Multi-modal User Interface Design for a Face and Voice Recognition Biometric Authentication System

Ilia Adami, Margherita Antona, and Emmanouil G. Spanakis(✉)

Institute of Computer Science, Foundation for Research and Technology - Hellas, 71110 Heraklion, Crete, Greece
{iadami,antona,spanakis}@ics.forth.gr

Abstract. Biometrics refer to unique measurable characteristics and information regarding individual's health, physical or mental condition and can be used to uniquely authenticate or verify a person's identity. They can be sorted in physiological such as fingerprints, palm print, face recognition, iris recognition, retina and DNA and behavioral such as typing rhythm (i.e. signature) and voice and can be described based on the uniqueness, potential change with time (i.e. facial changes), the feasibility to be collected (i.e. fingerprints) and the purposes of usage. In this work we study the use of a biometric technology for eHealth. We present the SpeechXRays project initiative that aims to provide a solution combining the convenience and cost-effectiveness of face and voice biometrics, achieving better accuracies by combining it with video, and bringing superior anti-spoofing capabilities. We explain how a novel user interface biometric platform is designed and adapted, for an eHealth use case, to enable secure access for medical specialists, nurses and patients to a collaborative eHealth platform that provides access to clinical and health related data within and possible outside a hospital. This is the first study, in the field, that gathered all necessary requirements (for a voice/face biometric system) and provides a formative evaluation and implementation of the SpeechXrays system user interface, for both end users and administrators, following a user-centered design approach, based on the holistic consideration of the user experience and the technical implication and functional requirements of the platform.

Keywords: Biometric authentication/verification · Voice · Acoustic User interface design · Heuristic/guidelines · Smartphone · Mobile Internet of things · Personal health systems · eHealth/mHealth

1 Introduction

Biometrics refers to the automated recognition of individuals based on biological (i.e., face, fingerprint, iris, voice, DNA, etc.) or behavioural traits (i.e., keyword dynamics, signature, gait, etc.) [13]. Biometric authentication is a natural alternative to traditional authentication systems like password schemes and secure electronic identification cards that promises increased security and user convenience [1]. A typical biometric authentication involves two stages, the enrolment stage and the verification stage.

P. Perego et al. (Eds.): MobiHealth 2017, LNICST 247, pp. 171–181, 2018.
https://doi.org/10.1007/978-3-319-98551-0_20

During the enrolment, the system acquires a biometric trait of an individual (i.e., iris, fingerprint, face, voice, etc.), extracts a specific feature set from it and stores it in a database as a template. It then assigns an identifier associating the created template with an individual. During the verification stage, the system once again acquires the biometric trait of an individual, extracts a feature set from it, and compares it against the templates that are stored in the database in order to verify the claimed identity [11].

SpeechXRays aims to develop and test, in real-life environments, a user recognition platform based on voice acoustics analysis and audio-visual identity verification. The vision is to combine and pilot two multi-channel biometrics techniques: acoustic driven voice recognition (using acoustic and not statistical only models) and dynamic face recognition. SpeechXRays aims to outperform current state-of-the-art solutions in the areas of *Security*: high accuracy solution, *Privacy*: biometric data stored in the device, *Cost-efficiency*: use of standard embedded microphone and cameras (smartphones, laptops) and most importantly ***Usability***: text-independent speaker identification (no pass phrase), low sensitivity to surrounding noise and state of the art **User interface design** for user interaction. Usability evaluation will be performed during the pilot of the two multi-channel biometrics techniques: ***acoustic driven voice recognition*** (using acoustic and not statistical only models) and ***dynamic face recognition*** in the project use cases involving 2000 users in 3 pilots: a *workforce*, an *eHealth* [23, 24] use case and a *consumer use case*. This paper describes the activities concerning the design, formative evaluation and implementation of the SpeechXrays system user interface, for both end users and administrators, following a user-centered design approach, based on the holistic consideration of the user experience and the technical implication and functional requirements of the platform. We present the methodology followed for the design of the user interfaces of the SpeechXRays system based on general usability and user interface requirements, as well as specific use cases requirements [22]. Based on this analysis several UI prototypes were designed and assessed following a formative usability evaluation approach. A mock up system was created to guide user interface development and integration to support UI adaptations as required by the SpeechxRays verification framework. Figure 1 presents the user interaction for the verification of medical personnel, for management of sensitive medial data such as medical information for patients, in the eHealth use case. We present a novel interface design methodology for interactive biometrics applications, taking into consideration all complex functional biometric processes and parameters, such as the scope/goal of the application, the functional and non-functional user requirements, the profile of the targeted end-users, the device type it will be served from, the context of the application (inside a hospital) and the interaction modes (touchscreen vs traditional mouse and keyboard), etc.

