expression, freedom of movement, freedom of association are all examples of efforts to protect identity. Lawrence Lessig cites four different means by which behaviour can be controlled: the law, the market, the architecture and social norms[48]. In essence, his contention is that in the online world, these forces are not operating effectively. Due to the complex architecture of the internet, social norms are often ignored, while the market capitalizes on the many facilities that the internet affords. At the same time, the legal community is not fully recognizing that the digital space may require an alternative legal approach. It is true that the legal system may well deal with issues relating to acceptable usage and architecture (as in the case of Napster), but its approach thus

Box 4.7: Digital information leaks

The Lexis-Nexis fiasco

In 2005, LexisNexis, a provider of information and services solutions, revealed that an intrusion into their databases had compromised the personal information of about 310'000 users. This was not the first digital information leak to be reported in the United States – in 2003 a security flaw at the florist's website 'ftd.com' left individual's personal information open for harvesting – it exposed the names, addresses, phone numbers and billing records of customers. Elsewhere, the personal and confidential information on 185'000 current and former patients of the San Jose Medical Group was lost, and the details of more than 1.4 million credit cards were obtained from transactions made by customers of DSW Shoe Warehouse.

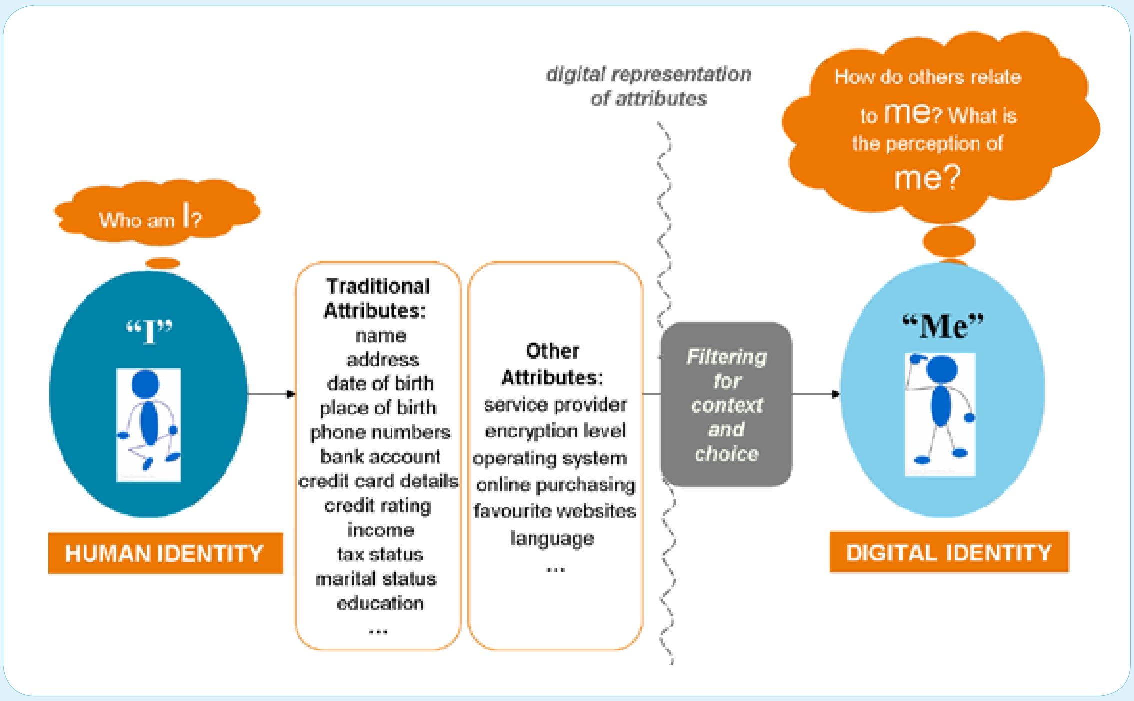
It seems that information leaks have become a real risk in today's digital age. More and more organisations are converting large amounts of information to digital formats. This may increase an organisation's productivity, but it also increases the risk of exposure to leaks and unauthorized access. In tandem, the growth of technological channels over which information can move – for example instant messaging systems and e-mail – means that the ability of an organisation to control its data is reduced. The vast scale of the LexisNexis leak forced the United States Congress to respond aggressively: Senator Dianne Feinstein introduced a bill that would require that consumers to be notified of certain types of security breaches. Given the increasing tendency towards the storage, use and exchange of information in digital format, coupled with the ubiquity of distribution media, it is likely that regulators and policy-makers will seek to enhance accountability and transparency among corporations that collect personal information on a more regular basis.

Image Source: flickr.com (jenica26)

Source: news.com, "LexisNexis flap draws outcry from Congress", April 2005 and "FTD.com hole leaks personal information", Feb 2003; Business Management, "Plugging information leaks", 2006

Figure 4.3: From "I" to "Me"

From human identity to digital identity



Source: ITU

far has focused almost entirely on protecting corporate interests and copyright. In other words, the legal system has not focused sufficiently on individual interests and the underlying architecture corresponding to them. Lessig also points to the key role of technology designers in giving users more control over their existence in the digital world and in promoting self-regulation. Legal structures and market forces alone are not equipped to address the issue of digital management, and certainly not at the requisite pace.

