Social Science Information
http://ssi.sagepub.com/

Identity, social status, privacy and face-keeping in digital society

Saadi Lahlou

Social Science Information 2008 47: 299
DOI: 10.1177/0539018408092575

Special issue: Cognitive technologies

Numéro spécial: Technologies cognitives

SSI

Saadi Lahlou

Identity, social status, privacy and face-keeping in digital society

Abstract. *Digitization of society raises concerns about privacy. This article first describes privacy threats of life-logging. It gives the technically novice reader a quick overview of what information and communication technology (ICT) is currently preparing for society, based on state-of-the art research in the industry laboratories: ubiquitous computing, aware environments, the Internet of Things, and so on. We explain how geolocation systems work and how they can provide detailed accounts of personal activity that will deeply affect privacy. At present, system designers rarely implement privacy-enhancing technologies – we explain why, based on empirical research. On the other hand, users, while expressing concern, do not protect themselves in practice – we list reasons for this. The problem is complex because the very nature of identity and social relations works against protecting personal data; this is the privacy dilemma. At least two key mechanisms in the production of good interaction and in the construction of social status are based on personal data disclosure. Then we discuss the nature of privacy, based on field observation. Privacy loss can be seen as 'losing face'. We detail this notion, based on a discussion of the notion of face, and especially the Asian social construct of 'Chemyon'. We then propose a new, positive, definition of privacy as 'keeping face'. This positive notion can be used to build constructive guidelines for enhancing privacy in systems design, compatible with the way designers perceive their role. These guidelines are presented in an annex, after a short conclusion that advocates a constructive – perhaps risky – role for social science in the construction of future information and communication technology.*[1]

Key words. *Avatar – Biometrics – Chemyon – Data mining – Face – Geolocation – ICT – Life-logging – Persona – PlaceEngine – Profiling – Privacy Enhancing Technology – Pseudonym – Security – Sensors – Tracking – Ubiquitous computing*

Social Science Information © SAGE Publications 2008 (Los Angeles, London, New Delhi and Singapore), 0539–0184

DOI: 10.1177/0539018408092575 Vol 47(3), pp. 299–330; 092575

Résumé. *La numérisation de la société soulève des inquiétudes concernant la vie privée. Cet article décrit d'abord les menaces que fait peser le traçage continu des actions permis par l'informatique ubiquitaire. Il donne au lecteur techniquement novice un aperçu de ce que les Technologies de l'Information et de la Communication (TIC) sont en train de préparer pour notre société dans les laboratoires de recherche: informatique ubiquitaire, environnements augmentés et 'conscients', Internet des Objets, etc. A titre d'exemple, nous expliquons comment les systèmes de géo-localisation fonctionnent, et comment ils peuvent produire un compte rendu détaillé et invasif de l'activité des individus. Or, actuellement, les concepteurs de tels systèmes ne mettent pas en place de garde-fous techniques – nous en listons les raisons. De leur côté, les utilisateurs, bien qu'exprimant de l'inquiétude, négligent en pratique de se protéger. Nous expliquons pourquoi: il s'avère que la nature même de l'identité et des relations sociales va à l'encontre de la protection des données personnelles. C'est le dilemme de la 'privacy' (respect de la vie privée): au moins deux mécanismes clés dans la production d'une bonne interaction et dans la construction du statut social sont précisément fondés sur la divulgation des données personnelles. Nous discutons ensuite de la nature de la 'privacy', en nous fondant sur des observations de terrain. Nous montrons comment une atteinte à la 'privacy' peut être considérée comme une perte de 'face'. Nous discutons cette approche, à partir de la notion de face, en particulier de sa version asiatique ('Chemyon'). Nous proposons ensuite une nouvelle définition, constructive, de la 'privacy' comme 'maintien de la face'. Cette approche positive est utilisée pour proposer des principes de conception de systèmes informatiques respectueux de la 'privacy', destinés aux concepteurs et compatibles avec l'ethos du métier. Ces principes de conception sont présentés in extenso en annexe, après une courte conclusion qui prône une attitude constructive et engagée des sciences sociales dans le développement des TIC.*

Mots-clés. *Avatar – Biométrie – Capteurs – Chemyon – Environnements augmentés – Face – Fouille de données – Géolocalisation – Informatique pervasive – Life-logging – Persona – PlaceEngine – Profilage – Pseudonyme – Securité – Technologies sauvegardant la vie privée – TIC – Traçage*

1. Privacy issues in the digitized society

People are concerned about privacy; they are afraid that the digital systems they use on an everyday basis may bring unwanted effects into their lives. We all know we can be tracked through our mobile phones, that our email can be intercepted, that data we leave on the Internet may be used to spam us, or even worse. Such concerns are legitimate: this section shows how the combination of information and communication technologies (ICT) and pervasive computing will soon enable continuous monitoring of individual activity, even beyond what science fiction imagined.

In this section, first we give a glimpse of tomorrow's ubiquitous systems (section 1.1). Then we take the example of geolocation and show how much it can reveal of our personal lives (section 1.2). Finally we show how geolocation is only one specific case of 'life-logging' by systems that continuously monitor activity (section 1.3). Therefore, we can see why ubiquitous computing, combined with powerful data-mining techniques, enables a third party to be aware of past, present and to some extent future actions of individuals, thus seriously threatening privacy.

1.1. A future of pervasive computing, sensors, tracking and data-mining

Our future is one of ubiquitous networks, distributed sensing, pervasive computing, ambient intelligence, unlimited digital memory and powerful data-mining systems.

Ubiquitous networks: in the last ten years, the amount of Internet access has been multiplied by 100. Every new access point comes with Wifi capability; networking technologies multiply and combine: high bandwidth fiber, Wifi, Bluetooth, power line. A growing number of neighborhoods install free or cheap wireless access, and, as prices go down, most devices will be seamlessly connected to the network: currently personal computers (PCs) and personal digital assistants (PDAs), but soon most machines. Within a few years, the Internet will be fluidly accessible almost everywhere, continuously, to every device.

Pervasive computing: most devices now incorporate some chips that enable them to communicate with the users, or with other systems, for monitoring, control, command, maintenance or cooperation. These chips follow Moore's law (twice as much computing power every two years for the same price, with ever smaller size and energy consumption). So, connected devices will have computing power. Intelligent tags on non-connected objects will enable them to communicate with the (ICT) framework when in range of tag readers. The new generation of radio-frequency identification (RFID) tags, the wireless equivalent of a bar-code, which can be read by a nearby radio antenna, enable this; millions of them are already in the market, tagging goods, people or mobile assets. So, in the future, virtually every object will be somehow visible to the computer systems through the network. This is called the *Internet of Things*.

Ambient intelligence and aware environments: these intelligent, connected, devices will incorporate or use sensors of many kinds. Sensors continuously become more powerful, smaller, more reliable and less energy consuming.

Devices will be connected with each other and with sensors, but also with large remote-computing centers that will enable complex situation analysis by using the continuous progress of pattern recognition. This produces a situation in which these devices are able to interact with the user while being aware of her intentions and needs, and provide adapted service in context. Such settings, where user interaction with her physical environment is supported by pervasive information technology, are called 'augmented environments'. Home and office automation are the prehistory of this forthcoming evolution.

Unlimited memory and powerful data-mining: The enormous flow of data captured and exchanged in these augmented environments will be stored in databases (e.g. 'data historians'), and will be retrievable by powerful search engines. Most transactions will leave a digital trace and lie in databases. Surveillance cameras will be ubiquitous in public spaces (already the case in the United Kingdom). Most industrial objects will be tagged individually and will be traceable through their entire life-cycle. Potentially, even communications between humans will be recorded, since they will take place through ICT or within ICT capture range (e.g. Internet telephony). The 'Semantic Web' currently under development will enable sophisticated 'intelligent' searches based on the *meaning* of content, rather than on today's simple pattern matching. The capacity of present-day web-search engines (e.g. Google, Exalead) to find within seconds relevant information in billions of web pages gives a glimpse of the computing power available for tomorrow's technology.

These evolutions are permitted by technology, they will be driven by the demands for elderly care, energy conservation and convenience. On the supply side, they will be pushed by competition for added value in the service industry, the economy of knowledge and entertainment, and the ICT industry. We can be absolutely certain that they will take place, for better and for worse.

Obviously this brave new world of interaction with intelligent devices, pervasive recording and total recall brings major changes to our social framework. We are creating a system that will, in a distributed and ubiquitous manner, be aware of all that we do: when we turn on the washing machine, what we write and to whom, where we go and what we do there, what we buy and when with whom and how we use it … and this virtually from cradle to grave. The system as a whole will know more about us than we know about ourselves.

1.2. Geolocation, life-logging and prediction

Geolocation, an already widespread technology, will illustrate the nature and extent of privacy implications. It is necessary to have at least some understanding of the technical capabilities of these new systems to understand how far they change the nature of the social game. This section gives a quick description for the non-technical reader and explains how some current systems can automatically produce individual and precise activity diaries.

