CyberActivist: Tool for Raising Awareness on Privacy and Security of Social Media Use for Activists

Borislav Tadic(✉), Markus Rohde, and Volker Wulf

Information Systems and New Media, University of Siegen,
57068 Siegen, Germany
borislav@tadic.biz,
{markus.rohde,volker.wulf}@uni-siegen.de

Abstract. Bosnia-Herzegovina (BH) and its entity Republika Srpska (RS) are among the most fragile democratic environments in Europe. In the first phase of our long-term participatory design case study, we engaged the some of the main activists in BH/RS, providing a structured picture of their practices in recent years, concrete needs and the various constraints under which they act. Our research highlighted importance and utilization of the social media for the activism in the region, but also problems such as limited budgets and know-how of the activists, intensive outsourcing practices, and a lack of awareness regarding data privacy and cyber security. Due to the perspective of BH/RS, the rising number of threats and impact incidents, and activist experiences from other unstable regions, we propose a more structured approach to privacy and security within activist circles and non-profit organizations. As the initial step in the second phase of our study, we offered a prototype of the free web application "CyberActivist" to BH/RS activists for user tests. Based on their qualitative feedback we defined the functional and non-functional requirements on further improvement of this privacy and security awareness tool. In the next phase, we will technically address their direct feedback, as well as design recommendations from relevant research and user experience literature. We also plan to propose design method improvements, design corresponding privacy and security trainings and to further internationalize the tool.

Keywords: ICT · Tool · Security · Privacy · Anonymity · Social media
Awareness · Activist · Activism · Non-profit · Political · Facebook
Bosnia · Srpska

1 Introduction

Bosnia-Herzegovina (BH) and its entity Republika Srpska (RS) are among the most fragile democratic environments in Europe. The relationship between this political environment, the kinds of activism that seem to be prevalent, and how best to support them is in the focus of our research. Our research follows the methodological concept of long-term design case studies, as it was elaborated for practice-oriented design research [3–5]. Design case studies are ethnographically informed studies that are

G. Meiselwitz (Ed.): SCSM 2018, LNCS 10913, pp. 498–510, 2018.
https://doi.org/10.1007/978-3-319-91521-0_36

"describing the original social practices, the design discourse, the design options considered, the appropriation process, the effectiveness of the artifacts' functions and the emerging new social practices" [3]. They are based on a participatory and cyclic approach of analyzing social practices in a pre-study, creating and implementing design solutions and evaluating the appropriation practices of users. This paper presents essential insights from the analytical pre-study and participatory design phase of a long-term design case study that is still ongoing.

In the first phase of our design case study, we identified the main activists in RS, providing a structured picture of their practices in recent years, concrete needs and the various constraints under which they act [1]. Empirical investigations of social media use and qualitative interviews with the country's activists indicate their strong interest in information and communication technology (ICT). Especially social media in the region is even more relevant since it basically becomes the only vehicle for activism other than direct action. Benefits for the use of ICT and social media by activists include e.g. more efficient access to their target group, easier information sharing with the general population, and quicker reaction to spontaneous "offline" activities [cf. 1, 22, 25]. At the same time, research highlighted problems of the activists such as limited budgets and know-how, intensive outsourcing practices, and a significant lack of awareness regarding data security. Although our activists are digitally very active and consequently ICT-literate, they are largely self-taught, being neither ICT-professionals nor "digital natives". After we conducted problem-centric interviews with six cyber activists, we clustered their needs and our observations in the following categories:

(1) a structured approach to cyber security, data privacy and anonymity within activist circles and the NPO sector
(2) specialized trainings tailored for cyber activists, the specific region and based on available resources
(3) support for practices enhancing self-learning and knowledge transfer within the specific BH/RS setting.
(4) sustainable models within ICT outsourcing and use of external freelancers within cyber activism.

Due to the perspective of BH/RS, the rising number and impact of privacy and security incidents, and an increasing relevance of social media and activist experiences from e.g. Turkey or "Arab Spring", we believe that a more structured approach to privacy and security within BH/RS activist circles and non-profit organizations is needed. Aiming to address these developments and elements (1)–(3) listed above, in the second phase of our design case study, we decided to implement a prototype of a web application named "CyberActivist" for awareness in the areas of privacy and security. Following a participatory design approach like Caveat [6] or Come_IN [2], we made our prototype software available to the BH/RS activists for a test in a real-world practice ultimately leading to documentation of clearly articulated requirements for improvement of their communication practices and the tool itself.