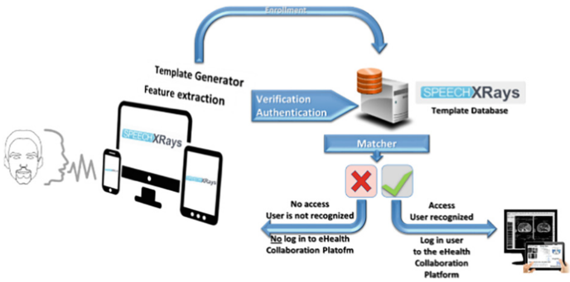

Fig. 1. SpeechXrays workflow for eHealth scenario

2 Design Methodologies and Results

Designing user interfaces for interactive systems in general is a complex process that has to take into consideration many parameters, such as the scope of the end application, its target audience, the functional and non-functional requirements, and the interaction mode (keyboard and mouse, touch, voice, gestures, etc.). In this paper we argue that traditional design guidelines and standards are not adequate, and thus, we focused our work on expanding existing lists with new guidelines to cover emerging interaction requirements for biometric authentication. Similarly, even though we have evidence for the creation of heuristics – for user interface design – in many different domains (robotics, virtual worlds, multimodal mobile applications, Smartphones, etc.), it seems that none of these is biometric related. Quiñones and Rusu [12] presented an extensive literature review conducted from 2006 till 2016 and identified 68 such domains, but none is related to biometric authentication – as described in SpeechXRays project. Even though recent research has shown that usability and reliability play an even more important role than privacy and trust in user acceptance of biometric authentication systems [7] and perceived convenience can be a bigger driver than any increase in security [8], a quick literature review will reveal that the majority of studies in this field concentrate mostly on the technical aspects of various biometric modalities [4, 5] conducting evaluations on their accuracy, reliability and overall performance, such as in the studies presented in [1–3, 9, 10]. As of today, at least to our knowledge, there are no concrete user interface guidelines for biometric authentication systems.

2.1 User Interface Design Methodology

The design of the user interfaces of the SPEECHXRAYS system was based on traditional HCI heuristics applied in the context of biometrics authentication. More specifically, Jacob Nielsen's list of usability heuristics [14] was used as the basis for the application's interface design (Table 1). Nielsen is an internationally known and well-respected usability engineer who along with Rolf Molich in 1990 developed a list of ten design principles for interactive applications [15].

The list was later refined by Nielsen to what is now commonly known as usability heuristics and the evaluation of any interface against these rules is known as heuristics evaluation. This list of guidelines was chosen because it has been validated through many studies over the years in the field of HCI and it has been proven as an effective method for safeguarding usability. In addition, a literature review on biometric authentication systems was performed to gather any design guidelines or principles specific to biometrics applications as they may have been published in recent empirical studies in this field. Lastly, since one of the main requirements of this biometrics, application was for the system to be device independent, common mobile specific design guidelines and principles were used. Table 2 presents with the list of the collected design guidelines that were used for the UI design, along with the suggested design techniques that were used to fulfill them. Finally, Fig. 2 showcases a sample of the user interface prototype along with the respective design guidelines applied.

Table 1. Applying Nielsen's 10 heuristics to a biometric system.