Most of us have already used a global positioning system (GPS) which, by triangulation with a set of satellites, informs us of our position in geographical space. There are now many other techniques which enable position location in space: triangulation can be done with ground antennas, e.g. mobile phone antennas or Wifi base stations; by beaconing (identifying a close element of the environment whose position is already known); dead-reckoning (calculating the trajectory from a known position based on inertia and measurement of displacement); scene analysis (recognition of a previously known setting that had already been geolocated); etc. These techniques are mature and will grow in precision. Already, for example, in all countries telephone providers or other entities can instantly geolocate mobile phone users; in some countries this is a commercial service.

Some people are disturbed by the mere existence of such capacities. But these are benign compared to the possibility afforded by continuous geolocation to provide individual *trajectories*.

A trajectory carries much more information than a mere set of positions. First it provides an activity direction, and can give access to intentionality. Then the temporal order of positions may give indications about causality. Finally, the sequence and temporal succession of positions provide a pattern that is more prone to identification. A *series* of trajectories from the same individual is even more revealing, because it yields access to habits. Intersections or convergences in trajectories can reveal a lot about social networks and communities of interests.

To illustrate what can be done with trajectories in space, let us mention just two recent developments. Rekimoto and colleagues (Rekimoto, Miyaki & Ishizawa 2007) have invented a smart geolocation system named PlaceEngine, based on Wifi access points triangulation. Users can download on their mobile a small software device that sends to the system the vector of nearby Wifi access points and their respective strengths, as can be sensed from the user's position.[2] The system returns the user's location, based on comparison with a map of all access points. A most interesting feature of the system is that the global map is created from the vectors sent by users: when an access point unknown to the system appears in a vector, it is added to the map in a position based on its concurrence with other access points. The Wifi map is calibrated with absolute GPS coordinates by client users equipped with GPS sensing-devices who send simultaneously GPS coordinates and Wifi coordinates, or simply tag their location by writing the exact

TABLE 1
Textual representation of location logs (Rekimoto, Miyaki & Ishizawa, 2007)

(a) Results of simple reverse-geocoding	*(b) Applying location name substation rules (e.g. Higashigotanda → Office)*
00:00-12:25 Home	00:00-12:25 at home
12:30 Kosugi Nakahara-ku Kawasaki-shi	12:30-13:30 commuting to office
12:35 Higashitamagawa Setagaya-ku Tokyo	
12:45 Shimomeguro Meguro-ku Tokyo	
12:50-13:25 Kami-Oosaki Shinagawa-ku Tokyo	
13:30-15:15 Higashigotanda Shinagawa-ku Tokyo	13:30-15:15 Office
15:30 Kamioosaki Shinagawa-ku Tokyo	15:30-15:45 moving to Shibuya Office
15:35 Ebisu-nishi Shibuya-ku Tokyo	
15:40 Jinguumae Shibuya-ku Tokyo	
15:45 Tomigaya Shibuya-ku Tokyo	
15:50-16:45 Tomigaya Shibuya-ku Tokyo	15:50-16:45 Shibuya Office
17:35-19:50 Higashigotanda Shinagawa-ku Tokyo	17:35-19:50 Office
19:50-20:10 Higashigotanda Shinagawa-ku Tokyo	19:50-20:45 going home
20:15 Kamioosaki Shinagawa-ku Tokyo	
20:20 Kamioosaki Shinagawa-ku Tokyo	
20:30 Okusawa Setagaya-ku Tokyo	
20:35 Shinmaruko Nakahara-ku Kawasaki-shi	
20:40 Hiyoshi Kohoku-ku Yokohama	
20:45-23:55 Home	20:45-23:55 at home

street (and floor) address. In a short time, Rekimoto and colleagues, with the gracious help of users, mapped Tokyo, and are now mapping Japan. Another interesting feature is that the system, unlike GPS, works indoors and in 3D.

With this system, Rekimoto not only provides geolocation, but what he calls *lifetag*. Indeed, spatial position is usually connected to activity. For example, 'home' and 'work' are settings but also locations. The same for 'restaurant', 'cinema', 'supermarket', 'garage', etc. If the user tags the places he often goes to, the system can provide his day's logs in terms of *activity* instead of mere spatial position, as the user's Smartphone automatically sends positions to the system throughout the day (see Table 1).

In this perspective, as Rekimoto et al. (2007) state, LifeTag is a system for *life-logging* (Gemmell et al., 2002). This example shows how easy it is, using a simple set of rules, to transform automatic tracing of location by automatic devices into interpretation of activity.

Simple statistical analysis can reveal interesting features or events, e.g. notice 'unusual behaviors'. The system can of course provide a lot of useful services for personal memory, and Rekimoto lists several. It can also be used, for example, to help people with memory disabilities (e.g. Alzheimer's), keep track of children, etc.; but it can also be used to search back into the past to see, for example, who was doing what and when.

John Krumm's work shows that such systems can also be used for inference and prediction. For example, the places where people usually stay at night have a high probability of being their home; and then their identity can be inferred by using a public phone directory (Krumm, 2007a, 2007b). Furthermore, as an individual tends to use the same trajectories regularly, final destination can be inferred from the first segments of the trajectory, and the system can then guess *in advance* where a person will be, and when. Krumm goes one step further and shows that, given the constraints of roads, the nature of places (e.g. supermarkets, airports, and so on) which are likely to be destinations, if provided with the first segments, a system can infer with increasing probability where a trajectory will end, based on databases of where the general population usually goes. Such a system can, for example, infer that the subject is now probably driving to the airport, and send a discount coupon for one of the airport parking lots. The larger the databases, the more will be known about the user, the more efficient the inference rules and the better the prediction. And, as we have seen, it is likely that all these parameters will grow more acute as pervasive sensing develops.

To sum up, continuous geolocation makes it possible, to some extent and with good probability, to infer what a person is doing on the fly, what she has done in the past and to some extent predict what that person will be doing in the next moments. This ubiquitous and quasi-divine knowledge of what a person is doing, has done and to some extent will do is completely new in the history of humankind. As we can see, it goes beyond the classic science-fiction fantasy of ubiquitous surveillance depicted in Orwell's novel *1984*. The system not only knows, it can search, compare, analyze, identify, reason and predict – automatically and on a continuous basis. To those who think there are technical limitations to the amount of data the system could process, and the number of objects followed, let us recall Moore's law. Some years ago, many believed that the World Wide Web was too large to be searched. Many of these same people now use Google on an everyday basis, and know better.

1.3. Geolocation and action-location

Now let us step back and see the implications of such capacity in the future augmented environment, where not only spatial position but many actions will be monitored by ICT systems. If the data run freely from one system to another, the global networked system will be continuously aware of where *in the activity space* people are. We call 'activity space' the general space of all variables that can describe a subject's state in the world: emotional state, social position, goals, geographical position, movements, belongings, etc. An activity is a trajectory in this space, where behavior can be described as changes in some of these parameters. *Life-logging* is recording the series of such parameters.

Geolocation is the capacity, through the capture of a specific event in time and/or calculations based on series of events, to locate the position of a specific object in geographical space at a given time. By doing something (e.g. interacting with some sensor) the subject signals its position in geographical space. Geolocation is then one specific case of 'action-location': the capacity to locate the position of an object in an 'activity space' at a given time.

People and objects follow trajectories in activity space (e.g. playing tennis). By doing something, the subject signals its position in an *activity* space, not only in geographical space. Geographical location can be an indicator of position in activity space (e.g. on the road to the tennis club, on the court, in the shower, on the road back, and so on). But many other parameters can be indicators of this activity: heartbeat rate, accelerometry, noise, pressure on soles, logging in at an automatic court door, paying for a drink at the clubhouse, etc. Some patterns of sensor activity are a signature of the activity being performed: e.g. paying with a credit card is a good indicator of shopping.

On top of this, each human has a specific way of performing a given activity; therefore pattern analysis of activity traces can enable recognition of both *what* is being done and *who* is doing it. For example, Hodges & Pollack (2007) tagged with RFID all items in an office coffee corner (coffee, sugar, milk, cups, etc.); they asked ten subjects to wear a tag-reading glove when preparing their coffee. By processing data with machine learning algorithms they were able to identify with over 75% accuracy *who* was preparing coffee, since each user had a rather specific routine. As Hodges & Pollack word it, sensors can capture patterns of 'object-use fingerprint' that can be used for human identification.

John Krumm examined for geolocation various ways of protecting the user against privacy attacks: reducing the quality of data,[3] and various kinds of anonymity.[4] The somewhat disturbing conclusion is that these countermeasures are not very effective. Algorithms using constraints on the physical nature of trajectories (e.g. maximum speed between successive locations), for example 'multi-target tracking' algorithms originally designed for military missile tracking, or other statistical techniques, are in most cases able to identify the correct conclusions anyway (Krumm, 2007a, 2007b).

