Evaluating Personal Data Control In Mobile Applications Using Heuristics

Patrice Pena
Userthink
patrice.pena@userthink.fr

Alain Giboin
UCA, INRIA, CNRS, I3S
alain.giboin@inria.fr

Karima Boudaoud
UCA, CNRS, I3S
karima.boudaoud@unice.fr

Yoann Bertrand
UCA, CNRS, I3S
yoann.bertrand@unice.fr

Fabien Gandon
UCA, INRIA, CNRS, I3S
fabien.gandon@inria.fr

***Abstract*—Allowing the users of mobile applications to control their personal data has become a key requirement. In the PadDOC project we studied the design of a mobile application intended to guarantee users the "exclusive control" of their personal data. We decided to use a heuristic evaluation method but we rapidly found that the criteria used were either too general or incomplete. As a result, we undertook to design a new set of heuristics which take this control activity into account, and which can be used by both usability specialists (HCI ergonomists) and computer scientists or engineers. This paper details the heuristics we designed together with the design method. It also reports the first test of the use of the criteria by a group of computer scientists, engineers and HCI ergonomists to evaluate a mock-up version of the PadDOC application. This test shows the benefits and limitations of the criteria.**

I. Introduction

Control of personal data refers to *"the claim of individuals* [we add: and groups] *to determine for themselves when, how, and to what extent information about them is communicated to others"* [8]. Allowing the users of mobile applications to control their personal data has become a key requirement, as reflected in claims of application users, application sellers, or application developers, such as: *"[We are witnessing] the shift towards people taking control of their data." —"Our personal data are precious — we must take back control." — "How to prevent abusive uses of our personal data, and how to keep the control of these data?" — "Personal data and privacy: How to take back control?" — "We [consumers, public] deserve more control over our data collected by companies." — "Consumers want to control how their data is used." — "[We want to] remain the masters of our personal data." — "Public concern about the use and management of personal data could be overcome if they were able to exert more control over how their data is used and by whom." — "Large companies are increasingly recognizing consumers' desire for more control and confidence over how their data is collected and used." — "New services are empowering consumers to take control of their own data." — "New mechanism makes Internet users take control of their personal data."*

Involved in a project aimed at designing a mobile application intended to guarantee users the "exclusive control" of their personal data–the PadDOC application– we were asked to assess that this control can be effectively performed. Having chosen to use a heuristic evaluation method to do this – i.e. a without-users evaluation method based on usability criteria called heuristics –, we found that the criteria used in the evaluation methods we identified were either too general or incomplete in terms of user's control activity. As a result, we undertook to design a new set of heuristics which take this control activity into account, and which can be used by both usability specialists (HCI ergonomists) and also computing scientists or engineers participating to the application development.

The paper is organized as follows: Section 2 presents the context of the present study; Section 3 discusses the related work; Section 4 describes the method we used to elaborate the heuristics together with the heuristics; Section 5 reports the test of the heuristics; and Section 6 concludes and discusses some perspectives.

II. II. Context: The PadDOC Project

The PadDOC project motivation was to simplify administrative and commercial transactions between customers and applicants through the use of a series of three secured devices: a mobile application called PadDOC (installed in the smartphone of the customer), a security key called PadKEY (installed in some interactive kiosk, at the applicant's premises), and a terminal called PadTERM (at the applicant's premises).

One of the PadDOC goals (and one of its main challenges) was to provide the users with the "exclusive control" of the storage, access to, and transfer of their personal data during their transactions. We will focus here on the customer's control activity in relation to the PadDOC application. Let's give a motivating scenario: Mrs Jones is about to rent an apartment.

Workshop on Usable Security and Privacy (USEC) 2021
7 May 2021, Auckland, New Zealand
ISBN 1-891562-73-8
https://dx.doi.org/10.14722/usec.2021.23008
www.ndss-symposium.org

She is in the premises of a real estate agent, facing a PadKey-connected kiosk. She has already noticed an apartment she likes. To set up her rental file, real estate Mr Smith asked her to provide him with a copy of various personal documents (e.g., identity documents) through the interactive kiosk. These personal documents being stored in a secured manner in Mrs Jones' PadDOC, she opens her application to carry out the transaction. She does it thanks the PadDOC user interface (see example in Fig. 1).

How can a customer like Mrs Jones control her personal data on PadDOC (and, more generally, on any mobile application)? What are the PadDOC design features (functionalities, graphical UI elements) proposed to her to control the transfer of her personal data? Do these features really help her to ensure this control? How to assess this? Which heuristics can be used? Could we use the existing ones or would we need to elaborate new heuristics? Let us start by considering the heuristics that exist.

III. Related Work

In this section we report a number of heuristics-based design frameworks, and related privacy frameworks, and discuss to what extent they allow to assess the control of personal data.

