International Journal of Sociotechnology and Knowledge Development
Volume 8 • Issue 1 • January-March 2016

Colour as an Indicator of Vulnerability of Users Within Social Networks

Amanda Cox, Charles Sturt University, Wagga Wagga, Australia
Yeslam Al-Saggaf, Charles Sturt University, Wagga Wagga, Australia
Kate McLean, Charles Sturt University, Wagga Wagga, Australia

ABSTRACT

Social networking users are presented with a plethora of profile and privacy settings; most of which are left defaulted. As a result, there is little understanding of the fields that make up the user profile, the privacy settings available to safeguard the user, and the ramifications of not changing the same. Concerns relating to the unprecedented quantities of Personally Identifiable Information being stored need to be addressed. By employing a risk matrix to a social media profile, a user could be alerted to the potential dangers of the information being contained within the profile. By adapting this tool, the risks to the individual user of a social media profile will be minimised.

KEYWORDS

Colour, PII, Privacy, Risk Matrix, Social Networks

INTRODUCTION

On any given day we find ourselves stopped at a stop sign or a traffic light. We have been educated that a red signal means STOP or DANGER. Can this logic be applied to a social networking environment? A related question is to what extent a social media user's Personally Identifiable Information (PII) can be protected by applying a colour code to indicate the danger of disclosing a user's PII? The extant literature highlights the plethora of privacy issues facing social media users and it is generally acknowledged that the onus of protecting privacy is on the user.

Previously proposed solutions, such as those outlined by Ge and Zhu (2011), include the application of complex algorithms such as Trust Third Party, Data Perturbation Technique, Secure Multiparty Computation and Game Theoretic Approach to perform privacy preservation of PII. The methodology that Ge and Zhu (2011) suggest removes the user's involvement. Thus vulnerability is potentially increased as users are not aware of the amount of (PII) held within their user profile. Many empirical studies have been conducted in the area of social networking sites (SNS). Sar and Al-Saggaf (2014) identified that the focus of these studies should include the privacy of user information and how this is shared over these sites, with or without user awareness or consent.

There are many considerations and risks associated with the social media applications for personal use. By employing a risk matrix to a social media profile, a user could be alerted to the potential dangers of the information contained within a profile.

Social media profile structures are multifarious to the average user, and much of the data captured is "hidden" within the profile. Thus, the main research question is:

To what extent can the privacy of Personally Identifiable Information within social networks be improved/protected by adapting a risk matrix as a tool to generate a value to indicate a use of colour?

This study allows user involvement, by showing the user the extent of their vulnerability. By displaying the level of vulnerability through colour-coding, the risks associated with "completing" a user profile will be mitigated.

DOI: 10.4018/IJSKD.2016010104

This paper comprises the following sections:

I. a brief background of the privacy issues surrounding social networks,
II. a description of the methods to devise a risk matrix to support the study, and
III. the methodology used to gather the data to develop a prototype of the risk matrix.

BACKGROUND

Facebook

Originally intended as a personal space to share information about oneself; Oeldorf-Hirsch and Sundar (2014) believe that Facebook has become a common venue for sharing external content with one's network. Baresch, Knight, Harp and Yaschur (2011) concur and enhance the sentiment by inferring that Facebook has become one of the leading referrers to news sites through links shared by friends when it comes to news items.

Sundar (2008) believes that Facebook encourages content distribution by making communication features such as status updates, photo and video-sharing options, and location check-ins prominent and easy to use. Van Dijck (2013, p. 12) states by "technologically encoding people's activities; formal, manageable, and manipulable, enabling platforms to engineer the sociality in people's everyday routines". Anderson (1997) touts the use of any media has the ability to be added to the norms, values, ritual, custom and language to modernised a culture.

Van Dijck (2013) also postulates that the use of Facebook will lead to the creation of a transparent social world where users act as a source of information allows users to experience a sense of agency by feeling that they have some control over information on the site.

With the abundance of information available on social networks, in particular, Facebook, a user may become overwhelmed and is, therefore, unlikely to realize the amount of personal information they have divulged.