We must, unfortunately, darken the picture even further. Krumm's work shows potential privacy threats within a single geolocation system. The future situation in which multiple systems (geolocation, communications, action-sensing and transaction logs) will track the user multiplies the threat by adding the possibility of triangulation between systems. If one can cross a trajectory in one tracking system with a trajectory in another, data can be merged and positions in each trajectory can benefit from the series of data from the other system, thereby limiting the possibility of ambiguity. For example, in the case of the coffee-making fingerprint studied by Hodges & Pollack, if the geolocation of the subject were available, her trajectory could be tracked back to an office, and identification made easier. In the future, such trajectory crossings will be commonplace: for example the MAC[5] address of the IP phone and the electronic wallet may be the same if the same Smartphone is used as the support device for both, and this MAC address may appear in every connection to the network.

These examples using state-of-the-art technology – which is very crude compared to what will be available ten years hence – show that combining ubiquitous sensing, databases, pattern recognition and search algorithms makes it possible to identify who is doing or did what, and to some extent to predict who will do what and when. This last capacity, prediction, is especially worrying because it enables the system, or whoever uses it, to prepare with precognition some interaction in real time with the subject. There is nothing magical about this precognition: it is merely the result of statistical extrapolation. For example, one can intercept the subject at some future point in her predicted trajectory and do something to her. This means new possibilities for control of and interference in other people's lives to a degree that was only imagined in science-fiction novels. Krumm's work on privacy attacks suggests that it will be difficult to avoid identification with technical countermeasures only and, therefore, if we want to safeguard privacy, we must turn to limitation of the tracking systems themselves and to legal regulation.

2. Designers and users are privacy concerned but do not act accordingly

Users are privacy concerned, as many surveys show. But these surveys also show that they do not take appropriate measures to protect their privacy. Most users of digital commerce give their credit card number online, complete online questionnaires, etc. Even though Google Mail explicitly states that it searches the user's email in order to guide advertising to their web pages,[6] it has millions of users, many of whom belong to the ICT research community and should be especially aware. Millions of users of FaceBook and other similar sites publicize their social network, although many of them know that these data, aggregated with data collected elsewhere, may be used by unknown third parties, including employers or 'government agencies', and/or for purposes they did not intend.[7]

Krumm (2007) gathered some interesting data concerning how little people care about handing out their personal location data. A study of 74 University of Cambridge students showed them accepting £10 to reveal 28 days of measured locations (£20 for commercial use) (Danezis, Lewis & Anderson, 2005); while 226 Microsoft employees were prepared to give 14 days of GPS tracks in return for a 1% chance of winning a $200 MP3 player; again, out of 62 Microsoft employees involved in a GPS survey, only 21% insisted on their GPS data not being shared outside; also, in a study of 11 subjects using a location-sensitive message service in Seattle, privacy concerns were fairly slight (Iachello et al., 2005); and in Finland, in 55 interviews on location-aware services, '[i]t did not occur to most of the interviewees that they could be located while using the service' (Kaasinen, 2003).

Not only do users not take action to safeguard their privacy, but systems designers show the same gap between concern and action. In our effort to create guidelines for designers, we sent a visiting scholar (Marc Langheinrich) 'troubadouring' around Europe to meet designers of disappearing computer systems, and interview them about the way they dealt with privacy (Langheinrich, 2003; Jegou et al., 2003; Lahlou, 2003). The troubadour tour of designers was instructive: the system designers interviewed all agreed on the importance of the privacy issue, but very few of them had in fact addressed it in their design. Among the reasons are:

- designers not feeling morally responsible;
- privacy design is not yet necessary (at the stage of design), or it is not necessary for prototype systems;
- privacy design is not necessary anymore (because other generic systems take care of it);
- the problem is too abstract;
- privacy is not part of deliverables.

(Langheinrich, 2003)

Designers tend to focus on maximum efficiency of the service of the system, easy programming and easy use. For example, it is much easier to create a new record for each user, as detailed as possible in order to keep track of her preferences, and to re-use this record whenever the user shows up.

The fact that there are few *positive* guidelines for privacy-respectful design is an obstacle for designers. Most privacy guidelines describe what the system *should not* do, but few if any describe what it *should* do. The nature of the definitions of privacy, which are mostly negative, can lead us to a better understanding of the problem. We propose in Section 4.3 some positive guidelines for privacy, based on a new approach to privacy that we describe in Section 4.2. But before that, let us examine another issue that partially explains why users seem so careless about handing out their personal data: social life needs private data to be publicized.

3. Why do we share our personal data?

This section describes the privacy dilemma: social interaction requires the disclosure of personal data. We show here that the most predictive of three ways of defining identity (physical, social, biographical) is the third, precisely the one that is most at stake in the future digital world.

Successful interaction requires that others act in accordance with our own goals, in each specific transaction and beyond. It also requires that the other interactants have a valid model of what kind of behavior can be expected from us, and what type of behavior they are legitimately expected to adopt with us. Without such knowledge, a client could get inappropriate service, a close relative might be treated as a stranger, or the transaction might fail because one of the parties reacted in an unexpected manner.

Social life brings many answers to these issues. First, situations tend to be interpreted as interaction frameworks where the mere fact of 'being there' provides behavioral cues. Somebody entering a shoe shop is implicitly a client who wants to buy shoes; somebody logging onto an online auction service is a potential buyer or seller. But how should this client be treated? Identity is one of the answers: an elderly lady will not be offered the same shoes as a young boy; a person identified as a returning customer may be given some 'preferred' service.

In social life, we usually give others some representation of the entity they are dealing with; we provide some definition of ourselves by giving an *identity*. The issue of identity is complex because it refers both to how we consider ourselves from a subjective point of view and how we define ourselves to others. There are several ways of defining identity: physical (subject as a body); social (subject as a social position); biographical (subject as the product of past experiences and desires).

A person can be considered as a body. Identification is then based on physical characteristics, some of which have transferred into modern biometrics (face recognition, voice identification); together with newer ones: fingerprints, iris scan, palm recognition, etc. That is the classic view. But in the digital world a body is of limited value: it can be used to customize transaction only if it is linked with some file describing individual characteristics.

A person can also be considered from a social perspective: what that person 'is' to others. Social position is a combination of role and status:[8] role is the set of behaviors that others can legitimately expect from the person, while status is the set of behaviors the person can legitimately expect from others (Stoetzel, 1963). Social position may provide useful cues for transactions in the digital world.

The third approach to the subject is psychological and subjective: I have been constructed through my own life history. I am the history of my past experiences, the sum of my preferences, my desires and my motives. I am the sum of my past actions. I am also the source of my future actions. In this subjective perspective, a person is the link between a series of past and future actions. This biographical subject is the most useful for customizing transactions, in the digital world as well as in the physical one, because it provides attested preferences and is usually predictive since people tend to behave now as they did in the past, or to follow trends which are visible in their past record.

Of course people want status, because status gives some power and control over one's environment. Sometimes status is a condition for obtaining access to some goods; often it determines *in what way* we get access to the same goods as others (faster, in priority, with more care and respect, etc.). A common example is fidelity cards, with which users try to get some 'higher' status. Another is the reputation score systems established in many online services. Generally, honorary titles and positions are a classic incentive used by institutions to motivate their members.

Let us now stress a key issue: status is gained through good practice of one's role – someone who properly does her share of work in all circumstances and plays her role properly will usually gain higher status. This social contract is a major mechanism of social control.

A consequence is that status is often claimed by showing proof of past activity. An example is the 'Gold client', who gets his status from the record of previous transactions. Just as we get special treatment in a restaurant where we often go, we would like to get preferred treatment from the systems with which we often interact; does this mean that we want them to keep a memory of all our past transactions? However it may be, *to claim status the subject has some interest in having his actions traced, the record kept, and displayed* to those with whom he has transactions. Herein lies a strong contradiction with keeping past actions private. But keeping such a record may have unexpected implications. For example, some records may be used against the subject's own interest: in one example, a retail company reportedly tried to use the fact that a client had a substantial record of alcohol buying to obtain a settlement in a dispute against this client, who had hurt his kneecap when tripping on spilled yogurt in a Los Angeles supermarket and was claiming for compensation (Vogel, 1998; Lahlou, Langheinrich & Roecker, 2005).

The dilemma is basically as follows: in order to perform interaction successfully (get what we want and get it comfortably) we must provide the others with some identity; but in doing so we reveal personal data; and once disclosed these data may be used for other purposes than the present interaction, beyond our awareness and will. This is the *privacy* dilemma again.

Subjects naturally want to protect themselves. Some subjects may be potential objects of action or control for other subjects, which actions they would prefer to avoid (e.g. social, economic or sexual transaction; training; evaluation; production; and more generally any kind of forced participation). Subjects may also want to hide their activity from others who draw on the same resources (competitors, stakeholders, partners, supervisors, etc.) in order to keep privileged access to that resource or not to be impeached, etc. In sum, subjects may want others to be unaware of some of their behaviors or characteristics, in order to avoid being predated, used, controlled, involved in unwanted activities, impeached, criticized or having their image modified.