A. Nielsen's Framework and Similar Frameworks

Heuristic evaluation[1] is a method of evaluation without users of an application's user interface (UI). It is based on usability criteria called heuristics [11]. Heuristic evaluation involves one or more analysts walking through the UI, comparing the UI's design against the heuristics and noting if the UI complies with or violates the heuristics. Among the ten heuristics proposed by Nielsen [10,11,12][2], the user's control activity is explicitly mentioned in the heuristic User control and freedom. This heuristic is defined as follows: "Users often choose system functions by mistake and will need a clearly marked 'emergency exit' to leave the unwanted state without having to go through an extended dialogue. Support undo and redo." However this criterion is very generic. It does not refer specifically to the personal-data control activity of the user. This is also the case for the similar frameworks proposed by Bastien and Scapin [1], Shneiderman and Plaisant [14][13].

Among the eight ergonomic criteria for evaluating human-computer interfaces proposed by Bastien and Scapin [1][3], the user's control activity is explicitly mentioned in the Explicit Control criterion. This criterion "concerns both the system processing of explicit user actions, and the control users have on the processing of their actions by the system". It is decomposed into two sub-criteria: Explicit User Action and User Control. The sub-criterion Explicit User Action "refers to the relationship between the computer processing and the actions of the users. This relationship must be explicit, i.e., the computer must process only those actions requested but the users and only when requested to do so". The sub-criterion User Control "refers to the fact the users should always be in control of the system processing (e.g., interrupt, cancel, paus and continue). Every possible action by a user should be anticipated and appropriate options should be provided".

Among the ten golden rules of interface design proposed by Shneiderman and Plaisant [14][4] the user's control activity is explicitly mentioned in the rule Support internal locus of control. This criterion is defined as follows: "Allow your users to be the initiators of actions. Give users the sense that they are in full control of events occurring in the digital space. Earn their trust as you design the system to behave as they expect."

Among the six design principles proposed by Norman [13][5], the user's control activity is explicitly mentioned in the Mapping principle: "This [principle] refers to the relationship between controls and their effects in the world. Nearly all artifacts need some kind of mapping between controls and effects, whether it is a flashlight, car, power plant, or cockpit. An example of a good mapping between control and effect is the up and down arrows used to represent the up and down movement of the cursor, respectively, on a computer keyboard."

All the criteria mentioned above are very generic. They do not refer specifically to the personal-data control activity of the user. They should be specified in terms of personal data. Some steps have been taken in that direction.

B. Nielsen's Framework Adaptations

Concerning the adaptation of the Nielsen's method, we notice several strategies. Here are three of them. A first strategy is to complete the set of Nielsen's heuristics by adding a heuristic related to privacy concerns. Thus, Yáñez Gómez, Cascado Caballero, and Sevillano [15] have added the heuristic Privacy to the set of Nielsen. For the authors, how the users perceive the privacy has an impact on the adoption of mobile technology (the other bases being acceptance of technology, comfort, and capacity of personalization). The evaluator checks the compliance of this heuristic by asking the following questions: *Are protected areas completely inaccessible? Can protected or confidential areas be accessed with certain passwords? Is there information about how personal data is protected and about contents copyright?* User's activity control is not mentioned explicitly in these questions, but it can be inferred.

A second strategy consists in attaching to the Nielsen's set an additional set of heuristics dedicated to privacy concerns. Furano, Kushniruk, and Barnett [4] thus derived a set of eleven privacy specific heuristics for assessing personal health records

[1]Note that heuristic evaluation is one of the recommended methods in Usable Privacy and Security education (see, e.g. [3]).

[2]Visibility of system status; Match between system and the real world; User control and freedom; Consistency and standards; Error prevention; Recognition rather than recall; Flexibility and efficiency of use; Aesthetic and minimalist design errors; Help and documentation.

[3]Guidance; Workload; Explicit Control; Adaptability; Error Management; Consistency; Significance of Codes; Compatibility.

[4]Strive for consistency; Enable frequent users to use shortcuts; Offer informative feedback; Design dialogue to yield closure; Offer simple error handling; Permit easy reversal of actions; Support internal locus of control; Reduce short-term memory load.

[5]Visiblilty, Feedback, Constraints, Mapping, Consistency, Affordance.