In Sect. 2 of this paper, we are looking at the related state-of-the-art work regarding the social media impact within global activism and the related privacy and security considerations. Section 3 provides an overview of the functionalities of the tool and Sect. 4 follows with the summarized outcome of the BH/RS activist experiences during and after the test of the “CyberActivist” prototype. Last section provides an outlook on planned next steps and research possibilities in this context.

2 Related Work

Social media based movements and their members leave behind digital footprints that authoritarian powers can exploit for the surveillance and oppression [7], e.g. using provocateurs and bots [32, 34]. [34] looked at social media focusing on one side with insider threat prediction and prevention, connecting malevolent insiders and predisposition towards computer crime with personality trait of narcissism. At other side, regardless of national scope, an important social threat is based on user generated content exploitation and leads to political affiliation profiling. Activists are a very relevant group here, esp. within authoritarian systems and even with potential employers. According to [32], human resource departments increasingly use social media screening, which produces negative reactions of the candidates in the US. If this would be the case in BH/RS, where non-employment is high and cyber activists can be marked as the opponents of the regime, they might be having additional difficulties finding jobs, if they are not careful with the information published online. [33] argues that many “difficulties associated with the protection of digital privacy are rooted in the framing of privacy as a predominantly individual responsibility”. This is very visible regarding Terms and Conditions of social media; although users of social media platforms are poorly informed about the changes in the privacy policies, it is often “setting forth the expectation that the user has been educated enough to now make decisions in their best interest”.

Social media relevance in regard to the privacy and security differs over activist heritage [29], age, gender [18, 19], habits [28], and changes over time [30]. [29] conducted a comparative study on social media use with focus on privacy aspects within 5 nations. Although a majority of users stated that is “important to prevent risks that might arise from privacy related behavior”, they had significantly different implementations, such as anonymizing their identity or self-disclosure. Mentioned implementations might easily be customized to address the needs of activists of other nations. Study participants reported that they had not yet experienced many privacy violations. In our case, RS activists have also their specific attitude, similar to the part of the attitudes from [29] which must be considered within the tools supporting their engagement. With effectiveness and practicality in mind, we implemented a prototype of a web application “CyberActivist” for awareness in the areas of privacy and security of social media, described in detail in the next section. It also might be used in other geographic contexts, similar to implementations of [29]. [18] has shown how different population structures have a different understanding of privacy, its enforcement and importance in the social media context. This may very well apply to our activists. [28] focused on undergraduate students’ experiences with social network system privacy. Students worried about their privacy being violated by someone physically locating them still felt comfortable sharing their personal information. More media literacy leads to better awareness about risks of sharing information on social media. This supports the thesis on need for specialized training for activists identified in [1]. [30] compared

Facebook users to understand how their privacy and disclosure behavior changed between 2005–2011. Besides concluding that users exhibited volatile privacy-seeking behavior, from less disclosure in the first years to an increase towards the end of the study, they warned from the often non-transparent “silent listeners”. Due to the increase in amount and scope of personal information that users revealed privately to other connected profiles, more information is available to Facebook itself, third-party apps, and indirectly advertisers. Authors of this paper assume that these findings are becoming even more relevant for numerous cyber activists, if we extend the list of “silent listeners” to state-related apparatus and highlight low privacy awareness of the activists present on Facebook (e.g. low interest in terms and conditions).

Following a participatory design approach [cf. 2, 6], our implementation was tested by the activists in their real-world practice. This led to the tuning of our tool based on direct interaction, and ultimately improved activist communication practices. We also orientated us on insights of e.g. [24, 26] and recommendations from best practices such as [9]. [26] proposed a framework including an open source implementation with semantic, hierarchical scoring structure for raising the awareness of social media users with respect to the information that is disclosed and that can be inferred by third parties with access to their data. It enables users to browse over different privacy-related aspects considering both information that is explicitly mentioned in users’ shared content, as well as implicit information, that may be inferred from it. [24] also claims that ICT and social media enabled better access to personal and location information of another person, and activists may not be aware of the possibilities here. Despite having regulatory policies, it is possible to extract quite exact location information of a person over time by using volunteered or contributed geographic information available from social media sites (e.g. GeoAPI of Twitter).

