Heuristics for Assessing the Effective Control of Personal Data by Mobile Applications' Users

Patrice Pena, Yoann Bertrand, Alain Giboin, Fabien Gandon, Karima Boudaoud

Heuristics for Assessing the Effective Control of Personal Data by Mobile Applications' Users

Patrice Pena
UCA, CNRS, I3S, Inria
930 Route des Colles
06903 Sophia Antipolis Cedex, France
patrice.pena@inria.fr

Alain Giboin
Inria, UCA, CNRS, I3S,
930 Route des Colles
06903 Sophia Antipolis Cedex, France
alain.giboin@inria.fr

Karima Boudaoud
UCA, CNRS, I3S, Inria,
930 Route des Colles
06903 Sophia Antipolis Cedex, France
karima.boudaoud@unice.fr

Yoann Bertrand
UCA, CNRS, I3S, Inria,
930 Route des Colles
06903 Sophia Antipolis Cedex, France
yoann.bertrand@i3s.unice.fr

Fabien Gandon
Inria, UCA, CNRS, I3S,
930 Route des Colles
06903 Sophia Antipolis Cedex, France
fabien.gandon@inria.fr

Abstract
The goal of this paper is to present a new set of seven heuristics to overcome limitations of existing sets of privacy heuristics in terms of personal-data control activity. These heuristics have been operationalized into sixty-five more specific heuristics to reflect personal-data control activity and its various dimensions and to assess effective control of personal data. Heuristics were tested, being applied to a mobile application called "PadDoc" that allows users to store and transfer their personal data in the context of secured administrative or commercial transactions.

Author Keywords
Privacy; Usability; Heuristic evaluation; Interaction Design; Human Computer Interaction.

ACM Classification Keywords
H.5.2 User Interfaces: Ergonomics; Evaluation/methodology; User-centered design.

1. Introduction
Allowing the users of mobile applications to control their personal data has become a key requirement. In the context of a project called PadDOC, we studied the design of a mobile application intended to guarantee users the control of their personal data. We decided to

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.

Table 1. Personal-data Control Usability Criteria

use an existing heuristic evaluation framework but we rapidly found that the framework's criteria were either too general or incomplete in terms of control activity. As a result, we undertook to design a new set of heuristics better taking this activity into account.

This paper is organized as follows: Section 2 presents briefly the limitations we have seen to existing frameworks; Section 3 describes the method we used to elaborate the heuristics together with their procedure of use; Section 4 reports a preliminary test of the heuristics; and Section 5 concludes and discusses some perspectives.

2. Related Work

We analyzed the following heuristics-based and related privacy design frameworks in order to determine to what extent they allow to assess the control of personal data: ■*Nielsen's Framework and Similar Frameworks* (Nielsen (1993, 1994, 2000)[1,2,3]; Bastien and Scapin (1995)[4]; Shneiderman and Plaisant (2010) [5]; Norman (2013) [6]); ■*Nielsen's Framework Adaptations to privacy concerns* (Yáñez Gómez, Cascado Caballero, and Sevillano (2014)[7]; Furano, Kushniruk, and Barnett (2017)[8]; Yeratziotis, van Greunen and Pottas (2012)[9]); ■*Other Design Frameworks* (*(1) Heuristics-based Framework:* Jensen (2004), Jensen & Potts (2007)[10,11]; Bellotti and Sellen (1993)[12]; *(2) Privacy-by-design (Technical) Framework:* Cavoukian (2009)[13], Cavoukian and Weiss (2012)[14]; Craggs and Rashid (2017) [15]); and ■*Frameworks Not Dedicated to Design* (*(1) Legal Framework:* Warren and Brandeis (1870) [16]; *(2) Political Framework:* Westin (1967) [17]; Palen and Dourish (2003) [18]; *(3) Psychological Framework:* Altman (1976) [19])

From this analysis, we concluded that the heuristics and criteria proposed in the frameworks are either very generic–they do not apply specifically to the control of personal data, they are not contextualized–or that 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.

2. Design of the Heuristics

To design the heuristics, we started from the criteria identified in the existing frameworks. We have transposed these criteria 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[1].

Regarding the heuristic evaluation procedure to be provided to the analysts, it is similar to the original heuristic evaluation procedure (Nielsen, 1994) [2].

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

[1] http://users.polytech.unice.fr/~karima/conferences/heuristics.pdf

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

Table 2. The seven new heuristics of Personal-Data control (grouped into three categories)

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.