Privacy Paradox

Privacy issues become all the more important as availability of publicly shared personal information is increased. Social media and networks facilitate an unprecedented level of accessibility and transparency. Facebook users express concern about the publication of personal information in the online environment, but at the same time, as Boyd (2007) states, users actively construct their identity online through the disclosure of personal information. There are many reasons for the increased risk of personal information being used for purposes other than that originally intended on social network sites. Fuchs (2010) indicates that Facebook's idea of privacy is based on an understanding of self-regulation and an individualistic perspective of privacy.

Dumas, Serfass, Brown and Sherman (2014, p. 376) state "users should not bear the entire burden of their privacy protection", especially when SNS dictate the terms of the agreement. Social networking users sacrifice privacy the very moment the "I accept" button is pressed. User data is used as a commodity for sharing with third parties, mainly advertisers. The problem Fuchs (2010, p. 148) describes "is that the users are not asked if they find targeted advertising necessary and agree to it". This technique uses the concept of 'user consent' in Facebook's Privacy Policy.

A sharp juxtaposition exists between the concern people express and their readiness to disclose personal information. Barnes (2006) has identified these phenomena as "the privacy paradox", a finding that has shown how, despite expressing a concern about Facebook privacy, people often do very little to protect themselves. Boyd (2006) cautions that social media users should think twice

before posting thoughts on status fields as these can easily be copied, forwarded, replicated, and taken out of context.

Personally Identifiable Information (PII)

Raghunathan (2013) defines Personally Identifiable Information (PII) as any information on an individual which, if combined with additional data, will enable the identification of that individual. PII includes physical characteristics including biometric details such as iris scans and finger prints; date of birth, gender, marital status, address, and postcode; educational, medical or contact details. Also included in this definition is the IP and MAC address of the computer from which the user is viewing SNS.

It should be noted that for the purposes of this paper the meaning of PII will be adopted from Krishnamurthy & Wills' (2001, p. 1) definition: "information which can be used to distinguish or trace an individual's identity either alone or when combined with other public information that is linkable to a specific individual".

Using Pseudonyms with Facebook Accounts

Anonymity and pseudonymity have a long history. Many authors of the 18th century published under the guise of anonymity for fear of prosecution (Folkenflik, 2011). The 19th century was the height of the use of the pseudonym for publishing authors (Hayward, 2011). Pseudonyms were used to disguise features that authors and artists themselves believed would lead to superfluous dismissal or outright rejection. (Hogan, 2012). Now in the 21st century, with the ever increasing use of social networks and guidelines comparable to Facebook's real name policy. The potential is accelerated for this leading to the end of using pseudonyms, which was one of the main concepts in support of privacy protection (Caron, Bosua, Maynard, & Ahmad, 2016). Facebook is not the only social networking provider presently pushing for the ubiquity of real names online others include Google and LinkedIn. These providers believe that it "minimizes inappropriate content and helps to create a more just society" (Hogan, 2012, p. 2). Buglass et. al trust that these policies are indicative of a growing trend for social networking platforms to move "toward non-anonymised communication driven in part by a desire to impinge on the growing problem of fake or erroneous profiles" (Buglass, Binder, Betts, & Underwood, 2015, p. 64). Regardless of social networking trends, the tool under development as part of this study will not authenticate against any policies provided by the social media platform. This tool will be only viewing the user profile and the associated fields and returning a value associated with a corresponding colour.

Data Leakage

Data leakage affects both the business world as well as individual users of social media. Zhang, Sun and Zhu (2010) state that data leakage occurs when there is an unauthorised transfer of data from a computer with a datacentre to the outside world; or when there is accidental or intentional revelation of intellectual property or confidential data in a public setting.