Although privacy and security requirements are sometimes in conflict, we can reasonably raise both aspects using tailored approaches [20, 27] and by creating visibility over vulnerabilities of an activist or his environment [23]. It is also important to consider differentiation of the social groups in their attitude towards privacy and security when developing ICT solutions [33] and unconventional approaches to promote privacy and security such as using celebrity engagement in social media [21]. Taking the example of one group of human rights activists, [33] highlights the importance of developing a collective approach to address their digital privacy and security needs. Digital security strategies cannot remove all threats; they can only mitigate their effects and deal with numerous elements such as authentication on Facebook. We included the question about the Facebook authentication into the *Self-assessment* within our prototype (see next section of this paper). [23] introduced methods for determining the amount of information that can be ascertained using only publicly accessible data and provides a framework for determining a user’s web footprint. Threat of user’s attributes that may be inferred by an adversary using only public sources of information has been reconfirmed by analysis across multiple social networks. The same method can be applied by cyber activists and other individuals to assess and act upon their own exposure in the public media.

3 Web Application “CyberActivist”

The development of the initial version of our web application “CyberActivist” (in English and Serbo-Croatian language) took six months in 2016, using HTML, JavaScript and CSS. One of the paper authors has written the whole source code of the initial version of the prototype that was provided to the activists for the test.

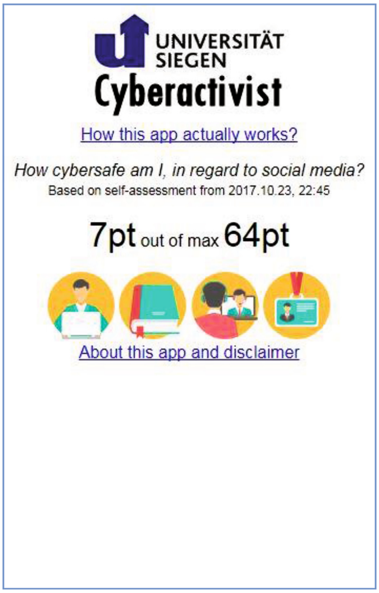
Primary functions of the tool are: to enable self-assessment of privacy and security in the context of social media and make results transparent to the user, then dynamically point to open, external, self-learning resources esp. in areas marked as “blind spots” and volunteering opportunities.

“CyberActivist” consists of four sections, which are represented by the icons on the primary screen after the application start: *Self-assessment*, *Self-learning*, *Contribute*, and *My Profile*. In addition, there is information about the so called *cyber safe score* of the self-assessment, visible only after the performed self-assessment, and hyperlinks to two information pages: *About the application* and *How does this application work*.

Self-assessment (Fig. 2) and *My Profile* (Fig. 4) sections enable users to gain transparency about the risks within their social media environment and to see how they are positioned regarding these risks. We are using easily understandable, user-centric language, knowing the average ICT proficiency of the target group, to help them gain insight and derive appropriate action. Section *Self-assessment* contains nine groups of questions: 25 general questions, applicable to most social media platforms, then specific platform questions on Facebook (11 questions), Google/Youtube (8), Twitter (6), Whatsapp (4), Viber (4), Skype (4), Instagram (6) and one group reserved for other platforms such as Linkedin (3), which can be answered through multiple-choice text options (e.g. “yes”, “no” and “I do not know”). An example of a question is “Do I know who will be accessing information I have put on social media?”. The question groups are focusing on the most frequently mentioned ICT tools and social media platforms mentioned by the activists in [1] and publicly available ranking information [cf. 8]. When results are saved, they are being recorded on the activist’s device using the local storage functionality of HTML and not transmitted to any remote server. The selection of questions and their formulation have been based on experience of one of the authors of this paper, as well as on similar international questionnaires and assessments such as [cf. 9–17]. The Section *My Profile* shows the data about the user available within browser he uses, e.g. whether Java is activated or what is the geographic location. It also enables the user to set the language of the application.

The main screen shows a so called “*cyber safe score*” (Fig. 1). This score is calculated based on the number of positive (“plus” point) and negative answers (“minus” point) from the self-assessment with the maximum score of 64 points being achievable. An example of the positive/negative answer is “I have/have not latest version of Twitter installed on my devices”. On the main application screen, the user is also being given an instruction to perform a self-assessment before being able to use the application’s full functionality and find out “how the tool actually works”.

Section *Self-learning* (Fig. 3) offers a customized array of reading materials based on the *cyber safe score* and improvement areas. Most materials are articles published by the relevant social media platforms, non-profit organizations or media with direct



UNIVERSITÄT SIEGEN

Cyberactivist

How this app actually works?