H1. Visibility of system status. The system should always keep users informed about what is going on, through appropriate feedback made available within reasonable time.
The user has to be clear on how long he/she has to speak and look into the camera of the device for the system to take the template sample needed, in order to minimize the risk of premature process quitting and incomplete data processing [1], which can lead to user confusion and frustration.
H2. Match between system and the real world. The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
Short textual descriptions should be available to clear out any misunderstandings and the main two processes, enrolment and verification should be presented in a separate way, but also in a way that the user understands that one precedes the other. All structural elements of the application (i.e. navigational menus, action buttons, title bars, etc.) should follow the conventional design guidelines for such systems.
H3. User control and freedom. 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.
The user of the biometrics authentication system should be able to cancel an already started enrolment or verification process (i.e. provide *CANCEL* button or *BACK* controls). It is also necessary to provide a *REDO* action control – to notify the user to go through the process again – especially for low quality recording, as well as an option to *RETRY* if a verification session is unsuccessful.
H4. Consistency and standards. Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
In order to achieve uniformity in the way the application is presented and behaves in different operational settings, it is important for the user interfaces to be designed following common design guidelines and standards both for mobile and desktop applications.
H5. Error prevention. Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
In the context of biometrics authentication, environmental conditions such as humidity, temperature, and illumination, as well as performance factors such as ability of capturing good quality video and audio samples, may affect significantly the performance and accuracy of the system increasing the likelihood of errors [19]. It is, therefore, essential for the system to be proactive in preventing them from occurring in the first place. In the eHealth use case – where users are mostly occupied with their nursing and treatment work, a proactive system would automatically offered alternative authentication method if certain environmental conditions are not met and cannot be changed, i.e., illumination too low [5].
H6. Recognition rather than recall. Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.

(*continued*)

Table 1. (*continued*)

User authentication is an interruption in the user's primary task, which may even cause a disruption to the working memory of the user [1]. Multimodal authentication, such as the case of face and voice recognition, is an even more demanding process for the user who is required to perform multiple actions to achieve successful task completion. Thus, the authentication process has to be clear, concise, and able to guide the user seamlessly through the steps.
H7. Flexibility and efficiency of use. Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
The experienced or frequent user of the biometrics authentication system that has already enrolled in the system and wants to access the secured network should be able to do so with just two clicks, one for activating the VERIFICATION mode of the process and one for RECORDING the voice and face sample.
H8. Aesthetic and minimalist design. Dialogues should not contain information, which is irrelevant or rarely needed. Every extra unit of information in a dialogue
competes with the relevant units of information and diminishes their relative visibility.
It is very challenging to design complex processes for mobile viewing and careful planning and designing is needed to avoid the risk of overcrowding the interface and creating confusion to the user. This can be achieved by clearly separating the navigational elements from the actual functional elements of the selected process, by providing one main action button for each screen and other types of commonly used mobile patterns.
H9. Help users recognize, diagnose, and recover from errors. Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
This heuristic deals with what should happen in case an error does actually occurs. When this happens, it is essential for the system to present the error in a meaningful way to the user. This means that it has to be expressed in plain language and be descriptive of what the problem was.
H10. Help and documentation. Even though it is better if the system can be used without documentation, it may be necessary to be provided. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.
Educating the user on how the biometrics authentication system works on a higher-level, how and where the biometrics data is stored and used by the application, how the templates are created and accessed, and how the system safeguards their privacy and security from cyber-attacks can eliminate confusion, skepticism, and other negative pre-notions that users that are not familiar with such systems may have formed.