Data leakage can occur through the simplest and seemingly innocuous of actions. An example of this can be seen from a study conducted by Kosinski, Stillwell and Graepel (2013, p. 1), which had 58,000 volunteers participate. Information gathered from the participants were "Likes" from Facebook, which were used to automatically and accurately predict highly sensitive personal attributes such as "sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness" etc. Buccafurri, Fotia, Lax, and Saraswat (2016) believe that "Likes" pose a serious threat to user privacy; with users unaware of the potential use of data that they innocently generate.

Data Gathering and Designing the Risk Matrix

To obtain details from social media user profiles, the researcher has used a tool called NodeXL which will return the resultant data. NodeXL is a free, open-source template for Microsoft Excel 2007, 2010

Table 1. Facebook Profile Fields

Field Name	Field Name
First Name	Picture
Middle Name	Profile Update Time
Last Name	Time Zone
Hometown	Sex
Hometown City	Relationship
Hometown State	Music
Hometown Country	TV
Current Location	Movies
Current Location City	About Me
Current Location State	Online Presence
Current Location Country	Locale
Birthday	

and 2013 that makes it easy to explore network graphs. This tool was created by the Social Media Research Foundation (2015). This group of researchers and practitioners working to create open tools, generate and host open data, and support open scholarship related to social media. The Social Media Research Foundation (2015) advises that when used in combination with the Social Network Importer for NodeXL, an add-in social media network graph data provider for NodeXL, users can directly download and import a variety of Facebook Fan Page and Group networks. Data returned by this tool includes details from a single user profile; therefore, a substantial number of participants is required. The tool populated the following Facebook profile fields:

In designing the risk matrix, assignment of weighting must be established. Breaking the weighting into two areas, firstly the weighting of singular fields and secondly weighting based on the likelihood of the field containing data.

Once the data has been gathered the matrix will contain the following data:

The greyed fields in Table 2 indicate that these fields were mandatory as part of setting up the Facebook account. In the example below the mandatory fields are also marked grey.

By using the Microsoft Excel function ISBLANK, the zeros (TRUE) and ones (FALSE) can easily be determined. As can be seen from this example, the data is guaranteed anonymity as only zeros and ones are used to populate the fields. For the spreadsheet prototype 111 user profiles where used; the data shown below is represented by one row equaling one profile.

The detail shown in Table 3 is the percentage for TRUE indicated by green text (if the field is left blank) or FALSE indicated by red text (if the field has data populated). These percentages were calculated on a sample of 111 user profiles. From this data, the determination of likelihood becomes easier.

In the context of this study 'likelihood' will be defined as per Kaplan and Garrick (1981, p. 17) who state that it is a numerical measure of a state of knowledge, a degree of belief, a state of confidence. The term 'consequence' will be defined for the purpose of this study as stated in the International Standards Organisations (2009) 3100:2009 Risk Management – Principles and Guidelines, as an outcome of an event that affects objectives.

For determining consequence in the risk matrix, we must contextualise the situation. In this scenario, the consequence of the risk is having one's identity stolen through the abundance of PII

Table 2. Example of generated data

First Name	Middle Name	Last Name	Hometown	Hometown City	Hometown State	Hometown Country	Current Location	Current Location City	Current Location State	Current Location Country	Birthday
1	0	1	1	1	1	1	1	1	1	1	1
Picture	Profile Update Time	Time zone	Sex	Relationship	Music	TV	Movies	About Me	Online Presence		Locale
1	1	0	1	1	1	1	1	1	1		1

Table 3. Percentage of responses from the prototype

First Name	Middle Name	Last Name	Hometown	Hometown City	Hometown State	Hometown Country	Current Location	Current Location City
100	9.01	100	68.47	68.47	67.57	68.47	66.67	66.67
0	90.99	0	31.53	31.53	32.43	31.53	33.33	33.33

Current Location State	Current Location Country	Birthday	Picture	Time zone	Sex	Relationship	About Me	Online Presence	Locale
65.77	66.67	64.86	100	0.9	100	49.55	24.32	100	100

within the user profile. By using percentages generated by the FALSE value, that is the field being populated; a range can now be generated.