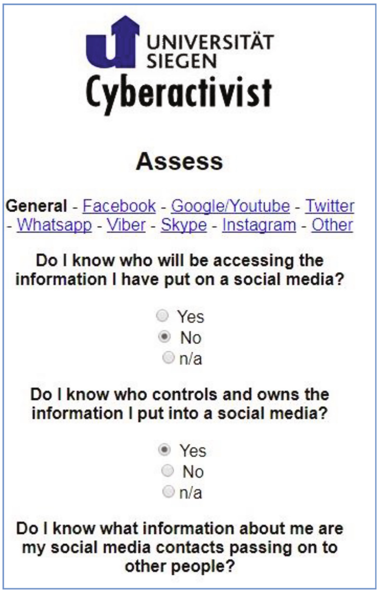
How cybersafe am I, in regard to social media?

Based on self-assessment from 2017.10.23, 22:45

7pt out of max 64pt

About this app and disclaimer

Fig. 1. Main screen showing sections and *cyber safe score*



UNIVERSITÄT SIEGEN

Cyberactivist

Assess

General - Facebook - Google/Youtube - Twitter - Whatsapp - Viber - Skype - Instagram - Other

Do I know who will be accessing the information I have put on a social media?

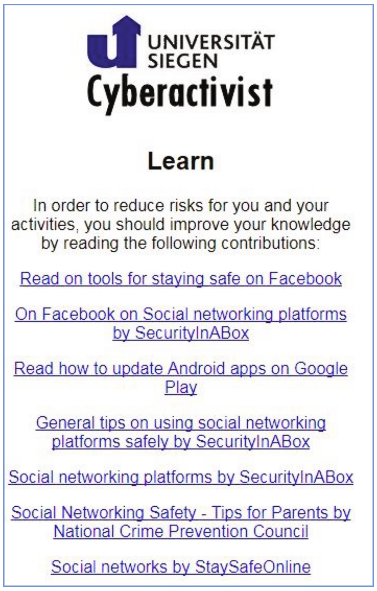
○ Yes
● No
○ n/a

Do I know who controls and owns the information I put into a social media?

● Yes
○ No
○ n/a

Do I know what information about me are my social media contacts passing on to other people?

Fig. 2. *Self-assessment* section/questionnaire



UNIVERSITÄT SIEGEN

Cyberactivist

Learn

In order to reduce risks for you and your activities, you should improve your knowledge by reading the following contributions:

Read on tools for staying safe on Facebook

On Facebook on Social networking platforms by SecurityInABox

Read how to update Android apps on Google Play

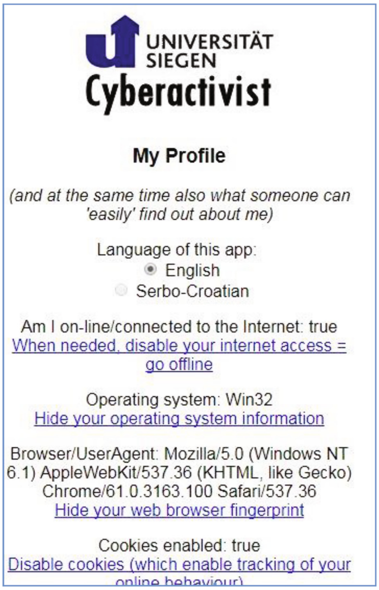
General tips on using social networking platforms safely by SecurityInABox

Social networking platforms by SecurityInABox

Social Networking Safety - Tips for Parents by National Crime Prevention Council

Social networks by StaySafeOnline

Fig. 3. *Self-learning* section/recommended reading



UNIVERSITÄT SIEGEN

Cyberactivist

My Profile

(and at the same time also what someone can 'easily' find out about me)

Language of this app:
● English
○ Serbo-Croatian

Am I on-line/connected to the Internet: true
When needed, disable your internet access = go offline

Operating system: Win32
Hide your operating system information

Browser/UserAgent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Hide your web browser fingerprint

Cookies enabled: true
Disable cookies (which enable tracking of your online behaviour)

Fig. 4. *My Profile* section

actionable advice on improving security, privacy and anonymity. In the case of the mentioned Twitter answer example, it would be a reading material related to "software patching" or "privacy and security settings of Twitter". It supports preferred way of (self-)learning of the BH/RS cyber activists, caused by resource limitations (e.g. training budget). Every click in this section opens an additional web browser window and shows the original web page outside the "CyberActivist" application.