For this reason, there have been calls from many quarters for technology designers to begin focusing on the creation of a single and predictable digital identity management system, with due support from the law and the market.

4.3.3 Designing for trust and predictability

This section outlines the main definitions and principles underlying digital identity management. It focuses on the need for predictable online environments, and summarizes some of the current thinking in this area.

Definitions and key concepts

Digital identity refers to the online representation of identity. More specifically, it refers to the set of claims (in their digital form) made about a user or another digital subject.

In this context, a "digital subject" can refer to a person, a group, a software programme or another entity. Typically, a subject might make a series of claims when trying to access a particular resource (e.g. information, goods, or monetary value). The Oxford English Dictionary defines "claim" as "a statement that something is the case". In the context of identity management, one can take this definition further as follows: a claim is "an assertion of the truth of something, typically one which is disputed or in doubt"[49]. The extension of the original definition to that which is "in doubt" refers to the characteristics of a distributed world like the internet. As networks become increasingly open to participation by many different actors or subjects, these claims need be evaluated and verified by those who need to rely on them.

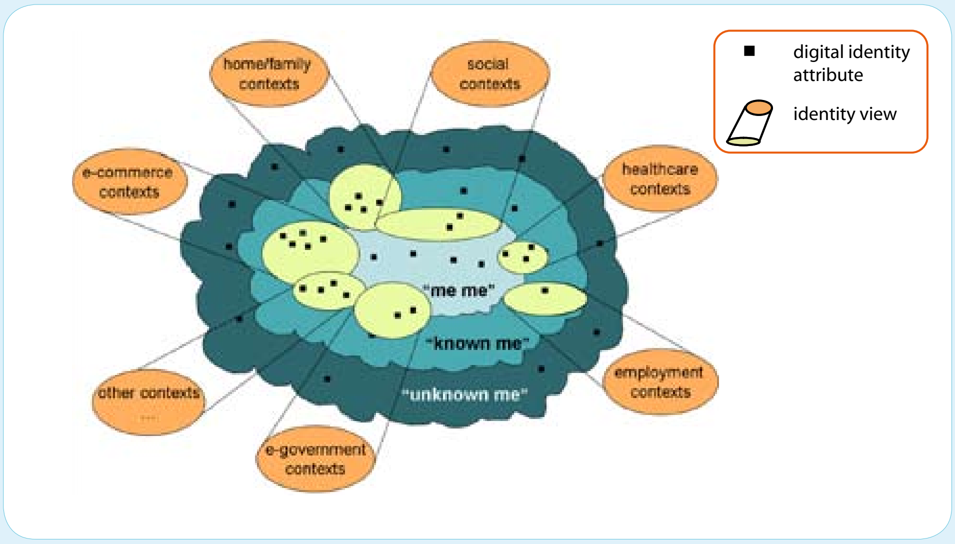
Digital claims can be made up of sets of data, also known as attributes or identifiers. Attributes can include a name, a date of birth, a bank balance, but also past purchasing behaviour, medical or employment records. Attributes can also include preferences, such as currency used, preferred language or seating for travel. Some information is static (such as a date of birth) and other information is dynamic (such as employer's name or dietary preferences). Attributes also ensure that the distinction between the public and private spheres of individual lives remains intact. As figure 4.3 illustrates, the core of human identity is accessible only by the individual self, wherein lies the values of freedom, self-awareness and self-reflection (i.e. the "i" of identity[50]). The series of attributes that are accessible by external parties (i.e. the "me" of identity) through information and communication networks must not compromise these essential values. The "me" that is known to the outside world is a representation of characteristics that are necessary to conduct daily life within a societal and/or corporate structure. There can be many different representations of the "me" depending on the nature of the interaction. In the information age, these representations are collectively known as "digital identity".

In order to establish trust between parties in the digital world, a subset of digital identity attributes needs to be communicated. Digital identities exist in specific contexts and the contextual relationship between them is crucial to managing transactions and interactions. The context will determine which subset of attributes is required, or which "partial identity" will establish enough trust for the transaction to go forward. Alternatively, individuals may also wish to decide which subset to use in a particular context. As such, the "me" that is perceived by the outside world is either known or unknown depending on context (figure 4.4).

Let us consider the case of Alice who is using partial identities to manage her interactions with many different parties, including her boyfriend Bob, her health care provider, her travel agency and various government services (figure 4.5). With her health care provider, she may share her name, address, blood group and health status. With her employer, she might share her insurance information, her name and address, and her employment records, but not her health status. As it is still early days with