On the other hand, subjects want to perform some activities upon or with other individuals or groups – which in turn may be reluctant. To interact with others they must be present to the others' awareness. So, being invisible is no solution. Social life is a continuous series of trade-offs between avoiding risk and searching for satisfaction.

To put it simply, the risk of social life is to go out for something you want and get caught in something you don't want, or be noticed by people you wish weren't aware. But not all privacy is contained in this dilemma. What is privacy?

4. Privacy

Privacy is a fuzzy notion. Its preservation has focused mainly on safeguarding the data disclosed in one interaction and kept on nominal records. As we shall see, this approach is too limited to encompass some of the privacy issues emerging in ubiquitous computing.

4.1. Privacy in the literature and in the regulations

Privacy was initially understood as 'the right to be left alone' (Warren & Brandeis, 1890), 'control over personal data' (e.g. Westin, 1970; Posner, 1984) and sometimes 'encryption'.

Historically, privacy concerns were raised mainly by large institutions or corporations gathering personal data sets; privacy guidelines try to protect individuals against abuse. The OECD 1980 guidelines, reviewed in 1998 (OECD, 1999), similar to the US 1974 Privacy Act, had a large impact; they have been translated into various local versions and have generated a continuously growing descent (see UCAN, 1997 for a history). These guidelines advise limitation of data collection, protection of collected data, limitation of use to initial purpose, right of access and modification by individuals, and implementation of responsibility and enforcement procedures. Most local 'design' guidelines are just variations of these classics, and the privacy policy statements by companies are claims that such principles will be followed. New guidelines gradually add new propositions.

With the growth of Internet services, new privacy threats have arisen, and new generations of guidelines have appeared. For example, the German Teleservices Data Protection Law (TDDSG, 2001), which encompasses online service, among other things, requires anonymity when feasible and traces limitations to profiling. Www.privacy.org, a joint project of the Electronic Privacy Information

Center (EPIC) and Privacy International, gives a glimpse of the literature on the topic, a large part of which is triggered by new technologies. P3P (Platform for Privacy Preferences; Cranor, 2002), PET (Privacy Enhancing Technologies; Borking, 1996; Borking & Raab, 2001), pseudonymity (Kobsa & Schreck, 2003) and other technologies, especially in cryptography, e.g. PGP (Pretty Good Privacy), PKI (Public Key Infrastructure), digital signatures, etc., are rapidly changing the landscape; user communities will soon be providing online resources to help users customize their systems.

Ubiquitous computing is specific in the continuous attention of systems to human activity and because systems take initiatives in data collection. This is especially true for 'Disappearing Computer' (DC) applications, where the presence of a processing unit is not apparent to the user. Therefore DC systems can potentially collect data beyond individuals' awareness. Moreover, as we saw earlier, the ubiquitous nature of systems enables multimodal and longitudinal capture of human activity by a set of distributed but connected systems (e.g. following a person along a journey in a building with a series of sensors, say, for the sake of customizing the environment according to the person's access level and preferences). In doing so, ubiquitous computing introduces a new threat to privacy. The very notions of 'alone' or 'control' may no longer be the appropriate conceptual tools in an environment populated by a ubiquitous population of non-human, intelligent, connected devices, some of which belong to the user herself. In other words, future privacy threats will not come only from large centralized databases; but also from the existence of distributed life-loggings which enable detailed profiling and prediction.

A vast body of literature tries to redefine the privacy concept, and in this respect there are almost as many visions of privacy as there are authors. There have been many discussions on privacy (see reviews above), and some bring quite interesting views, based on theory. For example Dourish & Palen (2003), in a paper grounded in a larger diversity of cases, propose a promising vision of privacy as 'negotiating boundaries'. Privacy is a vast and complex issue, which probably cannot be captured by one single definition; that there is a word 'privacy' does not guarantee there is a single reality behind it anyway (cf. Wittgenstein, 1921). Privacy is indeed difficult to translate in different languages, for instance.

Our approach was not guided by the ambition to define privacy, but by an empirical perspective: to find a simple mental framework that could guide designers of systems. The 'privacy as face-keeping' we propose seems especially productive in this design perspective, which is why, instead of engaging in a discussion of the vast literature, we now describe this specific approach.

4.2. Privacy as face-keeping

The fact that privacy is too abstract a concept remains a design issue (refer the designers' justification for doing nothing about it). Can we relate the privacy issue to the system being designed instead of referring to general risk avoidance? Some empirical observations put us on the track of the face-keeping nature of privacy.

We had taken an empirical approach aimed at observing privacy issues in advanced users' groups. Focus groups were organized with users, e.g. 'evil-creativity' seminars were held with specialists ('How could we abuse the system?'). But the approach that proved most fruitful was the observation of groups of subjects in an experimental privacy-deprived environment. For three years the K1 living laboratory experiment observed a population of 24 real users (mostly engineers working on a project), volunteers who accepted doing their daily work in a 400m^2 digitally augmented environment, designed as an observation laboratory (including 30 video cameras). This 'experimental reality' setting, installed in a large industrial R&D facility, more fully described in a former issue of this Journal (Lahlou, Nosulenko & Samoylenko, 2002) provided rich data for the design of augmented environments. It also enabled us to understand better what privacy issues emerge in daily life in a ubiquitous computing environment where everything is continuously observed and traced. In a way this advanced setting, in which all activity leaves digital traces, is a preview of our future 'normal' digitized world.

Specific attention was given to privacy issues by exploring in detail a series of incidents that occurred in the K1 building (Cicourel & Lahlou, 2002). A typical example of a privacy issue is when a subject is led to answer, in an open-space environment, a phone call which has nothing to do with her present work in the local project (family, friends, doctor, or a colleague with whom she works on another project).

In the real world, unlike in the world of design specification, normal subjects pursue *simultaneously* different lines of action. These activities draw on the same attention resources, and often take place in the same physical space- and time-span. But in these different activities, the subject does not necessarily put on the same *face*. For example one can be an expert, a manager, a project member, a company employee, a friend, etc. What can be said, done and disclosed when wearing these different faces may be quite different. Social rules, and especially politeness, are a way around some of the problems: we pretend not to attend to (see, or hear) what is discrepant with the face a person wears.

This research found, strangely, that cognitive overflow and privacy were two aspects of the same problem for subjects. They provoked similar stress reactions, uneasiness, the feeling of loss of control, of being forced into something, and sometimes anger or resentment. This captures something of the feeling of denial of the classic ‘right to be left alone’. A typical example of cognitive overflow is when the subject is sidetracked to another line of activity, either by external interruption or because he is prompted into it by the casual encounter of an opportunity to solve an urgent and pending issue.

> … the on-line demands of choosing and pursuing different tasks, sometimes in parallel, is inherently a concern with privacy issues because deciding the choice of a task invariably requires taking risks vis-à-vis what should or can be revealed about one’s actions (communicative, interpersonal, and knowledge competencies) and their consequences for one’s career, personal identity, and interpersonal relations. (Cicourel & Lahlou, 2002)

So privacy has something to do with keeping appearances coherent with the current activity vis-à-vis others, in other words ‘keeping face’ in this activity.

Managing faces and resources with competing activities is what should be considered the basic framework for systems design, since most privacy issues – as well as cognitive overflow issues – emerge from the difficulty of following simultaneously activity tracks or several ‘cognitive attractors’ (Lahlou, 2000) with divergent demands. It became clear that most privacy issues emerged from role conflicts between activities. This issue is also well highlighted by Phillips (2005). Not all role conflicts are privacy issues; and probably not all privacy issues are role conflicts. Nevertheless, it seems that privacy issues often arise at the onset of role conflict. This insight provided the concrete angle from which to approach the privacy issue from the point of view of the system being designed, through the notion of activity-related *face*. What does it mean to keep face?

4.2.1. Faces as social constructs. ‘Faces’ are a combination of roles and status. As stated earlier, roles specify what the subject is supposed to do (what others can reasonably expect from him), while status defines the way others are supposed to act with the subject (what the subject can reasonably expect from others) (Stoetzel, 1963). Face is a social construct which includes both a representation of what the subject is supposed to do and of what others are supposed to do with him. Faces are a kind of social user’s manual.

These representations of social roles and statuses are shared in a given population (cf. Moscovici’s ‘social representations’, 1961), and therefore smooth interaction is possible. Such conventions enable interaction, cooperation (Lahlou, 2001) and minor problem resolution. Faces can be, for example, ‘shopkeeper’, ‘buyer’, ‘teacher’, ‘student’, etc. The face system is an efficient social way to rule out chaos and make the world predictable. A face is constructed in reference to other faces with which it interacts. Routine interactions that occur according to social templates follow commonsense 'scripts' (Shank & Abelson, 1977; Rumelhart & Norman, 1983).

One given subject may put on different faces according to time and place (e.g. buyer and seller). Of course everybody knows that we all have several faces (e.g. at work and at home); but in a given situation a subject wears only one face, and all participants (pretend to) ignore the other faces; this enables appropriate interactions.