The *Contribute* section aims at knowledge sharing and multiplication effects, providing a non-customized list of organizations and websites providing privacy and security advice to activists, e.g. "TacticalTech" [36]. The list is based on the selection of the authors, based on the background of BH/RS activists.

"Cyberactivist" does not collect, process or send any information about the users or their online behavior to the author or any other subject. The application does not use cookies. All links included in the *Self-learning* section are to third party websites, which have separate privacy policies and the authors therefore have no responsibility or liability for their content or activities.

The format of the application - web-based, platform independent, free - is also chosen based on the activists' usage of phones and PCs as primary hardware. Making the "CyberActivist" source code open, with no modification and expansion constraints, improves its reach among activists. After completion, the authors and their academic institution plan to publish and keep the software free and open source providing a clear value adding to the activist and developer community.

4 Participatory Design: Feedback and Possible Improvements

After the development of the application, we have shared a link to the prototype for the test with the selected activists. We contacted all the activists who participated in our former research [cf. 1] and additional new activists we identified monitoring social media activities in the BH/RS.

Five activists responded to our invitation (Table 1). We asked them to test the application and did not provide them with any information besides that the web application is focused on privacy and security. They tested the application on one day, but did not invest longer than an hour of their time. Neither usage data nor self-assessment results were transmitted to the paper authors during or after the test. Activists also committed to the interview in the Serbo-Croatian language after the test, to document their impressions and feedback on possible tool improvements. The activists provided us with almost four hours of responses which were digitally audio-recorded in five separate sessions between May and September of 2017. One activist complemented his audio statement with an e-mail response. Skype with an audio recording plug-in was used as an interview tool. The key findings of our interviews were transcribed in English language and comprise approximately 50 pages.

All activists suggested that the application is simple. They all also agree that the purpose, background methodology, and the user interface of the "CyberActivist" application has to be further sharpened. There is a need to further optimize the main screen. Brad posed a question: "Is the tool meant for single use or for reuse?".

Table 1. Interviewed activists/participatory design phase

Pseudonym	Birth year	Role/Active since	Participated in our earlier research [1]
Brad	1980	Project Manager at local NPO, 2006	Yes
Ela	1984	Project Manager at the local branch of an international NPO, 2008	Yes
Adam	1981	Member of international NPO focused on the RS, 2008, located in Austria	No
Kevin	1981	Local journalist/an individual activist	No
Alena	1980	Individual activist for disabled population	No

Kevin did not even open sections *Self-learning, Contribute, and My profile* as access to these sections was not visible or intuitively displayed. With regard to navigation within the app, Alena suggested that a “Go Back” key is missing.

Adam suggested establishing separate scores for security and for privacy; as referenced in Sect. 2 of this paper, security and privacy aspects are not always correlated. The methodology to calculate the *cyber safe score* raised many questions among activists. Originally planned as the simple, high-level information of displaying general protection status, *cyber safe score* did not fulfill its purpose. The score was unclear for most activists (e.g. Ela: “I got 35 out of 65 points…” - what does it concretely mean, where are my weaknesses, what do I need to improve). The outcome from the self-assessment should be visible immediately, and not only later through links in the section *Self-learning*. The outcome should be explained in more descriptive language, rather than only by a number. Adam considers himself experienced within security and got only 2 points after the self-assessment. The other activist did not understand the logic of adding “plus” and “minus” points.

Most activists tested the tool on the laptop or desktop computer, not on the mobile device. However, Adam suggested that our application should be further customized based on the platform used (e.g. screen resolution, native user interface). The platform should also influence the offered advice in the *Self-learning* section. Differentiation between PCs and mobile devices in the answers within the *Self-assessment* section are also proposed, as usage patterns are differing.

Regarding the *Self-assessment* section, Adam commented that 25 questions in the general part of this section might be too much and proposed separation over several screens/pages. Another idea would be to show the progress of the questionnaire (“how much I still have to go?”). Almost all activists felt that there are lots of repetitions of the similar questions (e.g. same formulation “did you perform an update for… Twitter, Facebook, Whatsapp…”), however they meant that the “questions are clear”. Several questions in this section contain formulation “Do I or my organization use…”; Kevin suggested to clearly separate the two, as the answer may differ. Kevin’s proposal was also to add the answer option “I don’t care/It’s not important” to existing possible answers “yes/no/don’t know” in the self-questionnaire. Kevin also suggested reconsidering which questions are suitable for the “general questions” category. For him the question “do I trust my connections” would be differently answered for different social media platforms, e.g. for Facebook and Twitter. Two or more predefined answers are offered for every question in the *Self-assessment* section based on the multiple-choice logic. Alena claimed that there is no need for any choice to be marked as default, as it is with the choice "I don't know" in our case. Activists also suggested adding or rephrasing some questions such as "how to add to the group on social media, limiting member's access" or "would your identity disclosure jeopardize your close people/relatives". They claim that is positive that a person is not asked on all tools if they do not own an account on this specific social media.