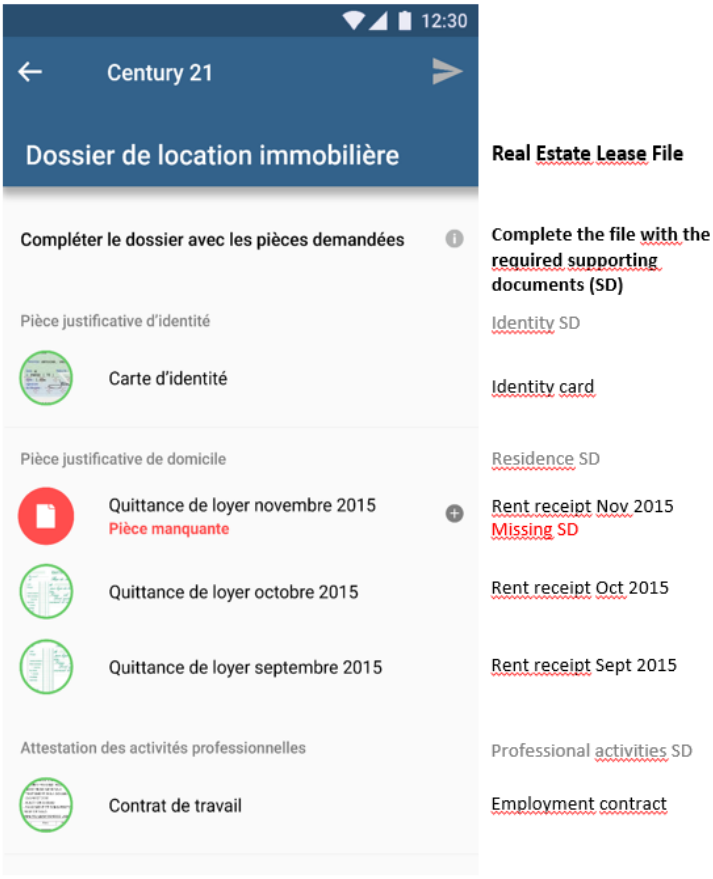

Fig. 1. Left: A screen of the PadDOC application showing the functionality "Complete the file with the required documents", and its corresponding graphical elements. Right: English translation of the screen textual items.

(PHRs) and health information systems (HISs). User's activity control is mentioned explicitly in heuristic 6 only: "The PHR contains a patient-controlled amendable privacy policy." But it can be inferred from the other heuristics (see, e.g., heuristic 3: "System provides a means for patients to specify consent directives in terms of access, use and disclosure of their PHI [protected health information]").

A third strategy consists in redefining the Nielsen's heuristics in terms of privacy/security. This was done for example by Yeratziotis, van Greunen and Pottas [16] with their seven heuristics. However, none of these heuristics refer explicitly to the control activity of the user. But again this activity can be inferred from the heuristics (see, e.g., heuristic 6: Errors–the system should provide users detailed security error messages that they can understand and act upon to recover). Note that this method has been used by Jamal and Cole (2009)[5] to evaluate the Facebook's advertising tool beacon.

C. Other Design Frameworks

The Structured Analysis of Privacy (STRAP) framework [6,7] offers eleven dedicated privacy heuristics intended for use by designers to evaluate the privacy vulnerability of interactive systems. Control activity is not mentioned explicitly in the heuristics. They mainly refer to mechanisms. However, the authors recommend taking into account the evaluation human factors in Bellotti and Sellen's [2] privacy heuristics reported below.

A second method is an adaptation made by Bellotti and Sellen [2] of the Questions, Options, Criteria (QOC) framework of MacLean et al. [9] to guide the privacy analysis process. Bellotti and Sellen proposed evaluating alternative design options based on eight questions and eleven criteria, derived from their own experience and from other sources. Bellotti and Sellen's criteria are similar to those of Heuristic Evaluation. User's activity control is mentioned explicitly in three of the eleven criteria: *Appropriate timing* ("Feedback should be provided at a time when control is most likely to be required"); *Flexibility* ("Mechanisms of control over user and system behaviors may need to be tailorable"); and *Meaningfulness* ("Feedback and control must incorporate meaningful representations"). The control activity may also be inferred from the other criteria (see, e.g., criterion *Fail-safety*: "The system should minimize information capture, construction and access by default").

TABLE I
PERSONAL-DATA CONTROL USABILITY CRITERIA

Criteria	Description
Control learnability	This criterion refers to the ease of use of the control mechanisms when the user is exercising personal data control for the first time
User efficiency in exercising the control	This criterion refers to the level of performance of the user when exercising personal data control
Control memorability	This criterion refers to how easy it is for the user to be efficient after a period of inactivity with the application
Control errors	This criterion refers to the number, criticity, and frequency of the errors made by the users when exercising control, and how easily the users fix the errors
Control usage satisfaction	This criterion refers to the level of transparency and of simplicity when using control mechanisms in the context of the main activity carried out by the user

D. Conclusion of Section III

The heuristics and criteria contained in the frameworks discussed above are either very generic–they do not apply specifically to the control of personal data, they are not contextualized–or they are incomplete–they do not reflect many control cases which could be encountered, or they are scattered. Generally speaking, they do not totally refer to the user's control activity. A contextualization, completion and bundling work should be necessary. The following two sections report our contribution to this work.

IV. DESIGN OF THE HEURISTICS

To design the heuristics, we started from the criteria identified in the existing frameworks. We have transposed these criteria (i.e. adapted them to the control of personal data) to obtain: (1) a definition of the acceptability of an application based on the communication of personal data; (2) a definition of usability criteria of personal-data control mechanisms, resulting in five control-oriented criteria (see Table 1); and (3) seven new heuristics of personal-data control, grouped into three categories (see Table 2). These heuristics have been operationalized resulting in sixty-five operational criteria (see Appendix).

Regarding the heuristic evaluation procedure to be provided to the analysts, it is similar to the original heuristic evaluation procedure [11].