The percentages shown in Table 3 allowed the researcher to gauge the types and frequency of personal information entered into atypical Facebook user profile. This data enabled the development of risk index required for the risk matrix and colour assignment. The risk index has two key elements severity and probability. Huihui et al. states that severity is the estimated impact of each risk when the related incident occurs and probability as the occurrence of each risk (Huihui, An, & Ning, 2010). Table 4 illustrates the generation of the risk index from the severity and probability. The elements of probability range 0.00~0.10 at unlikely to occur to the range of 0.90~1.00 as highly likely to occur. These elements are divided into levels low, medium, substantial, high and extreme.

Having explained the basis of the prototype, the use of sample data, preparation of the data for analysis, and the procedures that were used to generate likelihood and consequence, we now proceed to the discussion and development of the risk matrix.

Risk

Risk is part of everyday life. As previously stated, there are many risks associated with social media; thus as our need to communicate and collaborate with each other increases, so too does the level of risk.

Standards Australia (2009, p. ii) state that 'risk' can be described as the "effect of uncertainty on objectives". Rowe (1988) alternatively states that there is "potential for the realisation of the unwanted, negative consequences of an event". Pickering and Cowley (2010, p. 10) state that risk is considered as a derivation of an "estimate of probability or likelihood and consequence or severity".

Risk will be defined in this study as a function of likelihood and consequence. The combination of grades of consequence and likelihood creates risk rank.

Table 4. Risk Index Generation

Extreme	M	S	H	E	E
High	L	M	S	H	E
Substantial	L	M	M	S	H
Medium	L	L	M	M	S
Low	L	L	L	L	M
Origin	0.00~0.10	0.10~0.40	0.40~0.60	0.60~0.90	0.90~1.00

$$R = f\left(L\ ,C\right)$$

Smith, Siefert and Drain (2008), Cox (2008) and Donoghue (2001) concur that where L (likelihood) and C (consequence) can be quantified on ratio scales, making the multiplication operator meaningful is simple.

Acceptable Risk

When using any product there is a level of risk attached to the use. Ideally, the risks should be zero. Risk acceptance is a strategy whereby an individual or team decides to acknowledge the risk and not take any action unless the risk occurs. This strategy is adopted where it is not possible or cost-effective to address a specific risk in any other way (Project Management Institute, 2013).

Fox-Glassman and Weber (2016) simply explains that an acceptable risk level is a level that is ''good enough''. To elucidate further, the advantages of increased safety are not worth the costs of reducing risk by restricting your activity (Fox-Glassman & Weber, 2016). If an activity's existing level of risk is acceptable, no special action need be taken to increase its safety.

In the context of this study, acceptable risk will pertain to the amount of personally identifiable information required to open a social networking account. Any extra information entered into the profile increases the potential for the loss of identity.

Vulnerability

Sanghera et al. (2007, p. 324) state that risk and vulnerability go hand in hand; whether creating a disaster recovery plan, crossing the road or when developing a risk matrix. The Oxford Dictionary (2015) defines 'vulnerability' as being "exposed to the possibility of being attacked or harmed, either physically or emotionally". Cardona (2004, p. 1) further defines "vulnerability as the internal risk factors of a system that if exposed to a hazard can be affected or susceptible to damage." In the context of this paper, 'vulnerability' occurs wherever user privacy settings can reveal personal information.

RISK MATRIX

To assist in the generation of colour to show the level of vulnerability, a value must be generated. The resultant value will be obtained by applying a risk matrix. Cox (2009, p. 102) defines a risk matrix as having several categories "of probability and likelihood or frequency for its rows (or columns) and several categories of severity, impact or consequences for its columns (or rows)". Standards Australia (2004) further defines risk matrices as a "display of the two-variable relationships between likelihood and consequence". These are measured fundamentals of risk.

The characteristics of an effective risk matrix include but are not limited to having a consistent likelihood ranges that cover a full range of possible situations; provide detailed descriptions of the

consequences that relate to each consequential range; clearly define tolerable and intolerable risk level; provide guidance on what necessitates action in order to mitigate the scenarios with intolerable risk levels and lastly be easy to understand (Ristic, 2013).