Table 2. List of biometrics design guidelines and their matching techniques

G1: Visibility of system status
• Provide progress bars for all the system processes noted on the screen • Provide visual/sound feedback after each action • Visual cues for the status of devices involved in process
G2: Match between system and the real world
• Use familiar to the users wording • Use design patterns users are familiar with
G3: User control and freedom
• BACK button available at all screens • EDIT button available for user to change biometrics profile • TRY AGAIN button in case of failure during the processes of verification and enrollment • Provide alternative authentication method (i.e., traditional username / password)
G4: Consistency and standards
• Fluid and flexible User Interface (UI) layout and design • Unified UI look, feel, and experience for all access platforms
G5: Error prevention
• Contextual inline instructions for correct placement of capture objects • Status of bad operation and status of hardware • Warning of poor environment conditions during enrollment and verification.
G6: Recognition rather than recall
• All main UI components and navigational elements should be visible at all times • Follow simple, commonly design patterns for mobile devices
G7: Flexibility and efficiency of use
• Processing time and each process steps should be kept to a minimum • User should be able to cancel a process and restart it • Provide instruction section for novice users and immediate action for experienced users
G8: Aesthetic and minimalist design
• UI simple and not overcrowded with navigation elements and information • Context sensitive information only • One central action button per screen • Clear look and feel with discrete graphical elements that are not tiring to the eye
G9: Help users recognize, diagnose, and recover from errors
• Display errors clearly and in descriptive text • Error messages should not be in code • Clearly communicate any process errors occurring provide descriptive error messages
G10: Help and documentation
• Provide a dedicated section with instructions / tips on how to create a good quality biometric template • Provide both textual instructions and instructions in the form of a quick demo video or animated GIF

(*continued*)

Table 2. (*continued*)

G11: Focused content with one clear task
• Provide a goal oriented design by keeping calls-to-action front and center • All information displayed on each page should be about the function that is provided in the particular page
G12: Provide a clear navigational path
• Use menu and navigation design patterns conducive to mobile interaction • Keep menus short, one level of option only • Provide an easy way to get back to the homepage
G13: Develop a single underlying system that allows for a unified experience across platforms and device sizes
• Responsive UI with fluid layouts to accommodate various screen resolutions • Design the entire site for mobile interaction
G14: Design for Touch
• Design buttons with appropriate touch target size. • Use appropriate colors & contrast.

2.2 Mobile Application Design Guidelines

There are many sources for mobile application design guidelines, such as articles published by professionals and commercial companies on technology websites and blogs, as well as papers published on scientific magazines and journals. Mobile industry leaders, Apple and Google, have both provided extensive design guidelines to developers of mobile applications for each platform respectively. Many of the published mobile best practices lists are based on Nielsen's traditional heuristics and have been expanded to include guidelines specific to the mobile use context. For the purpose of this project, a selection of four guidelines were extracted from publications [16–18, 20, 21] and used in the design of the user interfaces prototypes. These four were selected because they are complementary to the Nielsen's heuristics.

G1: Focused Content with One Clear Task. Designing with minimalism in mind is even more essential for mobiles than desktop application because in mobile devices the users have to deal with smaller screens and touch interaction. Clutter and competing graphical and interaction elements do not enhance user experience and they should be kept to a minimum. Each page should have one central focus and that should be dedicated to the task at hand [17]. The application should guide the users seamlessly through task completion without disrupting their flow. In the biometrics application context, this applies both for the verification and the enrolment processes which include multiple steps.

G2: Provide a Clear Navigational Path. Again the limitations in the viewing space on mobiles calls for less elaborate menus and navigation mechanisms than those often found in desktop websites. Thus, multi-level menus with sub menus that show on hover