To help the analysts apply the heuristics, we elaborated a checklist in the same way as the well-known Xerox checklist, i.e. in the form of a table. This table includes five columns: (1) a column *List of Control*, which describes the heuristics; (2) a column *Y[es]*, to be ticked by the evaluator if the application complies with the corresponding heuristic; (3) a column *N[o]* to be ticked if the application does not comply with the corresponding heuristic; (4) a column *N[ot]/A[pplicable]*, to be ticked if the heuristic does not apply; and (5) a column *Screen Name / Problem Description*, in which, if appropriate, the evaluator mentions the name of the screen currently evaluated, and specifies the heuristic-related problem.

TABLE II
THE SEVEN NEW HEURISTICS OF PERSONAL-DATA CONTROL

Categories	Heuristics
Personal-Data Control	1. Control of personal space 2. Control of Personal-Data communications and access 3. Control of user presence
Personal-Data Exposure Risk Prevention	4. Visibility of Personal-Data security and exposure 5. Exposure risk prevention
User Experience of Personal-Data Control	6. Easiness and smoothness of control 7. Accessibility and flexibility of control

V. TEST OF THE HEURISTICS

In this section, we report the preliminary test we performed to observe the applicability of the heuristics. This test has been realized in the context of the PadDOC project. Its goal was three-fold. It was to evaluate: (1) the usability of the control of personal data to the user of the PadDOC application; (2) the validity of the personal-data control criteria and their application to a use case; (3) the contribution of these criteria to a privacy-oriented design approach.

A. Method

1) Participants and Device to be Evaluated: The evaluation was coordinated by a senior HCI ergonomist, specialized in privacy/security, who was in charge of the protocol and the analysis of the results. Five evaluators with two different profiles (privacy/security expert computer scientists or engineers and privacy/security novice HCI ergonomists) have participated to the heuristic evaluation.

The device to be evaluated is a mock-up of the PadDOC mobile application. The heuristic evaluation was based on 17 static screens of the PadDOC application that correspond to the task scenarios described below.

2) Evaluation Protocol: Three task scenarios were proposed to the evaluators to inspect the device's user interfaces[6]: (1) Installing the PadDOC application on one's Android smartphone and creating one's user account; (2) Signing in to access to one's secured storage space; (3) Conducting a real estate rental transaction and communicating one's personal data requested in the legal context of the transaction.

First, the evaluator-coordinator asked the evaluators one at a time to unfold the three task scenarios and to think aloud, i.e., to verbalize what they see, what they understand and how they will carry out the tasks referred to in the scenarios (how they will interact with the device and with the other users). When complete, the evaluators and the evaluator-coordinator inspected again the device's user interfaces using the operational heuristics' checklist (allowing thus to validate

[6]Note that the protocol was preliminarily tested by another senior HCI ergonomist, who was privacy/security experienced. The protocol was improved after this testing step.

or not these heuristics). During this inspection step, the evaluators (one at a time) and the evaluator-coordinator analyzed the problems they identified and made recommendations for improving the user interfaces.

Second, after every evaluator has completed the evaluation, the evaluator-coordinator:

- awarded to each evaluator, and for each general heuristic, a score on a standard grid worth up to 100; this score is computed as follows: for each evaluator and each general heuristic, one point is awarded for each ticked corresponding operational heuristic; the points are added up to obtain a raw score (e.g., for the general heuristic "Control of communication", $Comp\_1$ obtained a score of 8); the raw score of each evaluator is then converted into the corresponding standard score (a percentage): a score of 100 means that all the operational heuristics attached to a general heuristic have been ticked, a score of 50 means that half the operational heuristics have been ticked, a score of 0 means that no operational heuristics have been ticked;
- analyzed and categorized the identified problems in terms of severity level: (a) Minor problems: problems without affecting the security/privacy of personal data; (b) Major problems: problems detrimental to the use of personal data but not detrimental to the security/privacy of these data; (c) Critical problems: problems affecting the security/privacy of personal data — blocking the use of personal data — prohibiting the user from controlling one's personal data;
- finalized the recommendations against the device's and the project's objectives and constraints.

B. Results

Applying the criteria of personal data control allowed finding thirty different problems of usability of personal-data control mechanisms. In view of the status of the mock-up, two general heuristics could not be evaluated: *Control of User Presence*, and *Accessibility and Flexibility of Control*. In the end, the evaluation applied to the five other general heuristics: *Control of Personal and Shared Spaces*, *Control of Personal Data Communications and Access*, *Exposure Risk Prevention*, and *Easiness and Smoothness of Control*.

1) Overview: Applying the criteria of personal data control allowed each evaluator to find control problems for each general heuristic. Fig. 2 provides an overview of the problems found by each evaluator for each general heuristic. Number of Problems found by Evaluator's Profile

In view of the number of screens inspected by the evaluators, a fairly high number of problems have been found by each evaluator (see Table III). Nevertheless, if several and similar problems were found by the different evaluator profiles, the computer researchers and engineer who were security/privacy experts found more specific and critical problems than the ergonomists who were security/privacy novices.

2) Result Distribution by Level of Severity: Applying the data control heuristics allowed to find a lot of critical control problems exhibiting a risk of control flaw for the user, and a lot of minor control problems more strongly linked to control exercise's use of comfort. However, few minor problems were found (see Table IV).