Figure 4.4: Contextual identities

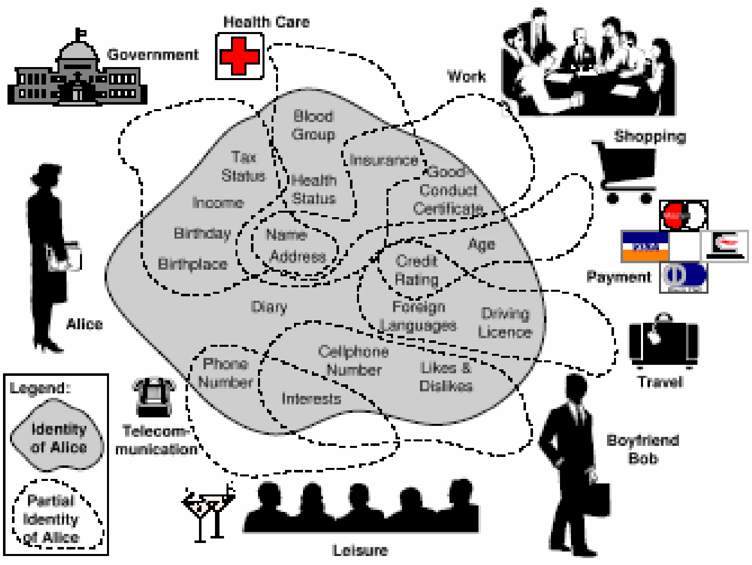
The known me and the unknown me in a digital context



Source: ITU, adapted from J. de Clercq & J. Rouault, "An introduction to identity management", Hewlett Packard, Dev Resources, June 2004

Figure 4.5. Identity as a subset of attributes

The many partial identities of Alice



Source: S. Clauβ & M. Köhntopp, "Identity Management and its support for multilateral security", Computer Networks 37 (2001), 205-219

her boyfriend Bob, she may share her mobile phone number, but not her fixed line number, which she might share with other friends.

In order to use these partial identities to conduct the various aspects of her daily life, Alice needs to justify her access to various resources. As such, she must present "credentials" to prove that she has the necessary identity attributes for a specific task in a specific context. These credentials establish trust with the different parties. Once Alice communicates her credentials to a "security authority" (which might also be a third-party "certification authority" or CA), the authority "authenticates" the credentials, through mechanisms such as a username or a password. Authentication methods can be simple or complex, depending on the level of risk associated with the particular resource (e.g. they may or may not use mechanisms such as PKI). For instance, a simple password might be sufficient to access a news article online, but more stringent authentication mechanisms may be called for in the case of financial transfers, e.g. name, address, credit card number, credit rating, security codes etc. Once credentials are authenticated, a security authority would forward them to a separate policy decision point (PDP), which would use a pre-determined security policy to assess the entitlements and permissions associated with the subject's identity and the particular resource in question.

Most of the notions relating to identity already exist in the physical world. A driver's license, for example, contains the necessary credentials to perform specific tasks, whether it is for driving a car or towing a trailer. Such a license can also provide the required attributes for buying alcohol. The process of buying alcohol is a good example of how identity is managed in the physical world—in this case by "Alex":[51]

1 Let us say that Alex wishes to buy vodka coolers for a college party, i.e. to perform an action on a "resource", and to do so, presents his driver's license (credential) to the clerk at a liquor store (security authority);

2 The clerk carefully examines Alex's driver's license to see if it looks real (validation);

3 The clerk then looks at the picture (biometric device) on the license and compares it to Alex's physical appearance. She asks Alex to take

his glasses and hat off to make him look as he appears in the picture;

4 The clerk satisfies herself that the picture in Alex's license resembles him (authentication);

5 If the clerk deems the license to be authentic, she verifies (verification) Alex's age (attribute);

6 The clerk then verifies whether Alex's age meets the minimum age requirements to purchase alcohol according to the national legislation (security policy);

7 The clerk finally allows a happy Alex to purchase the vodka coolers with some loose change (authorisation).

The privacy concerns in this scenario refer to the protection of attributes and preferences associated with Alex's identity. He is only required to produce proof of age to purchase the alcohol. He is not required to disclose data such as the name of his college or the address of his employer. Moreover, as Alex paid in cash, neither his name, age nor license number were recorded. As such, Alex's early predilection for vodka will not be automatically communicated to his biology professor or to his parents. The privacy of his actions in this case is assured because the data in question is: a) minimal: only a driver's license was presented, b) temporary: the license was only examined briefly by the store clerk, and c) un-linkable: it cannot be linked with Alex's other attributes (parents' name and address or professor's contact details). These same considerations should apply to the online world, and indeed many proposed digital identity management schemes have focused on principles such as "un-linkability" and data minimisation.

Design principles: from anonymity to pseudonymity

The process of digital identity management consists of three main phases:[52].

- **Verification** refers to the mechanisms which establish or create an identity, and which can later be used to make claims. These mechanisms can be very simple, such as choosing a username which is not yet in use (e.g. a username for a web-based e-mail account) or stringent, such as a photo or a personal visit.
- **Authentication** is the process of establishing trust in a claimed identity. As discussed above, authentication serves to prove that a transacting party is authentic (that they are who they say they are). Authentication for an individual user can be either: something they own (e.g. a token or RFID tag), something they know (e.g. a password), or something they possess inalienably (e.g. iris recognition or fingerprints). Authentication can be very minimal in some cases (e.g. requiring only the authentication of a user's age category), and in others it may be more stringent.
- Finally, **revocation** is the process of rescinding an identity an individual has been granted. This process should ensure that the revocation is properly recorded and that the identity in question is no longer in use (e.g. when an employee leaves a company, for instance, or in the case of death). This revocation process should also ensure that the identity can not be stolen.