The first improvement proposal for the *Self-learning* section was that the introduction text should not be shown if the self-assessment is not done. Some of the activists such as Adam did not notice the correlation between the *Self-assessment* and *Self-learning* sections. Activists also claimed that the explanation of the results is needed, such as "…because you don't understand X, you need to read Y and Z". Therefore, a clear link needs to be established between "negative" answers from *the Self-assessment* section, "minus" points of the cyber safe score and the proposed reading materials in the *Self-learning* section. Optimally, related reading materials should be grouped. Authored privacy and security advice is welcome, according to Ela.

Looking at the *Contribution* section, Adam asked whether the listed organizations want/need help or volunteers at all. The others found this section useful as it is. As BH/RS NPOs and activists are struggling with resources [1], Brad suggested an additional feature "find/engage an expert" (e.g. specialist for IT security or video production). He also proposed to integrate some "advertisement" in the tool such as „you are an IT expert - do you want to help and engage in our activities?".

The information in the section *My profile* was found to be useful, however not always self-explanatory (e.g. web browser information as "user agent string").

Brad suggested the replacement of the term "activist" with "socially responsible person", due to "negative connotation" of the term. In general, activists asked that tool's goals, benefits and "flow" are described more clearly in the tool itself (e.g. are results of self-assessment sent somewhere for analysis, how is the score calculated). In addition, better instructions on the tool proper usage are welcome.

In addition, all activists suggested that the used text for a Serbo-Croatian version can be improved. Activists advised the use of fewer Anglicisms in the text and less synonyms esp. in technical context (e.g. "data privacy" vs "data protection"). They also made proposals on how to increase readability, through consistent use of the local alphabet (e.g. "č vs c"), adequate font size and text margins on the different platforms. The *Self-learning* section was referred by Ela as useful as it's good to point to sources and practices from other countries. Other activists were only partially satisfied with the fact that all reading materials offered by the tool as a result of the self-assessment are in English (and not in Serbo-Croatian). This feedback is a good reminder that text quality and thorough localization of the tool plays an important role for acceptance among the activists.

This very qualitative feedback from the activists gathered specific functional and non-functional software requirements and enabled multiple ways of improving the tool. Several ideas for tool improvements are coming from state-of-the art research, e.g. aligning it to models such as "privacy nudge" [20, 27], considering integration with approaches such as "FaceCloak" [31] or adding features such as "celebrity cause" [21], which might be considered in future work and tool adaptations. Research on behavioral decisions and soft paternalism to design mechanisms led to development of so-called "privacy nudge" for Facebook users [27]. This alarm reminds Facebook users to consider the content and context of the information before posting them, helping individuals avoid regrettable online disclosures. Nudges provide visual cues about the audience for a post, time delays before a post is published and gives users feedback about their posts. Adaptation of this nudging might prevent activists' unintended disclosure. [20] also argues the idea of nudging the user with "Privacy Nudge" to help people make better privacy choices and decisions on online social networks. The proposed model will nudge users while posting by calculating Privacy Score and accessing last modified privacy settings for users which will alert users to adjust their privacy settings. FaceCloak protects user privacy on a social media by shielding a user's personal information while maintaining usability of the site's services [31]. This Firefox browser extension for the Facebook provides fake information to the social media and by storing sensitive information in encrypted form on a separate server. Although oriented on one platform only, it is an interesting concept that could be a measure related to our "*cyber safe score*". Celebrities, such as movie actors, often take up an active interest in the "good causes" such as prevention of engagement of children as soldiers in Africa. Their posts on the cause in the social media help draw attention to the cause among their numerous followers. This might be an opportunity for cyber activists, also in the context of awareness for protection of their privacy and security and lobbying for e.g. less surveillance in authoritative societies [21].

The authors themselves also identified ideas on improving the tool, such as those improving user experience, building a more intuitive graphical user interface and adding relevant information sources.