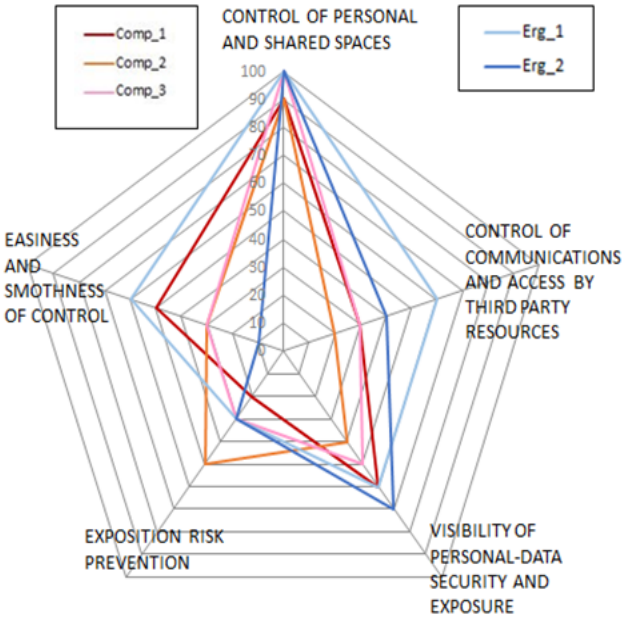

Fig. 2. Non compliances to heuristics found by the computing scientists and engineers ($Comp\_1$, $Comp\_2$, $Comp\_3$), and by the ergonomists (Erg_1, Erg_2) participating to the test

TABLE III
NUMBER OF PROBLEMS FOUND BY EVALUATOR'S PROFILE

Participant's Profile	Number of Identified Problems
$Comp\_1$	21
$Comp\_2$	23
$Comp\_3$	22
Erg_1	14
Erg_2	19

3) Result Distribution by Severity Level and by General Control Heuristic: In the case of the PadDOC project, applying personal-data control heuristics allowed showing that critical problems exist from the point of view of (see Table V, column "Critical"):

- The control of communications and access to third-party resources, including the fact that the device does not enough communicate on the mid-term and long-term outcome of the personal data transmitted in the context of the transactions.
- The risk prevention, including the fact that the user interfaces do not encourage enough the user to adopt a secure behavior, notably at the moment of creating a secured password.

TABLE IV
RESULT DISTRIBUTION BY LEVEL OF SEVERITY

Participant's Profile	Number of Identified Problems
Critical	11
Major	4
Minor	15
TOTAL	30

TABLE V
RESULT DISTRIBUTION BY SEVERITY LEVEL AND BY GENERAL CONTROL HEURISTIC

	Critical	Major	Minor
Control of Personal Spaces and Sharing Spaces	0	0	1
Control of Personal-Data communications and access	4	3	1
Visibility of Personal-Data security and exposure	0	0	8
Exposure risk prevention	4	0	0
Easiness and smoothness of control	3	1	5
TOTAL	11	4	15

- The easiness and smoothness of the control, notably at the moment of installing the application and of creating a user account, the form not being very engaging and not respecting some good practices.

Major and minor problems were found (see Table V, columns "Major" and "Minor"), which highlight the fact that the user interfaces provide the user with little contextual information, and do not display enough the security state of personal data and interactions. If this information is not essential from the security point of view, it is however crucial from the point of view of the user and of the level of trust she can play to the device when she is solicited to transfer her personal data.

From the users' point of view, applying the personal-data control heuristics thus allows identifying problems of usability of control mechanisms at the level of (see Table VI): (1) the information provided by the device to the user to account for the security state of the interactions and for the perception and visibility of security; (2) the resources made available by the device to encourage the user and to guide her to exercise control; (3) the workload required to learn and exercise the control when creating a user account and installing the application and during the interactions; (4) the security of data through criteria of security related to confidentiality, authentication, and access control; and (5) the user experience related to control exercise and its integration from the usage point of view.

TABLE VI
LEVELS OF EVALUATIONS OF PERSONAL-DATA CONTROL BY THE USER

Evaluation Level	Description
Informational	Feedback on the visibility of security, of the environments' security state, and of the exposure of personal data. Visibility / Perception of security. Contextual information useful in the context of interactions.
Resources	Resources made available by the device to make progress in exercising the control (education, sensitization to the exercising of control).
Workload	Ease of exercising control, of using mechanisms of personal data control and securing Ease of creation, memorability and recall of memory authentication factors
Security	User's ability to protect one's data (confidentiality, authentication, access control) Level of control guaranteed by the application
Usage Integration	Integration of the control within the usage

VI. DISCUSSION AND CONCLUSION

The existing sets of privacy heuristics being limited in terms of personal-data control activity, we sought to elaborate a new set of heuristics that better reflect this activity and its various dimensions, and that allows to assess that this activity is supported by a mobile application. From an analysis of existing frameworks, we proposed a set of seven general heuristics and operationalized them into sixty-five more specific heuristics. We have also proposed a typology of users and a typology of personal data in order to tailor the heuristic to: (a) the users' attitudes and behaviors toward personal data control, and (b) the nature of personal data.