Places, and more generally situations, are a natural approach to choosing the appropriate faces. Patterns in the setting will elicit meanings and foster specific activities. Each member of a culture knows by common sense what faces are appropriate for a given situation. In ambiguous situations, specific indications may be added for novice participants. When several members of the same culture interact in a situation, they normally endorse the relevant faces to perform collaboratively (e.g. teacher and student). This is why the approach based on not crossing some 'boundaries' (cf. above) is effective for privacy.

Interaction between faces is controlled by politeness rules. A main goal of politeness is to respect the other faces and facilitate their performance. This includes active monitoring of the other face's activity and preventing situations of risk for the face or the underlying body. Politeness rules eliminate most possibilities of conflict arising. For example, politeness rules will include salutations, which ensure faces are respectively aware of each other and accept interaction; taking turns, which enables each face to express goals, acknowledgments, specifications and more generally exchange the metadata necessary for interaction monitoring (Goodwin, 1981); reparations where failures are fixed in order to continue interaction (Goffman, 1959, 1963); closures which end interaction, and update records and statuses in the perspective of further interaction; etc. The very fabric of social life is woven with a million subtle 'inter-face' rules for managing transactions. Politeness rules are one class of the general framework of meta-rules for interaction between faces, which basically mean: 'be aware of faces, act accordingly and cooperate'.

Here we take 'face' to include more than mere presentation of self, as considered in Western psychology, following Goffman (1959, 1963). In the East Asian sense, 'face' (*chemyon* in Korean, *mientze* in Chinese, *taimien* in Japanese) is literally 'the appearance of one's self', and includes five facets: (1) moral integrity or virtue, (2) true intention, (3) position and role, (4) propriety and (5) outward behavior (Choi, Kim & Kim, 1997).

We consider that this elaborate East Asian social construct, polished through millennia of culture, can serve as a basis for privacy guidelines worldwide. The Asian construct of *chemyon* has moral aspects based on

Confucian philosophy that may go beyond our purposes (although this may be discussed), and highlights the status aspects; still (2) to (5) are relevant for our topic here. Maintenance of face is perceived as less important in intimate or informal settings, which is coherent with classic definitions of privacy.

In this perspective, one does not 'play' a face; one 'lives' a face. As a face, one has emotional involvement and can be hurt. Moreover, we believe that face as role construction has a direct connection with the intelligibility of the setting by the subject, because the nature of objects perceived depends upon the subject's goals (see Alexandrov, 2008). The face is what a subject 'is' at a given moment. Disrupting this face provokes disorientation of the subject, stress and discomfort or pain. Therefore any breach in the face is resented as an impeachment to being or becoming what the subject desires, and some kind of aggression towards his or her very being, an intrusion into his or her personal sphere.

The notion of persona has also been used in the ICT design literature, especially for interaction in media spaces. Persona is a partial individual construct, some sub-self or alias, whether they are created as an agent or proxy by the subject, or, as Clarke (1994) notes, a passive identity created by an external party by gathering activity traces of a subject. Although this notion may be close to the notion of face, it differs, since face is a social construct. Any member of a culture knows how a face should behave in a given situation and how others should behave with this face, while a persona is specific and lacks this institutional predictability.

Using the face system means displaying a specific set of characteristics and meanings, which guide others in performing the right behavior. Acting according to the face is part of using the face. Incidentally, some subjects might use the system deceptively in order to get more than what society would normally allow them. Every social system has installed systems that check this possibility by controlling the validity of an individual face, usually during face construction. Seals and tokens referring to the constructive authority (diplomas, IDs, tickets, receipts, habilitations, entitlements, certificates, referees, etc.) then prove legitimacy of faces and can be invoked in context. Formal rites of passage are sometimes organized, after which an individual can legitimately wear the face.

Of course, conflicts may arise from the fact that different subjects may have opposite interests. But this is precisely dealt with by the faces system. Although this system does not suppress *rapports de force*, constraints and some kind of violence, it makes the risks more predictable and ensures reciprocal awareness of participants.

Survival and competition are hence transformed into a game with rules, which is civilization. This system is the legacy of a long cultural evolution;

it should be considered as an installed psycho-social base, to which the new ubiquitous computing systems would better adapt. Pervasive computer systems must take into account this setting and contribute to it by providing subjects with extra resources based on the same interaction principles and politeness rules, rather than hoping to build quickly new user routines based on technical affordances of computer systems.

4.2.2. Losing face, and privacy. What makes the situations difficult to handle is the physical properties of human beings, namely that several faces may have the same bodily support. For instance, individual Paul may, at the same time, be an employee in a company, work on project A, work on project B, belong to a political organization, collect tropical insects, have an affair with one of his colleagues. Although none of these faces is a problem in itself, managing all of them on a continuous basis may be an issue. For example, Paul may need to minimize his 'project-B-member face' to the project-A-manager. Paul may also need to hide his professional email from tropical insect e-sellers to avoid receiving junk mail in his office mailbox.

Our hypothesis is that a privacy breach is a case of 'losing face' – that is, to be impeached to keep on the proper or desired face, to be forced to put on or endorse an unwanted face. This is the case even if the face we are forced to accept at this moment is one that we would (or already have) readily and happily put on in another circumstance.

This hypothesis seems at first sight different from classic definitions, for example the right to be left alone, to have control over one's data, or be allowed to cross certain territory borders. One crucial point to consider, which has been too often overlooked, is that privacy violation does not depend on what is done or disclosed but *to whom* it is disclosed. Privacy violation always implies some 'Other'. In almost any case, change the 'other', and there may be no more violation. Your banker browses your bank account, your doctor knows your illnesses, your sexual partner knows details of your sex life and your colleagues share your business secrets. All these actors are entitled, as faces, to access 'private' aspects of your life.[9] Privacy is not simply a matter of data, but of matching faces. Things go wrong when a 'wrong' face is displayed in a situation (e.g. your work colleagues get a glimpse of your sex life or of your health record).

Of course, keeping face is a local issue: a face that is relevant in one context may be irrelevant in another. This is why supporting privacy is support for activity-related face-keeping; it could also be support for keeping faces local.

The face-keeping approach may not cover all aspects of 'privacy', or may cover them in only a limited way. For instance, the case of 'being left alone' is obviously about privacy. But in what is it a problem of face? One could argue that it is in the fact that another person's presence forces some obligation to put on an appropriate face; which may not correspond to our mood. One is then forced into an unwanted face. In other words, to be left alone is the freedom to wear 'no specific face'; it is some kind of anonymity. Once again, the key question is 'who?' Even in situations where we would prefer to be left alone, in fact some persons happen to be welcome. But this argument may seem far-fetched. In all events, as stated earlier, we do not claim to solve the whole issue with this approach but rather to provide a constructive framework for designers, since we badly need designers to incorporate privacy safeguards in their systems.

4.3. A constructive stand

As we have seen in the previous sections, many classic privacy approaches are user or data protective. They are useful and give some insights into the issue by describing various types of privacy breach and what should be avoided. But this defensive approach hardly provides constructive guidelines for designers in ubiquitous computing systems. Defensive approaches (avoiding some type of event) may need to take account of the general context far beyond the local aims of the application; this is a daunting task for designers and thus is seldom implemented in practice. Constructive approaches (towards achieving a specified goal) may, on the other hand, provide operational guidelines for designers. In helping the designers to focus on precisely what activity is at stake in the system they are designing, the face-keeping approach is coherent with the design stand. Exact tailoring of the system to such activity[10] is the core of the European Disappearing Computer Privacy Design Guidelines (appended to this article) (Lahlou & Jegou, 2003). Here, for example, is Guideline no. 4, the 'Privacy Razor':

> Human user characteristics seen by the system should contain *only* elements which are necessary for the explicit goal of the activity performed with the system. No data should be copied without necessity. In case of doubt, remember further information may be added in context.
>
> During design, the privacy reduction consists in examining each of all variables describing user-face, and trying to eliminate as many as possible. Identity is seldom necessary. The best system is one so lean that nothing more could be taken away. Ideally, Client should 'Display Minimal Characteristics', and System should 'Require Minimal Characteristics to operate ...'.

'Privacy razor' is the core of the guidelines. It must be understood in a positive way, which is, tailoring the system *exactly* to deal with a specific face (e.g. 'airline client' when buying a plane ticket). Tailoring the system in a very strict way for the specific activities of this face makes it more difficult to distort the system for some unexpected use. In the example of the airline client, for example, identity is actually no more necessary than for taking a bus. It may be important to check that the passenger has the appropriate visas to enter the country of destination, but again this is not identity *per se*, rather a profile.