Digital identity management includes a number of different technologies that administer verification, authentication and revocation (such as electronic signatures, password management and synchronisation, PKI, directory services, to name a few). It is important to note, however, that this is a wide subject, encompassing not only technological elements, but also broad design principles and context-driven security policy. In particular, a satisfactory identity management system must accommodate the full range of options stretching from anonymity to full "identifiability". In some cases, disclosure of identity may not be required for parties to transact, e.g. in the case of browsing web pages or buying goods through an electronic money scheme. In other cases, a proof of identity issued by a trusted third party may be needed, e.g. in the case of purchase of high-value goods like property. In yet other situations, varying levels of accountability and authentication may be required, depending on the sensitivity of the transaction. One of the measures that has been identified as essential in this regard is the use of pseudonyms (also known as "nyms"). These make possible the use of partial identities, and can thus cover the entire range from anonymity to identifiability. Pseudonyms allow users to take on different identities depending on the specific context and parties involved. The use of a pseudonym is effective only when it cannot be linked with its holder (i.e. holder anonymity) or with other pseudonyms a holder may have. Nonetheless, when necessary, the holder of the pseudonym can be revealed and as such, he/she is liable and accountable for actions taken under that pseudonym.

Discussions regarding the principles upon which digital identity management systems should be predicated are ongoing both nationally and internationally. Not only are security experts evaluating the need for a coherent identity scheme that would stimulate online interactions, while protecting data and alleviating privacy concerns, but so, too are, lawyers, corporate strategists, and economists. Governments are taking a greater interest in this area, particularly in an effort to thwart illicit interactions and identity theft. The European Commission's approach to this question was first expounded in its PRIME (Privacy and Identity Management for Europe) project. The objective of the project is to give "individuals sovereignty over their personal data", and to "enable individuals to negotiate with service providers the disclosure of personal data and conditions defined by their preferences and privacy policy"[53]. This project calls into play some fundamental principles: user support, openness, consent, accuracy and completeness, data minimisation, notification, security, and access to law enforcement (box 4.8).

Forward with federation

As previously mentioned, identity management systems online have thus far been predominantly deployed by a single entity for a fixed user community, or represent walled garden systems, in which a number of service providers are grouped together for the purposes of secure exchanges and transactions (e.g. business-to-business commerce). Spurred by the resultant fragmentation of online identity, one of the newest trends in digital identity management is the federated system. A federated identity system is one in which no single entity operates the system, and one which creates an environment in which users can log on through a central identity provider and use the state of being authenticated to access resources across numerous domains. The main aim of federated identity systems is to facilitate the management of attributes for different applications and different contexts, i.e. partial identities (discussed above). An open federated model means that network identity and user information is available in various locations, and as such there is no single point of failure and users can be identified by different and disparate systems. For a federated identity system to work, there are three main requirements:

- standard formats for representing identity information;
- standard, secure and privacy-enabled protocols for the exchange of information between application components;
- the possibility of setting up trust relationships between entities that might share identity information[54].

The fact that a person can use a bank card at many different ATMs (automatic teller machines) around the world is due to the federated nature of that identity system. It allows travellers to retrieve cash at many cash points by simply entering a plastic card and a numeric password (personal identification number or PIN). This system works because banks have agreed to use common standards for authentication, and have secure and trusted systems in place to transfer information. Another good example of a federated identity system is the use of a national passport when travelling. In the online world, federated systems similarly aim to share the identities of users across multiple (often disparate) trusted domains[55]. In enabling effective access control and the secure transmission of personal data across domains, the occurrence and impact of identity fraud are minimized. For users, the key advantage is that the consolidation of identities improves the online experience, making it both simpler and more secure.

There are two main players in a federated identity scheme: a service provider and an identity provider (Box 4.9). These may also be part of the same organization. In a typical system, a user would have to register with an identity provider, usually face-to-face[56]. Individuals can then add additional attributes to their identities, as well as introduce the corresponding policies for the release of these attributes. When a user interacts with a service

Box 4.8: Designing for identity in Europe

European Commission PRIME Project's digital identity management system design principles

Although the European Union and its Member States have enacted legal frameworks to facilitate the exchange of personal data, a fast-changing digital world is widening the gap between rules and regulations on the one hand, and practical realities of online interactions, on the other. The PRIME (Privacy and Identity Management for Europe) project, sponsored by the European Commission and the Swiss Government, aims to restore the dignity of an individual's private sphere in an increasingly online world. As such, it looks to technologies to provide a comprehensive approach to managing privacy and identity.

Its main principles are elaborated as follows:

- Design must start from maximum privacy
- Explicit privacy governs system usage
- Privacy rules must be enforced, not just stated
- Privacy enforcement must be trustworthy
- Users need easy and intuitive abstractions of privacy
- Privacy needs an integrated approach
- Privacy must be integrated with applications.