5 Outlook

Especially the more detailed evaluation of users' appropriation of our prototype in the practice goes beyond the scope of this paper and will be object of future research. We base our original contribution to the HCI knowledge corpus on the long-term design case study which enabled numerous insights into practices of political activists in BH/RS, which led to a tool "CyberActivist". Our presentation includes the relevant state-of-the-art research, online and offline experiences with our prototype, unfiltered feedback of the activists, and differentiation through simple, yet unique awareness and self-learning capabilities on social media.

The tool enables activists to understand, address and mitigate the privacy and security risks related to use of social media. The authors plan first to adapt the tool based on the input from the section four of this paper, and eventually to publish it cost-free in multiple languages making it available to the global activist community. This will follow an intense exchange with other HCI researchers which have worked in multiple other geopolitical regions (e.g. Middle East) and incorporation of their thoughts on applicability and target group reach. In addition, in further publications we plan to continue our design case study by observing the development of the ICT and esp. social media use in BH/RS.

Authors and the research community can further refine the underlying research method, e.g. regarding the precision of the questions asked in the interview phase, or evaluation and consolidation of sometimes opposing improvement proposals of the activists. Industry best practices such as Scrum within agile software development [cf. 35] are a great opportunity for improvement of both, our method and quality of the tool. Continuous presence of the activists in the role of the "customers" during the development "sprints" would directly increase the quality of the tool, and potentially fully remove the need for interviews after the implementation of the new tool functionalities.

Our strong belief is that the tool's impact would be raised, if activists would receive free tailored and localized training on privacy and security aspects. In the future, authors will work on the conceptualization of such trainings and/or information campaigns. We believe that this holistic and integrated socio-technical approach will serve as an open, extendable, scientifically founded and practically easily applicable awareness instrument for activists in fragile democratic contexts worldwide.

References

1. Tadic, B., Rohde, M., Wulf, V., Randall, D.: ICT use by prominent activists in Republika Srpska. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI 2016, pp. 3364–3377 (2016). https://doi.org/10.1145/2858036.2858153
2. Aal, K., Yerousis, G., Schubert, K., Hornung, D., Stickel, O., Wulf, V.: Come_in@palestine: adapting a German computer club concept to a Palestinian refugee camp. In: Proceedings of the 5th ACM International Conference on Collaboration Across Boundaries: Culture, Distance & Technology, CABS 2014, pp. 111–120, NY, USA. ACM, New York (2014). https://doi.org/10.1145/2631488.2631498
3. Rohde, M., Brödner, P., Stevens, G., Betz, M., Wulf, V.: Grounded design – a praxeological is research perspective. J. Inf. Technol. **32**, 163–179 (2017)
4. Wulf, V., Rohde, M., Pipek, V., Stevens, G.: Engaging with practices: design case studies as a research framework in CSCW. In: Proceedings of ACM Conference on Computer Supported Cooperative Work (CSCW 2011), pp. 505–512. ACM-Press, New York (2011)
5. Wulf, V., Müller, C., Pipek, V., Randall, D., Rohde, M., Stevens, G.: Practice-based computing: empirically-grounded conceptualizations derived from design case studies. In: Wulf, V., Schmidt, K., Randall, D. (eds.) Designing Socially Embedded Technologies in the Real-World, pp. 111–150. Springer, London (2015)
6. McPhail, B., Costantino, T., Bruckmann, D., Barclay, R., Clement, A.: Caveat exemplar: participatory design in a non-profit volunteer organisation. Comput. Support. Coop. Work **7**(3–4), 223–241 (1998). https://doi.org/10.1023/A:3A1008631020266
7. Morozov, E.: The Net Delusion: The Dark Side of Internet freedom. Public Affairs, New York, USA (2011)
8. Kallas, P.: Top 15 most popular social networking sites and apps. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites. Accessed 28 Jan 2018
9. Deutschland Sicher im Netz, Sicherheitscheck. https://www.dsin-sicherheitscheck.de. Accessed 15 June 2017
10. Internet Privacy Practices Self-assessment. https://libraryfreedomproject.org/wp-content/uploads/2016/02/privacy-assessment-tool-to-print.pdf. Accessed 17 June 2017
11. Online Privacy and Security Questionnaire. http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/questions/privacy.html. Accessed 17 June 2017