The example of airline passengers is interesting. It was among our initial test scenarios for validating the guidelines with experts, but they appeared so sensitive (especially in the USA) to this issue after the 11 September 2001 terrorist attack that the very idea of anonymity for airline passengers was a problem. We changed the scenario to 'fast-train' passengers (who are just as subject to terrorist attack as airplane passengers, as history has unfortunately proved), and the attitudes of our test panel of designers changed. This showed how much current practice influences judgment of what seems 'feasible'. If we take the activity approach, the face of the passenger is 'traveler', and he will therefore be motivated to prove capacity for entering the destination country, which could be, for example, a biometric encrypted visa, anonymous to the airline company.

The constructive approach to privacy is to identify the characteristics of the face the user wants to put on in the specific context of the application and then turn these characteristics into specifications. Activity analysis may help provide the key tasks to be performed by the user, and the system can then be tailored accordingly. Nevertheless, designers may achieve the same goal using different techniques. There were many examples of web services or disappearing computer devices and systems that exhibit proper design (chats, auction sites, etc.) long before these guidelines were drawn up.

We believe that adopting a constructive design approach to privacy, where privacy-enhancing technology has positive and measurable goals, can give designers positive indications for system specifications. Moreover, defensive approaches to privacy are usually bounded by the state of the art of the technology. They may prove limited in the near future, when instant individual identification will be easy (e.g. through biometrics or profiles), and any aspect of human activity (including emotions and thoughts) may be monitored on a continuous basis by pervasive artificial systems. Even such a transient event as gaze is now reliably traceable by automatic devices (see Vertegaal & Shell, 2008). In general, constructive approaches, and the creation of entities, are more powerful ways to resist. No system built in a defensive perspective can resist hacking. By tailoring systems to consider only the local face of their users, one makes it more difficult to reconstruct identities from their activity logs and to connect them with other activity trajectories.

Finally, we believe a good system should always be on the user's side. The privacy-as-face-keeping approach, by forcing the designers to take the user's point of view in the construction of specifications, is one more step in that direction.

5. Conclusion

This article has examined the potential impacts of pervasive computing and augmented environments on privacy and identity. We have shown why privacy concerns are legitimate, how little is done to preserve privacy in the current systems developments – and why. We have shown that there are social causes: the very processes of claiming status and customizing interaction work against the preservation of personal data. We have discussed the nature of privacy, based on fieldwork, and come to the notion of privacy as face-keeping. We have proposed a new, positive approach to privacy, based on supporting 'activity-related face'. This approach can ground constructive guidelines for system designers, and an example of these guidelines is provided in an annex.

Social science often takes a critical stand on technological issues, which is easier than proposing solutions. Here we took the risk of being constructive, by venturing to propose guidelines based on a psycho-social analysis. We are aware that the 'face-keeping' model of privacy which grounds them may be imperfect and incomplete.

But as we have seen, the problem is social in nature; therefore, it is our responsibility as social scientists to search for solutions, and contribute to an effort to make our augmented, digital future more human-friendly.

6. Annex: European Disappearing Computer Privacy Design Guidelines, Version 1.2 (Lahlou & Jegou, 2003)

6.1. Foreword

These guidelines are aimed at systems designers of augmented environments, and more generally at all stakeholders in systems design. Privacy is a difficult issue. The system you (designer, sponsor, client) design may have very strong effects on the personal life of its future users. These guidelines are a modest collective attempt to help tackle the complex trade-offs designers of DC systems have to face. We wish you success in your design effort.

These are *privacy* guidelines, and therefore do not specifically address basic design rules for human computer interface or system security, on which there is ample literature to be consulted with profit (e.g. Schneiderman, 1992). Some guidelines specifically relevant to privacy issues are redundant with classic design rules. Some are redundant with more general privacy guidelines (e.g. OECD, 1999). Still, they were inserted to make these guidelines stand alone and be handy for designers.

Disappearing computing – 'DC' (aka ubiquitous, pervasive, attentive, etc. computing, or augmented environments: AE) is specific in the *continuous attention of DC systems to human activity*, and *because such systems may take initiatives in data collection*. Therefore DC systems potentially collect data beyond individuals' awareness. The following guidelines focus *on* *the specific issues of data collection by such systems*. This phase is problematic in all types of AE; in a work context it is also connected to legal issues and to 'Agenda 21' issues (cf. declaration of the 1992 Rio summit on sustainability).

AE collects information in order to be aware of user's needs, understand context and provide services according to user's preferences. The AE you are designing may collect data over the long term, which may potentially contain sensitive information about the user's habits, actions, and preferences. Your system may be connected to other systems, and the resulting data may produce even more knowledge about the user. Please note that such data as time of entry or departure from office (e.g. captured by a door) may be sensitive data, with legal or financial implications.

Concerning the files built from data collected by these systems, the general privacy guidelines should be applied. Most current guidelines worldwide correspond to the philosophy of the OECD 1980 guidelines. Please refer to those classic guidelines. Again, some present guidelines may be redundant with general privacy guidelines when specifically relevant.

The present guidelines are the result of a collective effort through a participative design process (Jegou et al., 2003) involving designers, users, and members of the DC and usability research community.[11]

6.2. The Guidelines

Privacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend *ex-post-facto* a poor design against misuse or attacks. These guidelines are a series of 9 rules, each presented as a short title, description of the goal and design comments. Generally the goals of the guidelines need effort to be reached. Comments give some directions for application.

6.2.1. Think before doing. Evaluate potential system impacts. The very nature of a system or its parts may contradict privacy in their intention.

Privacy issues should always be discussed in specifications. Discuss with clients/stakeholders specifications you think are questionable from a privacy standpoint. Designers as Humans have freedom of speech and a social responsibility. Be responsible; you may refuse contribution to some systems.

6.2.2. Revisit classic solutions. Search for existing solutions in the physical world or in old systems for a similar class of problem/service, and understand the way in which new technologies change the effects of classic issues.

Most emerging privacy issues (identification, transaction, control, payment, access keys, codes, etc.) have been socially resolved in other 'classic' settings. They may not always be reusable, but sometimes transposing these solutions or their mental model may capitalize on experience, minimize surprises and make systems more familiar to the human users. Location of data or devices (who holds what) in these classic solutions is often a crucial feature for privacy.

6.2.3. Openness. Systems should give human users access to what they do, do it and do nothing else. Help human users construct a valid and simple mental model of what the system does. Goals, ownership and state of system should be explicit, true and easily accessible to human users, in a simple format.

What the system does especially concerns here the final destination of data gathered by the system.

Each system should display, on request to the human user or his client-part (see glossary), the list of variables required from the human user for operation (cf. below, ‘Privacy razor’). Display of user profile should be a systematic design option. This possibility should be restricted to the user *only for his/her own* data (protecting data is an obligation, consider encryption).

Beware: excessive verbosity of systems and excessive notice to users without demand provoke bypass and are unrealistic. Openness is a goal, and the *possibility* for the willing user to access his/her data in the system; it does not mean systematic notice.

Open source is a guarantee of transparency.

When ‘system’ is another human user (live, mediated by communication system), disclosure should be symmetrical.

System state should be accessible on demand as display and as data.

6.2.4. Privacy razor. Human user characteristics seen by the system should contain ***only*** *elements necessary for the explicit goal of the activity performed with the system. No data should be copied without necessity. In case of doubt remember, further information may be added in context.*

During design, privacy reduction consists in examining each of all variables describing user-face, and trying to eliminate as many as possible. Identity is seldom necessary. The best system is one so lean that nothing more could be taken away. Ideally, Client should ‘display minimal characteristics’, and System should ‘require minimal characteristics’ to operate.

This includes display issues (display needs no copy; prefer displays on the user’s devices). Hardware sometimes copies data in cache or buffers: implement erasing procedure.

This is a hard guideline; it imposes a very clear vision of the system’s functionalities and is far from current practice. The list of variables should be made in any case, and choice left to the user for providing non-necessary data.

When appliances are embedded into larger systems, the privacy razor helps clarify which application gathers data for what. It may be a legitimate design choice to bypass locally the privacy razor rule for better global operation; consider the sensitivity of data at stake.

6.2.5. Third-party guarantee. Using a neutral or trusted third party may open more solutions or lighten design. It may enable entitlement, validation, control, claim, archive, etc., without direct data transfer between system and human user. In case of third-party involvement, give the user choice.

Using simultaneously three keys (human user, system, third party) enables transactions in which each party can impeach the transaction, and future cancellation of entitlement is possible.

Access rights to the services provided by the system may be granted through tokens. Token validation or verification should be possible only with the human user’s agreement; avoid direct identification of human user by system.

Third-party guarantee may prove useful to enable recovering from incidents (client claims with lost tokens, local system failure, identity theft issues…), without imposing the collection of extra local data capture *within the system* 'in case of such incidents'.

6.2.6. Make risky operations expensive. No system is one hundred percent privacy safe. Human users should be made aware of which operations are privacy sensitive. Operations identified as privacy sensitive should be made costly for the system, the human user, the third party.

This is a general design guideline, here also intended to make the operation costly and difficult for computer agents to do on a large scale. Systematic cost (a few cents or a small time delay), or the mere obligation to trace the record of who accessed the data may be a high enough cost to discourage potential abusers.