In addition, the PRIME White paper cites a number of important design principles:

- User support during the complete lifetime of the personal data – an integrated view must be given to help users make their choices (thus carefully designed and validated Human-Computer Interface is required)
- Openness with respect to privacy policies and practices, by means of readily available information to individuals by service provider in consider and understandable way
- Consent, based on conscious decision of individual (except where inappropriate)
- Accuracy, completeness and validity of the personal data users and maintained by service providers for explicitly stated legitimate purposes
- Data minimization–Service providers should aim to use the minimal set of personal data required to perform a particular service. Anonymous access should be offered wherever possible with pseudonym access, involving identifiers distinct from and not related to the user's real name
- Notification of the existence, use and disclosure of a user's personal data should be given to all. They should then have the right and ability to assert their privacy rights, such as access to own data and the right of correction of their personal data if necessary
- Security measures appropriate to the sensitivity of the personal information under protection
- Access to law enforcement agencies should be guaranteed on the basis of proper legal safeguards.

Image source: PRIME

Source: PRIME, European Commission

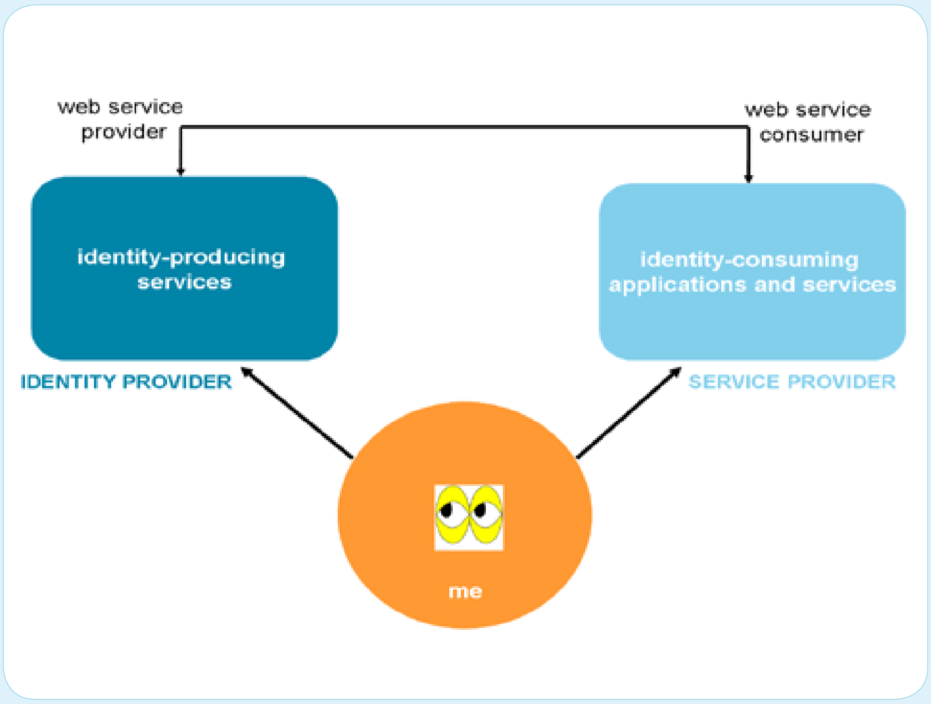
provider, the identity provider is responsible for sending that service provider the relevant user attributes in accordance with the release policies stored in its database. As such, a federated system has four main elements: a single sign-on, the mapping of identifiers, the sharing of attribute profiles, and user management (box 4.10).

Federated systems go a step beyond simple single sign-on (SSO) systems. Where SSO relied on setting up a central server to be accessed by each application, the notion of federation implies that local applications maintain their own data repositories that can respond to queries from both local and remote applications. If local applications encounter non-local users, they can query other federated repositories to authenticate and authorize them, according to their respective privacy and security policies.

Nonetheless, federated systems currently suffer from a number of shortcomings. First of all, registering identity through a face-to-face process may not always be possible, and in some cases can represent an important bottleneck. Second, the relative weakness and strength of identifiers are not taken into account. Third, although there have been a number of efforts to establish federated identity standards, the landscape for federation remains fragmented. The main players are Liberty Alliance[57] and the Organization for the Advancement of Structured Information Standards (OASIS), with the most established standard to date being OASIS's SAML or Security Assertion Markup Language. SAML is based on XML (Extensible Markup Language). Version 1.0 was standardized in November 2002 and it is expected that Version 2.0 (which was approved in March 2005) will go some way in bringing together the various federated identity management standards in use. However, interoperability has not yet been fully addressed between these standards, as well as between different versions of the same standard. Clearly, to ensure a truly consistent and global identity framework across domains and platforms, much more is needed.