Only heuristics were tested, being applied to PadDOC, a mobile application that allows the user to store and transfer her personal data in the context of secured administrative or commercial transactions. This test involved on the one hand two computing scientists and one computing engineers, who were privacy/security experts, and, in the other hand, two HCI ergonomists, who were privacy/security novices. This test aimed at determining the degree of relevance of the heuristics. We will now discuss some of the benefits and limitations of the heuristics, and of the corresponding heuristic method, and also of the testing method. We will then conclude on some perspectives to overcome the limitations and to explore new avenues.

a) Benefits: At a general level, the heuristics allowed covering more dimensions of the data control activity. At a more specific level: the operationalized heuristics allowed the evaluators to analyze the user interface in more details; the checklist allowed to collect more systematically the problems met during the inspection of the user interface; the illustrations of the heuristics, by linking the definitions of the heuristics

with the corresponding interface elements, allowed the evaluators to better understand the heuristics

b) Limitations: At a general level, the connection between the heuristics and the control activity is not complete, especially because we did not rely on a strictly speaking model of the activity of personal data control, but on existing heuristics. At a more specific level: the proposed checklist was a paper-and-pencil form, which does not allow, e.g., to develop comments; the proposed heuristics illustrations are static, not permitting always to well understand the underlying user interactions; the quality of the heuristic analysis strongly depending on the level of privacy/security expertise of the evaluators, this level was unbalanced between computing researchers and engineers, and HCI ergonomists; the test was performed with an incomplete mock-up; the tailoring of the heuristics to the user type and personal data type was not performed.

c) Perspectives: To overcome the limitations above, and to explore new avenues, several perspectives may be envisioned:

- Additional tests need to be performed, including the following variants: (a) making the evaluators achieve the first step of the evaluation without the evaluator-coordinator; (b) involving computing scientists or engineers who are privacy/security novices, and HCI ergonomists who are privacy/security experts; (c) evaluating a prototype or a product.
- The checklist could be computerized, allowing for example to connect more directly the checking to the corresponding application' screens.
- Customization procedure with respect to user types and personal data types should be defined and tested.
- The tailoring in terms of user types and personal data types could be complemented by: (a) a tailoring in terms of experienced situation – e.g., a Controller can prove less picky in a situation where he will find there is nothing to be afraid of; (b) a tailoring in terms of stakeholders, who are not owners of the data, but users – e.g., the applicants in the case of PadDOC; (c) a tailoring in terms data pirats or privacy pirats – the focus being here on the indue control taking by the pirats.
- The set of heuristics may be used as a grid for analyzing the results user testing of a mobile application. This would be an additional test of the relevance of the heuristics, and also a source for elaborating new heuristics.
- The present set of heuristics could be confronted with, and/or additional heuristics could be elaborated from a strictly speaking model of the activity of personal data control.

ACKNOWLEDGMENT

The PadDOC project was funded by the French "Fonds Unique Interministériel" (FUI) AAP16.

REFERENCES

[1] Bastien, J.M.C., Scapin, D.L., "Evaluating a user interface with ergonomic criteria", *International Journal Human Computer Interaction 7(2)*: 105-121, 1995

[2] Bellotti, V. and Sellen, A., "Design for privacy in ubiquitous computing environments". In *Proceedings of The Third European Conference on Computer Supported Cooperative Work (ECSCW'93)*, Milan, Italy: Kluwer Academic Publishers, 1993.

[3] Cranor, L., Hong, J., and Reiter, M.,"Teaching Usable Privacy and Security: A guide for instructors". Last updated 6 January 2007. Available at: http://cups.cs.cmu.edu/course-guide

[4] Furano, R.F., Kushniruk, A, Barnett, J., "Deriving a Set of Privacy Specific Heuristics for the Assessment of PHRs (Personal Health Records)", in F. Lau et al. (Eds.), *Building Capacity for Health Informatics in the Future*, IOS Press, 2017, pp125-130

[5] Jamal, A., Cole, M., "A Heuristic Evaluation of the Facebook's Advertising Tool Beacon", in *Proceedings of the 1st International Conference on Information Science and Engineering (ICISE2009)*, IEEE, 2009, pp1527-1530.

[6] Jensen, C., "Toward a method for privacy vulnerability Analysis", in *Proceedings of CHI 2004, Extended abstracts on Human factors in computing systems*, ACM, pp1563, 2004.

[7] Jensen, C., Potts, C., "Experimental evaluation of a lightweight method for augmenting requirements analysis", in *WEASELTech '07: Proceedings of the 1st ACM international workshop on Empirical assessment of software engineering languages and technologies*: held in conjunction with the 22nd IEEE/ACM International. Conference on Automated Software Engineering (ASE), 2007.

[8] Lazaro, Ch. Le Métayer, D., "Control over Personal Data: True Remedy or Fairy Tale? *SCRIPTed", A Journal of Law, Technology Society, 12 (1)*, 2015, pp3-34.