In some cases this guideline can be dangerous (e.g. access to medical data in emergency situations). Consider exceptions and plan solutions (e.g. third-party control).

6.2.7. Avoid surprise. Human users should be made aware when their activity has an effect on the system. Acknowledgement should be explicit for irreversible major changes. Cancellation should be an option as much as possible, not only in the interface but in the whole interaction with the system.

This is a general design guideline, but crucial in DC, where user awareness is lower.

System should display a response to human user's action if it has an influence on their state, and display any major changes of state. Traces of these acknowledgements should be recorded on system, and be recordable by user. Be aware of the trade-off between cognitive overflow and awareness; enable customizing default acknowledgements.

Technical and social solutions exist to make default privacy-level choices without overloading the user with acknowledgement demands. Consider P3P.

6.2.8. Consider time. Expiry date should be the default option for all data.

Expiry delay is often fixed by law. Use common sense. User benefits should be proportionate to risks.

Saving data is often a design choice for reasons not directly relevant to the service provided, e.g. security against system crash, cache, resource optimization or design simplicity. These design issues are legitimate but should be considered separately and resolved in relevant ways.

It makes a big difference to plan oblivion, even in the long (legal) term. Privacy issues may arise from traces of what users did long ago in former social positions.

The DC design case is quite specific: leave long-term recording to legal systems. In case of doubt, be on the user's side.

6.2.9. Good privacy is not enough. Safety, security, sustainability, equity … are important issues with which trade-offs may have to be considered. These trade-offs should be discussed with stakeholders or their representatives as much as possible.

The designer's point of view is always limited. Most rules are social compromises. Make explicit the trade-offs between privacy and other issues (e.g. reciprocity, emergency access, global security) and trace design choices for further discussion with stakeholders, and for future updates: new technologies may enable a better solution to the trade-off.

Things change. New issues appear. Make sure human users are empowered to feed back and complain by implementing the function in the interface.

6.3. Glossary of terms used in the EDC-PG guidelines

Activity: the sequence of actions at stake in the interaction between human user and system

Client part: is the part of the system that is located by the user

Device: a physical artifact which may interact with the system

Display: representation in a form directly available to the human senses

Human user: a human physical entity (person, group), with a physical body

Location: An entity, system, program, data or element is said to 'be located' where it can be completely destroyed, e.g. a system is said to 'be located' in a device if it has no copy elsewhere

Server part: the part of system that is not located by the user, seen by the user

System: the combination of material hardware and programmed software that are designed to provide services to faces, directly through the means of natural human body or through the use of devices

System-face: the system as seen by the human user. These definitions may be relative: in a peer-to-peer system, a client may be seen as someone else's server

User-face: the human user as seen by the system

6.4. OECD Guidelines, 1980–98

6.4.1. Collection limitation principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data human user.

6.4.2. Data quality principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

6.4.3. Purpose specification principle. § 9 The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of the change of purpose.

6.4.4. Use limitation principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with § 9 except: (a) with the consent of the data human user; or (b) by the authority of law.

6.4.5. Security safeguards principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6.4.6. Openness principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

6.4.7. Individual participation principle. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

6.4.8. Accountability principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Saadi Lahlou is a social psychologist; he worked on social representations, text mining and consumer behavior. For the last 15 years, he has been analyzing the determinants of human behavior in real settings and ‘natural experiments’ in industry, with protocols using digital ethnography and video, including the subcam, a miniature video-camera worn at eye-level by users. Saadi Lahlou heads the Laboratory of Design for Cognition at EDF R&D, and is associate research director at the CNRS-EHESS/IIAC/ Centre Edgar Morin. He has also been the scientific director of the Cognitive Technologies research program at the Fondation Maison des Sciences de l’Homme since 1998. *Author’s address*: EDF R&D, Laboratory of Design for Cognition, 1 avenue du Général de Gaulle, 92141 Clamart, France; EHESS, 54 Bd Raspail, 75006 Paris, France. [*email*: lahlou@ehess.fr]

Notes

[1] This research was co-funded by the Fondation Maison des Sciences de l’Homme/DEVAR and EDF R&D Cognitive Technologies program; and EU IST/ Disappearing Computer Initiative contract No IST-2000–25134 (Ambient Agoras).

[2] Like the mobile phone, the Wifi network is based on radio antennas (‘access points’). Most individual users with high bandwidth access have one such access point at home, which can be detected by Wifi devices, even if they are not allowed to connect. In a city like Tokyo, these antennas form a fixed network of hundreds of thousands of beacons, which enable very precise geolocation.

[3] For example, false reports or obfuscation: feeding the system with inaccurate data by not giving the exact position, but a random position close by.

[4] Pseudonyms, or ambiguity, like k-anonymity, that is sending the position request from a random user among the k users present in close range of the actual user.

[5] The media access control address (MAC address), or now the Extended Unique Identifier (EUI) a number that acts like a name for a particular network adapter, and enables identification of the device by the network in order to send the data packets.

[6] ‘When you use Gmail, Google’s servers automatically record certain information about your use of Gmail. Similar to other web services, Google records information such as account

activity (including storage usage, number of log-ins), data displayed or clicked on (including UI elements, ads, links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL) … The Gmail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Gmail. Google's computers process the information in your messages for various purposes, including formatting and displaying the information to you, delivering advertisements and related links, preventing unsolicited bulk email (spam), backing up your messages, and other purposes relating to offering you Gmail' (Google Mail Privacy policy statement, 2007).

7. 'FaceBook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the FaceBook service through the operation of the service (e.g. photo tags) in order to provide you with more useful information and a more personalized experience. By using FaceBook, you are consenting to have your personal data transferred to and processed in the United States … we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the FaceBook service or using the FaceBook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies' (FaceBook privacy statement, Jan. 2008).

8. The notions of role and status have been debated for almost a century in psychology and sociology (since the first attempts to define the notion [James, 1905/1890; Mead, 1934; Lewin, 1935; Linton, 1945; Parsons, 1951; Coutu, 1951; Bates, 1956]) and one can find many variations in their definitions between authors (for a detailed review see Rocheblave-Spenle, 1969). For the sake of simplicity, we adopt here the definition given by Stoetzel (1963).

9. A few aspects are strictly private, and shared with no one. As a matter of fact, these aspects are often 'embarrassing', which means they may even have to be hidden from other parts of our own ego, or we would lose face vis-à-vis ourselves. So, protecting privacy is making sure each aspect of ourselves will only be accessible with the 'right' faces, and not with the wrong ones.

10. To understand the nature of activity, 'activity theory' (Rubinstein, 1940; Leontiev, 1975; Nosulenko & Rabardel, 2007) is a very powerful tool for producing and specifying tasks and operations in context when initial goals are known. This theory is increasingly being made available to non-Russian speakers (see Nardi, 1996 for a human–computer interaction oriented introduction).

11. Special thanks go to Hugues Bersini (ULB, BE), Jan Borchers (Univ. Aachen, DE), Gillian Crampton-Smith (Interaction Design Institute Ivrea, IT), Volker Hartkopf (CMU, PA, USA), Calle Jansson (Univ Stockholm, SE), Elie Liberman (Strat-e-go, BE), Preben Mogensen (University of Aarhus, DK), Valery Nosulenko (Academy of Sciences, Russia), Norbert Streitz (Fraunhofer IPSI, DE), Terry Winograd (Stanford University, CA, USA) for their valuable input to discussions of the guidelines.

References

Alexandrov, Y. (2008) 'How we fragment the world: view from inside versus view from outside', *Social science information sur les sciences sociales* 47(3): 423–63.

Bates, F. (1956) 'Position, role and status: a reformulation of concepts', *Social forces* 34(4): 313–21.

Borking, J. (1996) 'Der Identity Protector', *Datenschutz und Datensicherheit* 11: 654–8.

Borking, J. & Raab, C. (2001) 'Laws, PETs and other technologies for privacy protection', *The journal of information, law and technology* (JILT) 1: http://elj.warwick.ac.uk/jilt/01-1/borking.html/.

Choi, S.-C., Kim, U. & Kim, D.-I. (1997) 'Multifaceted analyses of chemyon ("social face"): an indigenous Korean perspective', in K. Leung, U. Kim, S. Yamaguchi & Y. Kashima (eds) *Progress in Asian social psychology*, vol.1: pp. 3–22. Singapore: John Wiley.

Cicourel, A. & Lahlou, S. (2002) 'Technology, privacy, and limited capacity processing: a case study', Working paper, Laboratory of Design for Cognition, EDF R&D, Clamart, France.

Clarke, R. (1994) 'The digital persona and its application to data surveillance', *The information society* 10(2): http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html.

Coutu, W. (1951) 'Role playing vs role-taking', *American sociological review* 16(2): 180–7.

Cranor, L. (2002) *Web privacy with P3P*. Sebastopol, CA: O'Reilly & Associates.