Figure 4.6: Identity production and consumption in a federated system

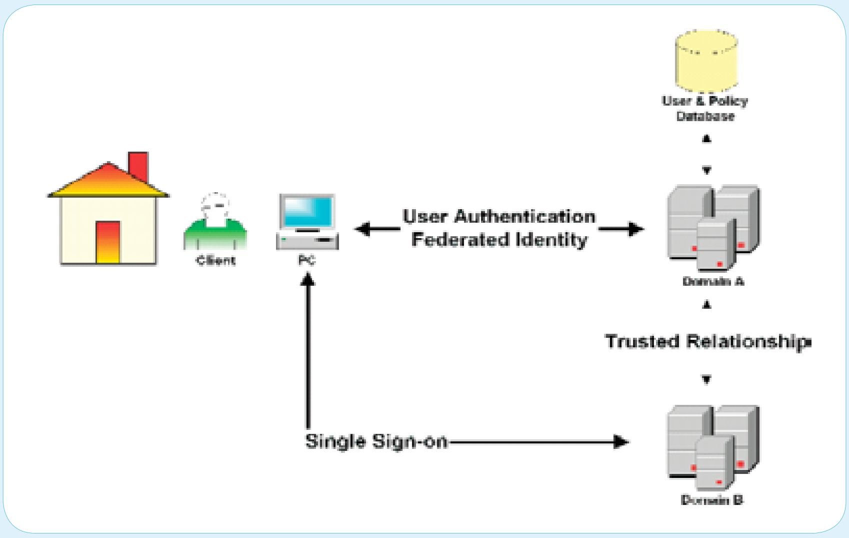
Main players in a federated identity scheme



Source: Adapted from Sun Microsystems and Liberty Alliance

Box 4.9: What's in a federation?

Main concepts underlying federated identity



There are four main concepts underlying federated identity:

1. Single sign-on means that authentication information of a user is communicated across multiple domains. After a user logs in to any one particular domain, that information can be passed on to other trusted domains, without the need for re-authentication.

2. Identifier mapping provides the linkage of different user identifiers for the same user in multiple domains. For example, a user can be "alicedoe" in one domain but "adoe" in another. Both names would then be linked by identifier mapping in a federated system. The user can be accepted in different applications even though the identifiers may be different. This enables the use of pseudonyms and partial identities.

3. Attribute profile sharing means that information about users can be accessed by different domains. Basic information can be retrieved by trusted applications, according to the agreed privacy and security policies.

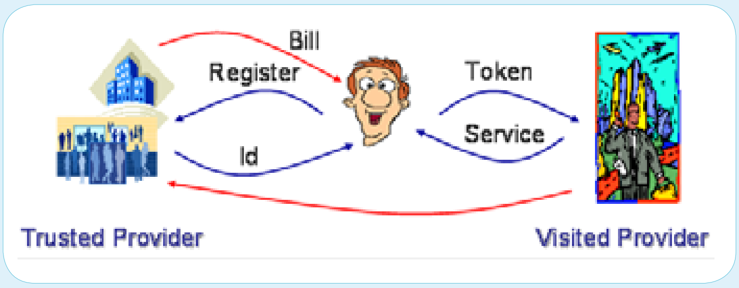
4. User management refers to the creation, modification, provision and deletion of federated identity.

Source: R. Tam, "Federated Identity: A Fairytale or Reality", The ISSA Journal, July 2005

An important step in this direction is the European research project Daidalos ("Designing advanced network Interfaces for the delivery and administration of location independent, optimised personal services"), which has as its main objective the promotion of an end-to-end service in a heterogeneous network environment. The Daidalos project explores how identity can be used across layers: from the core network to web services at the edges–in mobile, fixed or broadcast environments (box 4.11). As such, it builds on existing standards, such as SAML and Liberty Alliance, but aims to create a single solution which can be used regardless of platform. A European project launched in 2003 by Deutsche Telekom and partners like NEC and Lucent, Daidalos has a 50 million Euro budget, and involves 37 partners. More recently, it submitted a proposal to the International Telecommunication Union (ITU) that would incorporate the results of the project in global standardization activities[58]. Discussions are currently ongoing within the ITU-T's standard-setting study groups as to how best to move forward on this important issue.

Box 4.10: Extending identity in a wireless post-3G environment

European Daidalos project gives users "handles" for control



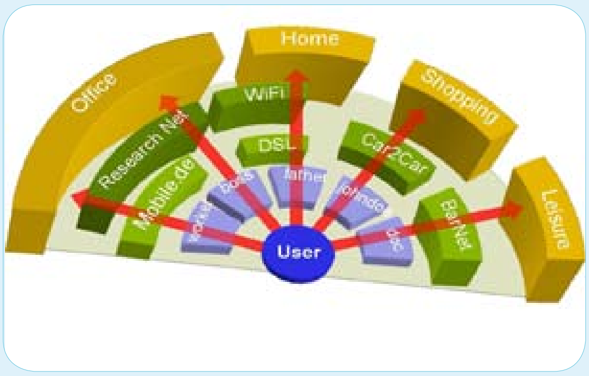
Daidalos is a European Union IST 6th Framework Research Project in the Beyond 3G Area running from November 2003 to December 2008. It has 37 Partners and is led by Deutsche Telekom AG. Its goal is to integrate mobile and broadcast communications to deliver ubiquitous end-to-end services across heterogeneous technologies.

In particular, the project is intended to:

- Give customers a diverse range of personalized services – seamlessly and pervasively supported by the underlying technology ;
- Establish mobility via an open, scalable and seamless integration of complementary heterogeneous network technologies including broadcast, ad-hoc, moving and sensor networks ;
- Empower network and service operators to develop new business activities and provide profitable services in an integrated mobile world.

One of the project's five key Concepts binding various project elements together is the Virtual Identity (VID). Specific aspects of the Daidalos VID concept include:

- Providing a global identity for network, transport, accessing services, content and beyond;
- Represent and link a set of users' contractual rights and duties in terms of authentication, authorization, QoS, etc;
- Allowing users to define context and preferences, thereby simplifying management of these attributes;
- Decoupling the roles of providers of identity, billing and services.