[9] MacLean, A., Young, R. M. ,Bellotti, V. , Moran, T. P., "Questions, options, and criteria: Elements of design space analysis", *Human-Computer Interaction (HCI) Journal 6(34)*, 1991, pp. 201–250.

[10] Nielsen, J., *Usability Engineering*, Toronto, ON: Academic Press, 1993.

[11] Nielsen, J., "Heuristic evaluation". *Usability inspection methods, 17(1)*, 1994, pp 25-62.

[12] Nielsen, J., *Designing Web Usability*. Berkeley, CA: New Riders Publishing, 2000.

[13] Norman, D. A., *The design of everyday things*. Revised and expanded edition. Basic books, 2013.

[14] Shneiderman, B., Plaisant, C., *Designing the User Interface - Strategies for Effective Human-Computer Interaction*, 5th Edition. Addison-Wesley, 2010, pp. I-XVIII, 1-606.

[15] Yáñez Gómez, R., Cascado Caballero, D., and Sevillano, J.-L., "Heuristic Evaluation on Mobile Interfaces: A New Checklist", *The Scientific World Journal*, Volume 2014, 1-19.

[16] Yeratziotis, A. van Greunen, D., Pottas, D. "A Framework for Evaluating Usable Security: The Case of Online Health Social Networks", in *Proceedings of the Sixth International Symposium on Human Aspects of Information*, 2012.

VII. APPENDIX: THE SET OF HEURISTICS

Table VII below gathers our seven general heuristics of personal-data control (grouped into three categories), and their corresponding operational criteria.

TABLE VII
THE HEURISTICS OF PERSONAL-DATA CONTROL

A. PERSONAL-DATA CONTROL	
1. Control of Personal Space	
Secure Personal Space	The system provides a secure personal space dedicated to the storage of personal data
Confidentiality of Personal Space	In the personal space, personal data are not shared
Unique access	Only the user has the right to access to the personal space
Availability of personal data	Personal data are always available in the personal space
Private sharing space	The system provides a secure and confidential sharing space dedicated to the communication of personal data
Intentional action of sharing	Personal data are shared in the private sharing space following a deliberated action of the user
Controlled access to private sharing spaces	The accesses to sharing spaces are protected by an authentication mechanism (password or token for example)
Administration of personal and private sharing spaces	The user is the administrator of her/his personal space and the sharing space: (1) the access to the personal space and personal data is controlled by the user ; (2) the user can add or delete personal data
Security of public spaces	In case of use of a public equipment, a space is reserved to protect the user from physical intrusions and access attempts to the user's screen

3. Control of User Presence	
Control of the presence or availability of the user	The user can control efficiently the display of her presence or availability regarding other users and indicate for example to the other users that she/he does not want to be disturbed at a certain time
Optimal presence and availability of the user	The presence and availability of the user is optimal : she/he is not isolated from the system or other users or exposed without being aware
Availability of the service	The service or a part of the service provided by the system is functional if the user does not share any personal data
Control of notifications and communication channels	The user can control the communication channels and the notification systems: the user controls the reception of for example emails, SMS, notifications, newsletters sent by the system
Blocking of undesirable applicants, other users or certain users	The system allows the user not to be contacted by other applicants, users or certain users

2. Control of Personal-Data Transmission and Access	
Control of personal data to be transmitted	The user filters the personal data to be transmitted : she/he can select the data that she/he would like to communicate and can decide to not share the data that she/he would like to keep confidential
Control of final applicants	The user can choose the applicant(s) according to the usage context and control to whom the personal data will be transmitted
Control of read access rights	The user controls the read access right of the applicants of the personal data that she/has shared
Control of the communication context of personal data	During the sharing of personal data, the system inform and remember the user the usage case and the reason why personal data are required and transmitted
Control of the granularity level of personal data	The user can select the granularity level of the personal data to be transmitted: in the case of geolocalisation data, the user can select the city where she/he lives without revealing her exact address or filter certain personal data contained in the documents such as filtering the amount of an invoice when providing a proof of address
Control of the visibility of the user activity	The system allows the user to manage the visibility of her activity : she/he can for example restrict the visibility of the actions she/he has done on a social platform or decide to not authorise the browser to access to the navigation history
User confirmation	The system requires from the user an authorisation each time it communicates her personal data or activates external resources: the system does not access or transmit personal data without a confirmation from the user. For example the system requires a confirmation from the user if an application would like to access to geolocalisation data or activate Bluetooth of the smartphone
Control of the systematic geolocalisation	The user can refuses that an application geolocates her/him systematically
Control of access rights to private sharing spaces	The user administers the access rights of the applicants to the private sharing spaces
Control of read access rights	In the private sharing space, the user administers the applicants' read access rights
Bidirectional control	The control is bidirectional: it is applied on outgoing personal data from the personal space and available in the sharing space and on ingoing accesses to the sharing space
Control of indirect access	The user can interrupt the indirect accesses to personal data
Access control to external resources	The user can deactivate the accesses to external resources: for example, access to her/his smartphone contacts, camera, or NFC
Respect of the legal and social framework	The collection and processing of data respect the social and legal framework