3. Test of the Heuristics

The preliminary test aimed to determine the applicability of the heuristics has been performed in the context of the PadDOC project. The goal was to evaluate: (1) the usability of the control of personal data given to the user of the PadDOC mobile 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.

3.1. 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 separately 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.

3.2. Evaluation Protocol

Three task scenarios were proposed to the evaluators to inspect the device's user interfaces: (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 by *thinking aloud* their interaction with the device. Once the tasks completed, the evaluators and the evaluator-coordinator inspected again the device's user interfaces using the operational heuristics' checklist, allowing thus to validate 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; the raw score of each evaluator is then converted into the corresponding standard score (a percentage)
- 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

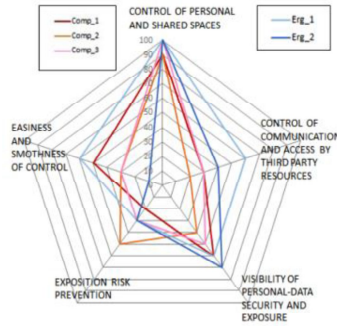

Figure 1. Non compliances to heuristics found by computer scientists and engineers, and by ergonomists

Heurist.	Crit.	Maj.	Min.
A	0	0	1
B	4	3	1
C	0	0	8
D	4	0	0
E	3	1	5
Tot.	*11*	*4*	*15*

Table 3. Result distribution by severity level (Critical, Major, Minor) and by general control heuristic (A = Control of Personal Spaces and Sharing Spaces, B = Control of Personal-Data communications and access, C = Visibility of Personal-Data security and exposure, D = Exposure risk prevention, E = Easiness and smoothness of control)

of personal data | prohibiting the user from controlling one's personal data};

3.2. Results

Applying the criteria of personal data control allowed finding thirty different problems of usability of personal-data control mechanisms. The evaluation applied to five general heuristics (see Figure 1 and Table 3). Figure 1 provides an overview of the problems found by each evaluator for each general 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 3, 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;
- 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 3, 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 allows identifying problems of usability of control mechanisms at the level of: (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.

4. Discussion and Conclusion

In this paper, we proposed a new set of heuristics to overcome limitations of existing frameworks. These heuristics allowed covering more dimensions of the data control activity and the operationalized heuristics allowed the evaluators to analyze the user interfaces in more detail. The main limitation of these heuristics is that the quality of the heuristic analysis depends strongly on the level of privacy/security expertise of the evaluators. To overcome these limitations, additional tests need to be performed: (a) making the evaluators achieve the first step of the evaluation without the evaluator-coordinator; (b) involving privacy/security novice computing scientists/engineers and privacy/security expert HCI ergonomists; (c) evaluating a prototype or a product.

5. Acknowledgments

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

References

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

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

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

[4] Bastien, J.M.C., Scapin, D.L. (1995). Evaluating a user interface with ergonomic criteria. *Int. J. Hum. Comput. Interaction 7(2)*: 105-121.

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

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

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

[8] Furano, R.F., Kushniruk, A, & Barnett, J. (2017). 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, 125-130.

[9] Yeratziotis, A. van Greunen, D., & Pottas, D. (2012). A Framework for Evaluating Usable Security: The Case of Online Health Social Networks. *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012)*, 97-107.

[10] Jensen, C. (2004). Toward a method for privacy vulnerability Analysis. In *Proceedings of CHI 2004, Extended abstracts on Human factors in computing systems*, ACM, 1563.

[11] Jensen, C., & Potts, C. (2007). 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).

[12] Bellotti, V. and Sellen, A. (1993). 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.

[13] Cavoukian, A. (2009) *Privacy by design, the 7 foundational principles*. [Revised: January 2011]. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[14] Cavoukian, A., & Weiss, J.B. (2012). *Privacy by Design and User Interfaces: Emerging Design Criteria – Keep it User-Centric*, Information and Privacy Commissioner Paper, 12 p.

[15] Craggs, B., & Rashid, A. (2017). Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design. *In Proceeding of the 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, Buenos Aires, Argentina, 22-25.

[16] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review 4(5)*, 193-220.

[17] Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59 (2)*, 431-453.

[18] Palen, L., & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, 129-136.

[19] Altman, I. (1976). Privacy. A Conceptual Analysis. *Environment and Behavior 8(1)*, 7-30.