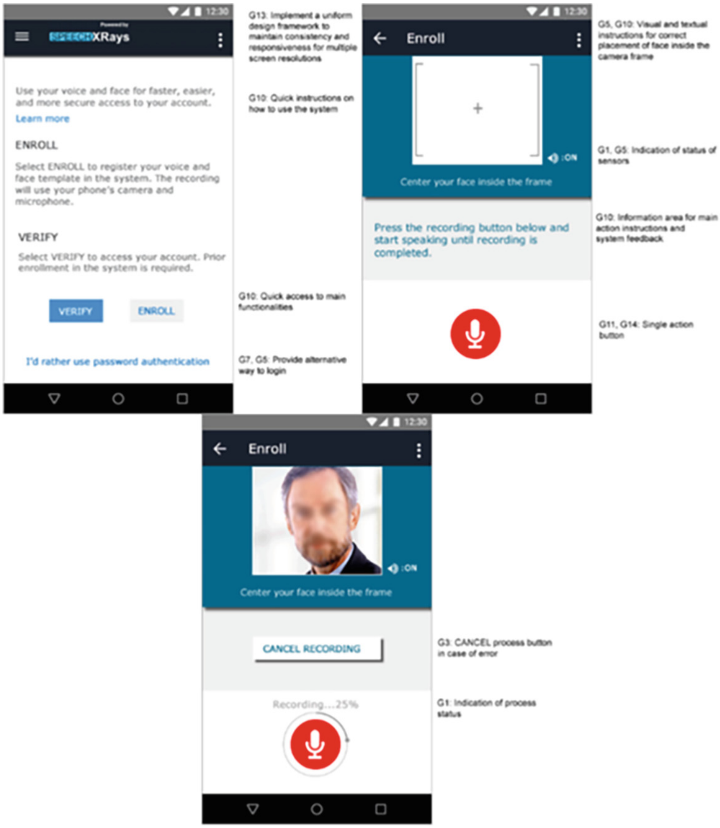

Fig. 2. SpeechXRays user interface samples with applied guidelines

and side navigation bars are not recommended in mobile design. In addition, the navigable path to task completion should be clear so that the users will be able to understand right away how they can interact with the application to achieve task completion [17].

G3: Develop a Single Underlying System that Allows for a Unified Experience Across Platforms and Device Sizes. This guideline is extremely important for all mobile applications and is referred in many studies [16, 17] and especially important for this biometrics authentication system since it addresses one of the main user requirements for the system which is, to be device independent. One of Google's guidelines is to optimize the entire site for mobile use. Participants in their study had a much easier time navigating mobile-optimized sites than trying to navigate desktop sites on mobile devices. Sites that included a mix of desktop and mobile-optimized pages were actually harder for participants to use than all-desktop sites. Thus it is suggested to design the entire site for mobile use.

G4: Design for Touch. Designing for touch requires extra care to account for fingers of all shapes and sizes applying varying kinds of pressure to touch screens that respond differently. All form controls, action buttons, and other interaction elements must measure at least 44 points by 44 points and have adequate space around them, so that they can be accurately tapped with a finger [20, 21].

3 Conclusion and Future Work

Despite the rising issues for the security of the biometric data, biometric technology is used for a number of different types of applications ranging from modest (time and attendance of personnel for a small industry) up to expansive (integrity of a whole population cohort such as voters database). Depending on the applications, the benefits of deploying biometric tools may lead to increased security, increased convenience and increased accountability compared to other authentication methods (PINs, passwords etc.). Prior to opting for a biometric system, one must also consider the existing security solutions and requirement in the specific application domain where the biometric system will be embedded. This is critical especially when dealing with services that would allow access to sensitive medical data. The UI described here along with the presented list of design guidelines, will be evaluated to study insights on how to optimally design a modular biometric platform able to be used in the eHealth domain [25]. Users (i.e. Medical specialists) will use the remote biometrics tool of SpeechX-Rays to access a collaboration platform containing patient's eHealth record and the data for management of patient's chronic conditions. The pilot study will also test the context-dependent feature that allows administrators to modify the false accepting rate or false rejection rate trade-off in order to reduce the risk of false reject for low security data and reduce the risk of false accept for high security data.

Acknowledgement. This work is supported by the research project "SpeechXRays" which receives funding from the European Commission (EC) through Horizon 2020 Grant agreement No. 653586.

References

1. Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., Ben-David, S.: Biometric authentication on a mobile device: a study of user effort, error and task disruption. In: Proceedings of the 28th Annual Computer Security Applications Conference, pp. 159–168. ACM, December 2012
2. Nandakumar, K., Jain, A.K.: Biometric template protection: bridging the performance gap between theory and practice. IEEE Sig. Process. Mag. **32**(5), 88–100 (2015)
3. Chingovska, I., Dos Anjos, A.R., Marcel, S.: Biometrics evaluation under spoofing attacks. IEEE Trans. Inf. Forensics Secur. **9**(12), 2264–2276 (2014)
4. Toledano, D.T., Pozo, R.F., Trapote, Á.H., Gómez, L.H.: Usability evaluation of multi-modal biometric verification systems. Interact. Comput. **18**(5), 1101–1122 (2006)

5. Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M.: Biometric authentication on iphone and android: usability, perceptions, and influences on adoption. In: Proceedings of USEC, pp. 1–2 (2015)
6. Miltgen, C.L., Popovič, A., Oliveira, T.: Determinants of end-user acceptance of biometrics: integrating the “Big 3” of technology acceptance with privacy context. Decis. Support Syst. **56**, 103–114 (2013)
7. De Luca, A., Hang, A., Von Zezschwitz, E., Hussmann, H.: I feel like I’m taking selfies all day! Towards understanding biometric authentication on smartphones. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 1411–1414. ACM, April 2015
8. Patrick, A.S.: Usability and acceptability of biometric security systems. In: Financial Cryptography, p. 105, January 2004
9. De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and I know it’s you! Implicit authentication based on touch screen patterns. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 987–996. ACM, May 2012
10. Blanco-Gonzalo, R., Diaz-Fernandez, L., Miguel-Hurtado, O., Sanchez-Reillo, R.: Usability evaluation of biometrics in mobile environments. In: 2013 6th International Conference on Human System Interaction (HSI), pp. 123–128. IEEE, June 2013
11. Jain, A.K., Nandakumar, K., Ross, A.: 50 years of biometric research: accomplishments, challenges, and opportunities. Pattern Recogn. Lett. **79**, 80–105 (2016)
12. Quiñones, D., Rusu, C.: How to develop usability heuristics: a systematic literature review. Comput. Stand. Interfaces **53**, 89–122 (2017)
13. Jain, A., Ross, A.A., Nandakumar, K.: Introduction to Biometrics. Springer Science & Business Media, Berlin (2011)
14. Nielsen, J.: Usability inspection methods. In: Conference Companion on Human Factors in Computing Systems, pp. 413–414. ACM, April 1994
15. Molich, R., Nielsen, J.: Improving a human-computer dialogue. Commun. ACM **33**(3), 338–348 (1990)
16. Yáñez Gómez, R., Cascado Caballero, D., Sevillano, J.L.: Heuristic evaluation on mobile interfaces: a new checklist. Sci. World J. **2014** (2014)
17. Joyce, G., Lilley, M.: Towards the development of usability heuristics for native smartphone mobile applications. In: Marcus, A. (ed.) DUXU 2014. LNCS, vol. 8517, pp. 465–474. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07668-3_45
18. Vilar Neto, E., Campos, F.F.: Evaluating the usability on multimodal interfaces: a case study on tablets applications. In: Marcus, A. (ed.) DUXU 2014. LNCS, vol. 8517, pp. 484–495. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07668-3_47
19. Unar, J.A., Seng, W.C., Abbasi, A.: A review of biometric technology along with trends and prospects. Pattern Recogn. **47**(8), 2673–2688 (2014)
20. Apple Developer: UI design do’s and don’ts (2017). https://developer.apple.com/design/tips/
21. Google Developers: Up and running with material design (2017). https://developer.android.com/design/index.html
22. Spanakis, E.G., Spanakis, M., Karantanas, A., Marias, K.: Secure access to patient’s health records using SpeechXRays a multi-channel biometrics platform for user authentication. In: 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Orlando, FL, USA, 16–20 August 2016 (2016)

23. Chronaki, C., et al.: An eHealth platform for instant interaction among health professionals. In: Computers in Cardiology 2003, Thessaloniki Chalkidiki, 21–24 September 2003, vol. 30, pp. 101–104 (2003). (02766574)
24. Spat, S., et al.: A mobile android-based application for in-hospital glucose management in compliance with the medical device directive for software. In: 2nd International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2011), Kos Island, Greece, 5–7 October 2011 (2011)
25. Spanakis, E.G., et al.: Technology-based innovations to foster personalized healthy lifestyles and well-being: a targeted review. J. Med. Internet Res. **18**(6), e128 (2016). https://doi.org/10.2196/jmir.4863