The Daidalos VID concept allows users to build virtual identities that they can associate with specific profiles and activities. The communications system will not be able to identify the person associated with each identity unless lawful disclosure is required, since each identity will be supported by independent communication features, from the lower layers to the higher communication identifiers. Although linkage of activities is still possible across the multiple activities made under the scope of a virtual identity, the same user can carry out completely unlinkable sets of communication activities by using separate virtual identities.

Virtual Identities are built around identifiers that users obtain from trusted providers, which can be used across different levels of access and across providers ranging from network access providers over service providers to content providers. Users may conceal their identities from visited providers and conceal their service usage from their trusted provider.

The Daidalos project aims to complete its Framework and Architecture for Virtual Identities in March 2007. Based on this, prototypes will be developed in 2007 and integrated in 2008.

Source: European Commission Project Daidalos, A. Sarma (NEC)

4.3.4 The road ahead

Though the importance of digital identity mechanisms is finally being recognized, much work remains to be done. Information regarding individual identities is becoming an increasingly valuable commodity, and as a consequence, its protection and management has become a pressing matter.

In this regard, global standardisation efforts and open source initiatives are crucial. No common set of technical standards has thus far emerged, and consequently a wide range of authentication methods remain in use. Moreover, legal and policy considerations require further harmonization at the global level. There is also a need to develop a business case for digital identity management through concerted public-private sector dialogue. This is not only to stimulate development but also to ensure the widest possible take-up among both consumers and businesses.

A number of questions remain to be addressed, but it seems at this time that the notion of federation offers the best model upon which to base identity frameworks in the digital age. In order to ensure the global impact of such a system, dialogue at the international level seems indispensable.

Endnotes of Chapter four

1 Eileen Green, "Technology, leisure and everyday practices", in *Virtual Gender: Leisure, pleasure and consumption*, E. Green and A. Adam (eds), Taylor and Francis, New York, London, 2001, pp. 173-188.

2 Jennie Caroll, John Murphy, "Who am I? I am Me! Identity management in a networked world", 4th International We-B Conference, 24-25 November 2003.

3 The concept of "avatar" originates in Hindu philosophy, in which it commonly refers to the bodily/physical projection (incarnation) of a higher being in the manifested (earthly) world. The literal meaning of the Sanskrit word "avatāra" is "descent", and as such typically implies the deliberate descent into lower (mortal) realms of existence, for a specific objective (i.e. in order to help humankind).

4 This use of avatar in this context is said to have been popularised by Neal Stephenson in his 1992 novel *Snow Crash*.

5 Terry Flew, New Media: An Introduction, Melbourne: Oxford University Press, 2002.

6 See http://us.cyworld.com

7 Lara Srivastava, "Mobile phones and the evolution of social behaviour", *Behaviour & Information Technology*,Vol.24, No.2, March–April 2005,111–129.

8 UMTS Forum, "Social Shaping of UMTS: Preparing the 3G Customer", 2003.

9 For more information about the "skype me" mode, see skype.com (at http://support.skype.com/?_a=knowledgebase&_j=rate&_i=442&type=no).

10 The Cincinnati Post, "Nocturnal life often the norm for young", 13 September 2005, available at http://news.cincypost.com/apps/pbcs.dll/article?AID=/20050913/LIFE/509130330/1005. See also The Register, "Mobile phones disrupt teenagers' sleep", 17 September 2003 (available at www.theregister.co.uk/2003/09/17/mobile_phones_disrupt_teenagers_sleep).

11 Hans Geser, "Sociology of the Mobile Phone", University of Zurich, 2002.

12 Johann Cas," Privacy in Pervasive Computing Environments – A contradiction in terms", *IEEE Technology and Society Magazine*, Spring 2005, pp. 24-33.

13 As the French essayist Michel de Montaigne said in the 16th century of the gap between the private and the public spheres of existence: "A man must keep a little back shop where he can be himself without reserve. In solitude alone can he know true freedom", Michel de Montaigne, Essais, 1588.

14 Felix Stalder, "The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy", *Sociological Research Online*, Vol. 7, no. 2, August 2002.

15 Jurgen Bohn, Vlad Corama, Marc Langheinrich, Friedemann Mattern, Michael Rohs, "Living in a World of Smart Everyday Objects – Social, Economic and Ethical Implications", Human and Ecological Risk Assessment, Vol 10, No. 5, October 2004.

16 ITU, ITU Internet Reports 2005: The Internet of Things (available at www.itu.int/internetofthings).

17 Paddy Nixon et al, "Security, Privacy and Trust Issues in Smart Environments", The Global and Pervasive Computing Group, University of Strathclyde, United Kingdom.

18 Robert W. Lucky, "Everything will be connected to everything else", *Reflections – IEEE Spectrum*, March 1999.

19 Gary T. Marx, "Murky Conceptual Waters: The Public and the Private", *Ethics and Information Technology*, Volume 2, No. 3, July 2001.

20 Anne Adams, "Users' Perception of Privacy in Multimedia Communication", Proceedings of the AMC Conference on Human Factors in Computing (CHI 99), ACM Press, 1999, pp. 54-54.