12. USAID Privacy Office, Privacy Impact Assessment. https://www.usaid.gov/sites/default/files/SocialMediaPIA.pdf. Accessed 17 June 2017
13. Academic Frontier Project. Survey on the internet security awareness. http://www.kansai-u.ac.jp/riss/en/shareduse/data/17_E_questionnaire.pdf. Accessed 17 June 2017
14. Purdue University, Information Security Questionnaire. https://www.cerias.purdue.edu/assets/pdf/k-12/questionnaire/infosec_questionnaire.pdf. Accessed 17 June 2017
15. Warwick University, Information Security Awareness Questionnaire. http://www2.warwick.ac.uk/services/gov/informationsecurity/questionnaire. Accessed 17 June 2017
16. Federal Trade Commission, Privacy impact assessments. https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments. Accessed 17 June 2017
17. Kumaraguru, P.: Privacy and security in online social networks, NOC. https://onlinecourses.nptel.ac.in/noc16_cs07/preview. Accessed 17 June 2017
18. Madden, M.: Privacy management on social media sites. http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites. Accessed 17 June 2017
19. Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., Beaton, M.: Teens, social media, and privacy. pp. 2–86. Pew Research Center, 21 Jg (2013)
20. Saad, T., Khan, F.: Nudging Pakistani users towards privacy on social networks. In: 2016 SAI Computing Conference (SAI), pp. 1147–1154. IEEE (2016)
21. Tsaliki, L.: Tweeting the good causes: social networking and celebrity activism. In: Marshall, P.D., Redmond, S. (eds.) A Companion to Celebrity, pp. 235–257. Wiley, Boston (2016)
22. Lynch, E.: The new social imaginary vs. the education activist: social media as a conduit for protest and resistance. Hofstra University (2017)
23. Singh, L., Yang, G.H., Sherr, M., Hian-Cheong, A., Tian, K., Zhu, J., Zhang, S.: Public information exposure detection: helping users understand their web footprints. In: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 153–161. ACM (2015)
24. Kar, B., Ghose, R.: Is my information private? geo-privacy in the world of social media. In: GIO@ GIScience, pp. 28–31 (2014)
25. Fullam, J.: Becoming a youth activist in the internet age: a case study on social media activism and identity development. Int. J. Qual. Stud. Educ. **30**(4), 406–422 (2017). https://doi.org/10.1080/09518398.2016.1250176
26. Petkos, G., Papadopoulos, S.: PScore: a framework for enhancing privacy awareness in online social networks. In: 2015 IEEE 10th International Conference on Availability, Reliability and Security (ARES), pp. 592–600 (2015)
27. Wang, Y., Leon, P.G., Scott, K., Chen. X., Acquisti, A.: Privacy nudges for social media: an exploratory Facebook study. In: Proceedings of the 22nd International Conference on World Wide Web companion, pp. 763–770. ACM (2013)
28. Magolis, D., Briggs, A.: A phenomenological investigation of social networking site privacy awareness through a media literacy lens. J. Media Lit. Educ. **8**(2), 22–34 (2016)
29. Trepte, S., Masur, P.K.: Cultural differences in media use, privacy, and self-disclosure: research report on a multicultural survey study. University of Hohenheim, Germany (2016)
30. Stutzman, F., Gross, R., Acquisti, A.: Silent listeners: the evolution of privacy and disclosure on facebook. J. Priv. Confidentiality **4**(2), 7–41 (2014)
31. Luo, W., Xie, Q., Hengartner, U.: Facecloak: an architecture for user privacy on social networking sites. In: IEEE 2009 International Conference on Computational Science and Engineering, CSE 2009 (2009). https://doi.org/10.1109/cse.2009.387
32. Drake, J.R., Hall, D., Becton, J.B., Posey, C.: Job applicants' information privacy protection responses: using social media for candidate screening. AIS Trans. Hum. Comput. Interact. **8**(4), 160–184 (2016)

33. Kazansky, B.: FCJ-195 privacy, responsibility, and human rights activism. Fibreculture J. **26**, 189–207 (2015)
34. Gritzalis, D., Kandias, M., Stavrou, V., Mitrou, L.: History of Information: the case of privacy and security in social media. In: Proceedings of the History of Information Conference, pp. 283–310, Athens, Greece (2014)
35. Schwaber, K., Beedle, M.: Agile Software Development with Scrum. Pearson International Edition, USA (2002)
36. Tactical Technology Collective. https://tacticaltech.org. Accessed 28 Jan 2018