To evaluate risk in this study, the Borda method will be applied. Stutzke (2005) states that the Borda method grades the risk from the "greatest to the least critical, on the basis of the multiplication criteria". Huihui et al. (2010) agree that the Borda method significantly reduces "the number of risk ties because of its quantitative calculation"; this methodology does not require any further subjective assessments.

This approach requires the following variables: (derived from Huihui et al. (2010))

- n - the number or risks to be evaluated
- i - impact of risk to be evaluated
- k - the evaluation criteria (consequence, likelihood)
- m - the number of k (usually m=2)
- R_{ik} - the number of risk with a higher level than risk i under the criteria k
- B_i - the Borda index for risk

Th Borda index for each risk can be calculated by the following formula (Huihui, An, & Ning, 2010, p. 1272);

$$b_i = \sum_{k=1}^{m} (N - R_{ik})$$

Colour Coding

The choice of colours used as indicators for this study are important and had to be recognisable to the user. It was decided for the purposes of this study to use a combination of International and Australian Safety Standard colours. Upon investigation the colours listed below are based on the International Standard (2011) ISO 3864-1: Graphical symbols — Safety colours and safety signs (Part 1: Design principles for safety signs and safety markings and Standards Australia (1985)). AS 1318-1985: SAA Industrial Safety Colour Code were parallel to those listed in Australian Standard AS 2700-2011 Colour standards for general purposes (SAI GLOBAL, 2011).

Table 5 describes the colours that will be used by the risk matrix. It also describes the combination of the colours Red, Blue, Green (RGB) to display the appropriate safety colour.

In the matrix seen in Table 5 the Likelihood (probability) and consequence (adverse result of the event) and the colour that is assigned to the risk rating value. The 5x5 matrix described below is typical of those created according to AS/NZS ISO 31000:2009 which was the first international risk management standard using AS/NZS 4360:2004 as the first draft (International Standards Organisation, 2009).

Table 6 describes the level of risk along with a description of the consequence attached. The baseline will be centred on the mandatory fields needed to create the profile. A risk rating of four will be awarded, as the First Name and Last Name fields are combined to give a single field.

Semi-Quantitative Risk Assessment

There are three methods to perform a risk assessment; qualitatively, semi-quantitatively and quantitatively. This study will be adopting the semi-quantitative method. To assist in this quantification, the study will employ a risk matrix.

Table 5. Colour Coding

Colour Name	RGB Code	Sample
Australian Standard AS2700 R13 Signal Red	186, 48, 43	
Australian Standard AS2700 G21 Jade	18, 116, 82	
Australian Standard AS2700 B23 Bright Blue	23, 79, 137	
Australian Standard AS2700 Y15 Sunflower	255, 167, 8	
Australian Standard AS2700 X15 Orange	227, 108, 42	

Table 6. Example 5 x 5 Risk Matrix

	Consequence	Insignificant	Minor	Serious	Major	Catastrophic
Likelihood	Weighting	1	2	3	4	5
(L)ow	1	L 1	L 2	L 3	L 4	M 5
(M)edium	2	L 2	L 4	M 6	M 8	S 10
(S)ubstantial	3	L 3	M 6	M 9	S 12	H 15
(H)igh	4	L 4	M 8	S 12	H 16	E 20
(E)xtreme	5	M 5	S 10	H 15	E 20	E 25

The World Health Organisation (2009, p. 37) states that Semi-quantitative risk assessment offers a transitional level between the "textual evaluation of qualitative risk assessment and the numerical evaluation of quantitative risk assessment, by evaluating risks with a score".

Radu (2009) states that this methodology is used to describe a relative risk scale. A semi-quantitative approach allows the use of different scales to distinguish the likelihood of an undesirable event occurring and the subsequent consequences. Radu (2009, p. 646) believes that the use of semi-quantitative assessments is particularly useful as the quantification of risk is difficult.