21 CNN.com, "Program to fingerprint US visitors starts", 5 January 2004 (available at www.cnn.com/2004/US/01/04/visit.program).

22 *New York Times*, "Bush lets U.S. Spy on callers without Courts", 16 December 2005 (available at www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200). See also *New York Times*, "Spy Agencies mined vast data trove, officials report", 24 December 2005 (available at www.nytimes.com/2005/12/24/politics/24spy.html?ex=1293080400&en=016edb46b79bde83&ei=5090).

23 Clayton Northouse (ed.), Protecting what matters: technology, security, and liberty since 9/11, Brookings Institution Press, Washington D.C., 2006.

[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm).

[25] Council Decision 2004/496/EC of 17 May 2004.

[26] See http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-317/04

[27] Benoit Otjacques, Patrick Hitzelberger, and Fernand Feltz, "Identity management and data sharing in the European Union", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

[28] James X. Dempsey and Lara M. Flint, "Commercial data and national security", *The George Washington Law Review*, Vol. 72, Number 6, August 2004.

[29] East West Institute – Global Security Programme, Consortium on Security and Technology, "Information Security and Identity Management: Report of the 1st meeting", Number 2, December 2005 (available at http://enisa.europa.eu/doc/pdf/studies/EWIReport_Information_Security_and_Identity_Management.pdf).

[30] June Buchanan and Patricia Ryan, Private and public faces of ethics: Convergence and divergence, International Institute for Public Ethics Conference, Reconstructing 'the Public Interest' in a Globalising World: Business, the Professions and the Public Sector, Brisbane, Australia, 4-7 October 2002.

[31] Ludwig Siegele, "How about now? A survey of the real-time economy", The Economist, January 2002.

[32] CNET.com, "Yahoo! buys e-mail list service eGroups in stock deal", 28 June 2000 (available at http://news.com.com/2100-1023-242517.html).

[33] Felix Stalder, "The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy", *Sociological Research Online*, Vol. 7, no. 2, August 2002.

[34] Paddy Nixon et al, "Security, Privacy and Trust Issues in Smart Environments", The Global and Pervasive Computing Group, University of Strathclyde, United Kingdom.

[35] See http://freenetproject.org

[36] This categorization is taken from Felix Stalder, "The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy", *Sociological Research Online*, Vol. 7, no. 2, August 2002.

[37] See Wikipedia on the history of cryptography (at http://en.wikipedia.org/wiki/History_of_cryptography).

[38] See the international PGP home page (at www.pgpi.org).

[39] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Volume 22, Number 6, 1976.

[40] Peter Gutmann, "PKI: It's not dead, just resting", *IEEE Computer*, August 2002.

[41] The Register, "How to clone the copy-friendly biometric passport", 4 August 2006 (available at www.theregister.co.uk/2006/08/04/cloning_epassports/page2.html).

[42] Felix Stalder, "The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy", *Sociological Research Online*, Vol. 7, no. 2, August 2002.

[43] Lara Srivastava, "Mobile phones and the evolution of social behaviour", *Behaviour & Information Technology*, Vol.24, No.2, March–April 2005,111–129

[44] ITU, ITU Internet Reports 2005: The Internet of Things *(*available at www.itu.int/internetofthings).

[45] Jennie Caroll, John Murphy, "Who am I? I am Me! Identity management in a networked world", 4th International We-B Conference, 24-25 November 2003.

[46] Kim Cameron, "The Laws of Identity", Microsoft Corporation.

[47] Danah Boyd, "Faceted Id/entity: Managing representations in a digital world", MIT Media Lab.

[48] Lawrence Lessig, Code and Other Laws of Cyberspace, New York: Basic Books, 1999.

[49] Kim Cameron, "The Laws of Identity", Microsoft Corporation.

[50] Frank Ramdoelare Tewari, Master's Thesis, Faculty of Economics, Erasmus University, Rotterdam, December 2005.

[51] Philip J. Windley, Understanding digital identity management, The Windley Group, 2003.

[52] The Open Group Identity Management Work Area & Skip Stone, Identity management: A white paper, March 2004.

53 European Commission, PRIME White Paper.

54 Lauren Wood, Alex Acton, “Identity Management and Federation”, BC.Net Conference, 25 April 2006.

55 Ray Tam, “Federated Identity: A fairytale or reality?”, ISSA Journal, July 2005.

56 Elisa Bertino and Abhilasha Bhargav-Spantzel, “Digital Identity Protection in Federations”, CERIAS, Department of Computer Science, Purdue University, 21 December 2005.

57 The Liberty Alliance is a global body working on defining open standards, privacy advice and industry guidelines for digital identity interactions: its members include over 150 member organizations, e.g. governments, end-user businesses, system integrators, and vendors (see www.projectliberty.org).

58 Warren’s Washington Internet Daily, “NGN Identity Management Eyed for ITU Standardization”, Volume 7, Issue 149, 3 August 2006. It is to be noted that ITU, in collaboration with DAIDALOS will be staging a workshop on Digital Identity for NGN on 5 December 2006 (for more information, see www.itu.int/ITU-T/worksem/ngn/200612/index.html).