Ambient Agoras:
Dynamic Information Clouds in a Hybrid World
IST-2000-25134

D15.4 –European Disappearing Computer Privacy Design Guidelines v1.

WP15 – Privacy Issues

Report Version:	*1.0*
Report Preparation Date:	*31.10.2003*
Covering Period:	*01.10.2002 – 31.10.2003*
Classification:	*PU*
Workpackage Leader:	*Electricité de France LDC*
Author(s):	*Saadi Lahlou, François Jegou*
Project Coordinator:	*Fraunhofer IPSI (Darmstadt, D)*
Partners:	*Electricité de France LDC (Paris, F)* *Wilkhahn (Bad Münder, D)*

Table of Contents

1 Foreword

These guidelines are aimed at systems designers, but more generally at all stakeholders in disappearing computing (DC) systems design.

Privacy is a difficult issue. The system you design may have very strong effects in the personal life of its future users.
These guidelines are a modest, collective, attempt to help you in tackling with the complex tradeoffs designers of DC systems have to face.
We wish you success in your design effort.

They are *privacy* guidelines, and therefore do not address specifically basic design rules for human computer interface or system security, on which there is ample literature to be consulted with profit[1]. Some guidelines are redundant with classic design rules when specifically relevant with privacy issues.

Disappearing Computing –"DC" (a.k.a. Ubiquitous, Pervasive, Attentive etc. Computing, or Augmented Environments) is specific in the *continuous attention of DC systems to human activity*, and *because DC systems take initiatives in data collection*. Therefore DC systems are potentially collecting data beyond individuals' awareness. The following guidelines (European Design Guidelines for Privacy in Ubiquitous Computing, in short "EDG-PG") focus on the specific issues of data collection phase by such systems.

Concerning the files built from data collected by these systems, the general privacy guidelines should be applied. Most current guidelines worldwide are in the philosophy of the OECD 1980 guidelines. Please refer to those classic guidelines, e.g. in the annex of this document. 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 involving members of the DC and usability research community[2][3].
Their present state is far from perfect, as there is presently too little experience of DC systems operating "in the wild" to have large scale feedback. Also, technological evolution challenges guidelines in strange and unforeseen ways. Therefore these guidelines will need periodic update.
This version (EDC-PG 2003) is to be further amended in a continued design cycle. The rules provided here are a backbone for a larger operational document presenting inspiring examples and case stories. An implementation guide gathering good practice should be constructed collectively.
A committee will organize this update and implementation guide construction, in cooperation with other organizations involved in the privacy issue.
Links will be available at www.rufae.org/privacy.

[1] E.g. Schneiderman, B. (1992). Designing the user interface (2nd ed.). Reading MA: Addison Wesley.

[2] Jegou F., Lahlou, S., Langheinrich, M., Lieberman, J. *Design of Privacy Enhancing Technology.* Ambient Agoras IST-DC report D15.3. LDC, EDF. R&D, Oct. 2003.

[3] Special thanks 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 (Univ. Aarhus, DK), Valery Nosulenko (Acad. Sciences, Russia), Norbert Streitz (Fraunhofer IPSI, DE), Terry Winograd (Stanford Univ, USA) for their valuable input.

2 European Disappearing Computing Privacy Design Guidelines, V1. [EDC-PG 2003]

Privacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post 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.

2.1 Think before doing

Evaluate potential system impacts. The very nature of a system or its parts may be against privacy in their intention.

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

2.2 Re-visit classic solutions

Search for existing solutions in the physical world or in old systems for the 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 solved in other "classic" settings. They may not always be re-usable, but sometimes transposing these solutions or their mental model may capitalize experience, minimize surprises and be more familiar to the subjects.

2.3 Openness

Systems should give user access to what they do, do it, and do nothing else. Help subjects 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 subjects, 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 subject or his client-part the list of variables which are required from the subject for operation (cf. infra. "Privacy razor"). User profile display 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 is unrealistic. Openness is a goal, and the *possibility* for the willing user to access his/her data in the system, not systematic notice.

Open source is a guarantee of transparency.
When system is another subject, transparency should be reciprocal.
System state should be accessible on demand as display, and as data.

2.4 Privacy razor

Subject 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.
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 severe 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 clarifying 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.

2.5 Third party guarantee

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

Using simultaneously three keys (subject, system, third party) enables transactions where each party can impeach the transaction, and where 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 subject's agreement, avoid direct identification of subject by system.

2.6 Make risky operations expensive

No system is 100% privacy safe. Subjects should be made aware of which operations are privacy-sensitive.
Operations identified as privacy-sensitive should be made costly for the system, the subject, the third party.

Genera design guideline, here also intended to make the operation costly and difficult to be done on a large scale by computer agents. Systematic cost (a few cents or small time delay), or mere obligation of tracing 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).

2.7 Avoid surprise

Subjects 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 subjects' action if it has influence on their state, and display major change of state. Traces of these acknowledgements should be recorded on system, and 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.

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 may be considered as such and solved in different 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-time record to legal systems. In case of doubt, be on the user's side.

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 stake-holders or their representatives as much as possible.

The designer's point of view is always limited. Most rules are social compromises. Explicit the trade-offs between privacy and other issues (e.g. reciprocity, emergency access, global security) and trace design choices for further discussion with stake-holders, or updates: new technologies may enable a better solution on the tradeoff.
Things change. New issues appear. Make sure subjects are empowered to feed-back and complaint by implementing the function in the interface.

3 Glossary:

In the EDC-PG guidelines:
“Activity” is the sequence of actions at stake in the interaction between subject and system.
“Subject” is a human physical entity (person, group), with a physical body.
“System” is the combination of material hardware and programmed software which are designed to provide services to faces, directly through the means of natural human body or through the use of devices.
“Device” is a physical artifact which may interact with the system.
“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.
“Display”: representation in a form directly affordable to the human senses.
“Server part” describes the part of system which is not carried by the user, seen from the user.
“Client part” is the part of the system which is carried by the user.
“User-face” is the subject as seen by the system.
“System-face” is the system as seen by the subject. These definitions may be relative : in a peer-to-peer system, a client may be seen as someone else’s server

4 Annex : OECD Guidelines, 1980-1998

OECD. Directorate for Science, technology and Industry. Committee for Information, Computer and Communication Policy. Working Party on Information Security and Privacy . 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. May 1999.

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 subject:

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.

3. Purpose Specification Principle
9The purposes for which personal data are collected should be specified not 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 change of purpose.

4. Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security Safeguards Principle

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

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.

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.

8. Accountability Principle

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