B. PERSONAL-DATA EXPOSURE RISK PREVENTION	
4. Visibility of Personal-Data Security and Exposure	
Data collection warning	The system informs the user each time the system collects personal data or access to third-party resources
Display of required data	The system informs the user and presents explicitly the data required and used by the system
Display of the history	The system displays the history of the transactions carried out with personal data
Display of shared data	The system displays the list of personal data shared with applicants
Display of the external resources used by the system	The system displays the list of external resources that it uses
Confidence indicator	The system informs the user about the confidence level regarding the external resources: files, data, URLs, other users, applicants, etc.
Notification of the security state regarding the personal or private sharing space	The system informs the user about the current security level of her/his personal space by providing for example an information on the security level of her/his password
Iconography	The system uses explicit metaphors to signal a usage risk of the system or absence of risks in a secure environment such as the use of padlock or safe box
Visibility of personal information	The user distinguishes easily her personal information from the other users' or system's information
Display of indirect access	The system displays the list of indirect access to the personal data of the user: commercial partners, third-party, other users, etc.

5. Exposure Risk Prevention	
Implicit control	By default, the system ensures personal data confidentiality and transmission without requiring actions from the user such as ciphering of data or the user of HTTPS. The control is implicit for the user
Alarm	The system informs the user if the system is not secured about an usage risk for example when the browser detects that the connection is not secured and/or that a web site uses an invalid certificate
Protection help	The system incites and helps the user to create a unique secure password, using capital and lowercase letters, numbers, special characters, and unrelated with personal elements such as surnames or family birthdays
Assistance to strong authentication	The system guides and assists the user to increase the security level of the personal space: for example by asking the mobile phone number to ensure a strong authentication
Risks awareness	On a platform dedicated to privacy and security of data as a web site for example, the system informs the user about existing threats and risks and make her/him aware about the protection of personal data
Retrieval of personal data	The system sets up protocols to help the user in case of theft of personal data, loss or damage of supports, identity spoofing, etc.
Final confirmation	The system asks the user to authenticate again to perform certain sensitive actions
Automatic disconnection	The system disconnects automatically if no action is performed by the user

C. USER EXPERIENCE OF PERSONAL-DATA CONTROL	
6. Easiness and Smoothness of Control	
Execution rapidity	The control of personal data can be rapidly done and requires few actions from the user
Minimal workload	The workload due to the control of personal data is reduced
Simplicity of control mechanisms	The control mechanisms of confidentiality of personal data and authentication modes of the system can be used easily and do not constrain the user to bypass them: the user should not write her/his password on a post-it for example or should not use a password that has already been used
Integration of control mechanisms	The control mechanisms are adapted and integrated to the context of the user and of her/his interactions: the system offers control mechanisms to the user only when interactions require a control action from her/him
Optimal control	Control of personal data and the control level are optimal regarding the experience of the user: control of personal data does not penalise the experience of the user and does not affect the principal activity of the user or the quality and fluidity of the interactions
Save settings	The system does not systematically ask the user if she/he can access external resources each time they are used: the response is saved as a setting and the user can modify this setting later
Overview of state changes	In case of parameter settings (confidentiality, security or sharing of personal data), the system informs the user about the state changes on the exposure of her personal data or about the security of the system
Surface representation of the control	The surface elements such as dialogue boxes, messages, labels, buttons, icons help the user to take the right decisions and do the right control actions according to her/his usage context
Surface representation of the control	The surface elements such as dialogue boxes, messages, labels, buttons, icons help the user to take the right decisions and do the right control actions according to her usage context
Configuration of the control settings	The setting part of the system has a section "privacy / personal data" that displays all the accesses to personal data and gathers all the control mechanisms applied to personal data

7. Accessibility and Flexibility of Control	
Accessibility of the control and authentication mechanisms	The authentication and control mechanisms on personal data are accessible to users having a visual, physical, cognitive or sensory disability
Usage conditions of the control mechanisms	In the case of mobile devices, the control mechanisms must be usable all the time depending on the context of use, i.e.: light too low, dazzling light, sound too high, difficulty to concentrate in public environments, etc.
multi-support and multi-versions control exercise	The control of personal data is done on all the supports and versions of the system
Flexibility of the control	The system offers expert users configuration menus, tools, and advanced information
Legal conditions of the collection and processing of personal data	The system has specific sections for the conditions of usage, collection, processing, storage and transmission (to third-parties) of personal data
Accessibility of the legal usage conditions of personal data	The usage conditions are accessible and adapted to the expertise level of the users: the general usage conditions are understandable, the vocabulary is adapted and does not use techno-legal jargon
Readability of the legal usage conditions of personal data	The general usage conditions are readable and the user find easily the information she/he is looking for: the text is short and structured (title, sub-title, text-body), display of the text on light background, sober colour of the text, size of the characters adapted to the supports, typography without serif, text column adapted.
Readability of the legal usage conditions of personal data in mobility	The display of the general usage conditions is adapted to mobile supports
Modification of the legal usage conditions of personal data	The system informs the user about any change in collection and usage conditions of personal data