Danezis, G., Lewis, S. & Anderson, R. (2005) 'How much is location privacy worth?', in Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University, 2–3 June 2005. http://homes.esat.kuleuven.be/~gdanezis/

Dourish, P. & Palen, L. (2003) 'Unpacking "privacy" for a networked world', in *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pp. 129–36. Ft Lauderdale, FL: ACM.

Gemmell, J., Bell, G., Lueder, R., Drucker, S. & Wong, C.. (2002) 'MyLifeBits: fulfilling the Memex vision', Proceedings of ACM multimedia'02, 1–6 December 2002, Juan-les-Pins. http://research.microsoft.com/barc/MediaPresence/MyLifeBits.aspx

Goffman, E. (1959) *The presentation of self in everyday life.* New York: Doubleday Anchor.

Goffman, E. (1963) *Behavior in public places: notes on the social organization of gatherings.* Glencoe, IL: The Free Press.

Goodwin C. (1981) *Conversational organization: interaction between speakers and hearers*. New York: Academic Press.

Hodges, M. & Pollack, M. (2007) 'An "object-use fingerprint": the use of electronic sensors for human identification', in J. Krumm, G. D. Abowd, A. Seneviratne & T. Strang (eds) *UbiComp 2007: ubiquitous computing 9th international conference*, pp. 289–303. Conference held at Innsbruck, Austria, 16–19 September 2007. Berlin: Springer (Lecture notes in computer science).

Iachello, G., Smith, I., Consolvo, S., Abowd, G., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J. & Lamarca, A. (2005) 'Control, deception, and communication: evaluating the deployment of a location-enhanced messaging service', in *UbiComp 2005 proceedings*, pp. 213–31. Berlin: Springer (Lecture notes in computer science).

James, W. (1905) *The principles of psychology*. New York: Henry Holt.

Jegou, F., Lahlou, S., Langheinrich, M. & Lieberman, J. (2003) 'Design of privacy enhancing technology', EU Ambient Agoras IST-DC program report D15.3. LDC, EDF. R&D, October 2003.

Kaasinen, E. (2003) 'User needs for location-aware mobile services', *Personal and ubiquitous computing* 7(1): 70–9.

Kobsa, A. & Schreck, J. (2003) 'Privacy pseudonymity in user-adaptive systems', *ACM transactions on internet technology* 3(2): 149–83. http://www/ics.uci.edu/~kobsa/papers/2003-TOIT-kobsa.pdf

Krumm, J. (2007a) 'Computational location privacy: present and future', Cognitive Technologies symposium: geolocation, psychological and social impacts, oral presentation, Fondation Maison des Sciences de l'Homme, Paris, 12 November 2007.

Krumm, J. (2007b) 'Inference attacks on location tracks', Fifth international conference on Pervasive Computing (Pervasive 2007), Toronto, Ontario, Canada, 13–16 May 2007.

Lahlou, S. (2000) 'Attracteurs cognitifs et travail de bureau', *Intellectica* 30: 75–113.

Lahlou, S. (2001) 'Functional aspects of social representations', in K. Deaux & G. Philogene (eds) *Representations of the social*, pp. 131–46. Oxford: Blackwell.

Lahlou, S. (2003) 'A positive approach to privacy', EU Ambient Agoras IST-DC program report D15.2.3. EDF R&D/LDC.

Lahlou, S. & Jegou, F. (2003) 'European disappearing computer privacy design guidelines V1 [EDC-PG 2003]', EU Ambient Agoras IST-DC report D15.4. LDC, EDF. R&D/LDC. http://www.rufae.net/privacy.htm

Lahlou, S., Langheinrich, M. & Roecker, C. (2005) 'Privacy and trust issues with disappearing computers', *Communications of the ACM* 48(3): 59–60.

Lahlou, S., Nosulenko, V. & Samoylenko, E. (2002) 'Un cadre méthodologique pour le design des environnements augmentés', *Social science information sur les sciences sociales* 41(4): 471–530.

Langheinrich, M. (2001) 'Privacy by design – principles of privacy-aware ubiquitous systems', *Ubicomp 2001*, pp. 273–91. Berlin: Springer-Verlag (Lecture notes in computer science).

Langheinrich, M. (2003) 'The DC-privacy troubadour – assessing privacy implications of DC-projects', position paper for Tales of the Disappearing Computer conference, Santorini, Greece, 1–4 June 2003. http://www.vs.inf.ethz.ch/publ/papers/dctales-privacy.pdf

Leontiev, A. N. (1975) *Activité, conscience, personnalité*. Moscou: Editions du Progrès.

Lewin, K. (1935) *A dynamic theory of personality*. New York: McGraw-Hill.

Linton, R. (1945) *The cultural background of personality*. New York: Appleton-Century.

Mead, G. H. (1934) *Mind, self, and society*. Chicago, IL: Charles W. Morris.

Nardi, B. A., ed. (1996) *Context and consciousness: activity theory and human–computer interaction*. Cambridge, MA: The MIT Press.

Nodder, C. (2003) 'Say versus do; building a trust framework through users' actions, not their words', workshop on Privacy at *Ubicomp 2003*, Seattle, Washington, September 2003. http://guir.berkeley.edu/pubs/ubicomp2003/privacyworkshop/

Nosulenko, V. & Rabardel, P., eds (2007) *Rubinstein aujourd'hui. Nouvelles figures de l'activité humaine*. Paris: Octares, Editions Maison des Sciences de l'Homme.

OECD Directorate for Science, Technology and Industry (2003) Committee for Information, Computer and Communication Policy's working party on Information Security and Privacy (1999) *Inventory of instruments and mechanisms contributing to the implementation and enforcement of the OECD privacy guidelines on global networks* DSTI/ICCP/REG(98)12/FINA. Paris: OECD.

Parsons, T. (1951) *The social system*. Glencoe, IL: The Free Press.

Phillips, D. J. (2005) 'From privacy to visibility: context, identity, and power in ubiquitous computing environments', *Social text* 23: 95–108.

Posner, R. A. (1984) 'An economic theory of privacy', in F. Schoeman (ed.) *Philosophical dimensions of privacy*, pp. 333–45. Cambridge: Cambridge University Press.

Rekimoto, J. (2007) 'Toward cybernetic-city: sensonomy and location aware computing', Cognitive Technologies symposium: geolocation, psychological and social impacts, oral presentation, Fondation Maison des Sciences de l'Homme, Paris, 12 November 2007.

Rekimoto, J., Miyaki, T. & Ishizawa, T. (2007) 'LifeTag: WiFi-based continuous location logging for life pattern analysis', in J. Hightower, B. Schiele & T. Strang (eds) *Location- and Context-Awareness third international symposium*, *LoCA 2007*, pp. 35–49. Proceedings of the conference at Oberpfaffenhofen, Germany, 20–1 September 2007. Berlin: Springer (Lecture notes in computer science series).

Rocheblave-Spenle, A. M. (1969) *La notion de rôle en psychologie sociale*. Paris: Presses Universitaires de France (2nd edn).

Roecker, C. (2002) 'Specific report on privacy', EU Ambient Agoras program report no.15.2.1, Disappearing Computer initiative.

Rubinstein, S. L. (1940) *Osnovy Obshchei Psikhologii* [Foundations of general psychology]. Moscow: Uchpedgiz.

Rumelhart, D. & Norman, D. (1983) 'Representation in memory', Center for Human Information Processing, University of California at San Diego, Report no. ONR 8302, UCSD Chip 116.

Schneiderman, B. (1992) *Designing the user interface*. Reading, MA: Addison Wesley (2nd edn).

Shank, R. & Abelson, R. P. (1977) *Scripts, plans, goals, and understanding*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Stoetzel, J. (1963) *La psychologie sociale*. Paris: Flammarion.

TDDSG (2001) Act on the protection of personal data used in teleservices (Teleservices data protection act – *Teledienstedatenschutzgesetz TDDSG*) of 22 July 1997, amended last by Article 3 of the bill on legal framework conditions for electronic commerce, *German Federal Law Gazette* 1: 3721: http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf.

UCAN (1997) Privacy rights clearinghouse, 'A review of the fair information principles: the foundation of privacy public policy': http://www.privacyrights.org.

Vertegaal, R. & Shell, J. S. (2008) 'Attentive user interfaces: the surveillance and sousveillance of gaze-aware objects', *Social science information sur les sciences sociales* 47(3): 275–98.

Vogel, J. (1998) 'When cards come collecting – how Safeway's new discount cards can be used against you', *Seattle weekly* 24–30 September.

Warren, S. D. & Brandeis, L. D. (1890) 'The right to privacy', *Harvard law review* 4(5): 193–220.

Westin, A. F. (1970) *Privacy and freedom*. New York: Atheneum.

Wittgenstein, L. (1921) *Tractatus logico-philosophicus*, with an introduction by Bertrand Russell. London: Kegan Paul, Trench & Trubner; New York: Harcourt, Brace, 1922.