The World Health Organisation (2009, p. 37) technique offers a more consistent and rigorous approach to "assessing and comparing risks and risk management strategies than does a qualitative risk assessment, and avoids some of the greater ambiguities that a qualitative risk assessment may produce".

Gadd et al. (2003, p. 14) states that in conducting semi-quantitative risk assessments, "simple qualitative techniques, supplemented by for example measurements to identify the presence of hazards or the use of simple modelling techniques may be appropriate". Gadd et al. (2003, p. 14) also discuss modelling techniques may be used to "derive order of magnitude estimates of the severity of the consequences and likelihood of realisation of hazards". These estimates can be combined to obtain estimates of the order of magnitude of the risk.

Table 7. Risk Level Descriptions

Risk Level	Description	Consequence	Likelihood (of field in Facebook user profile being populated)
Low	Safe – the profile contains minimal personally identifiable information. This level of risk will be used as a baseline.	Insignificant - Theft of identity is low.	>10% chance of field being populated (extremely unlikely to occur)
Medium	General Warning (Informational) – profile contains some personally identifiable information.	Minor - Theft of identity is minimal	>25% chance of field being populated (unlikely to occur)
Substantial	Action Required – profile contains a substantial amount of personally identifiable information.	Serious Theft of identity is substantial.	>50% chance of field being populated (May occur about half of the time)
High	Immediate Action Required - profile contains a high amount of personally identifiable information.	Major - Theft of identity is likely.	>70% chance of field being populated (likely to occur)
Extreme	Unsafe - profile contains a large amount of personally identifiable information.	Catastrophic - Theft of identity is highly likely.	99% chance of field being populated (very likely to occur)

TOOL DESIGN

Within social media, there are ever increasing privacy issues. The tool designed as part of this study will try to limit a users' vulnerability by visually alerting them to the contents of their profile.

The functionality of the extension will be such that when a user is modifying a Facebook profile, the web browser page will change colour as an indicator of vulnerability the development of a web browser extension (Vena) will be the outcome of this research project.

Vena will not store profile information; instead profile fields will be populated with 0s and 1s to aid in the determination of the vulnerability total. These methods will be used to calculate a value based on the risk matrix; a total field will be populated and a value will be passed to a total counter. The total counter will store a value that has been assigned a colour; the webpage background colour will be stored within a cookie.

Vena will be first created to suit the Chrome browser. The reasoning behind the choice of browser is based on statistical usage. Chrome usage as of June 2016 was at 52.76% popularity (PC Advisor, 2016). The browser extension will then be adapted to suit the other available browsers such as Internet Explorer, Firefox, and Safari;

Tool Design Stages

The software developed for the outcome of this study will be known as Foundation Software. The new extension Vena will be developed to suit individual users. The web extension will use the Facebook API (application programmable interface) to sign into the social media user's account and retrieve profile details; perform the value calculations and change the web page background colour.

Figure 1 provides a high level overview of the development of Vena. Further adaptions to the Foundation Software are comprehensively describing the development and potential of the tool is listed in Table 8.

Accessibility

The developer recognizes the importance of allowing people of all abilities to use Vena. At the initial stage of development (Stage 1) Vena will not possess the features to allow those with low vision to use the extension easily.

In adopting WCAG 2.0 and the Colour Contrast Analyser as described in Table 8. Vena will become a universally accessible tool to assist all users of social networks protect their PII.

CONCLUSION

The use of social networks has embedded itself into our culture. In embracing, these networks the architects have placed the onus of regulation of their use onto the individual.

Solutions proposed in the literature for the privacy issues discussed above include the application of complex algorithms to perform privacy preservation of PII. These remove the involvement of the user, and the methodology has the potential to increase vulnerability as users are not aware of the amount of PII held within their user profile.

Using a risk matrix as a tool to determine user vulnerability will allow this study to discover the extent to which privacy of PII within social networks can be improved through the use of colour.

This tool could be used as a basis for the development of interactive interfaces to assist social networking users with protecting their PII in the ever increasing transparent social world.

Figure 1. Vena design phases

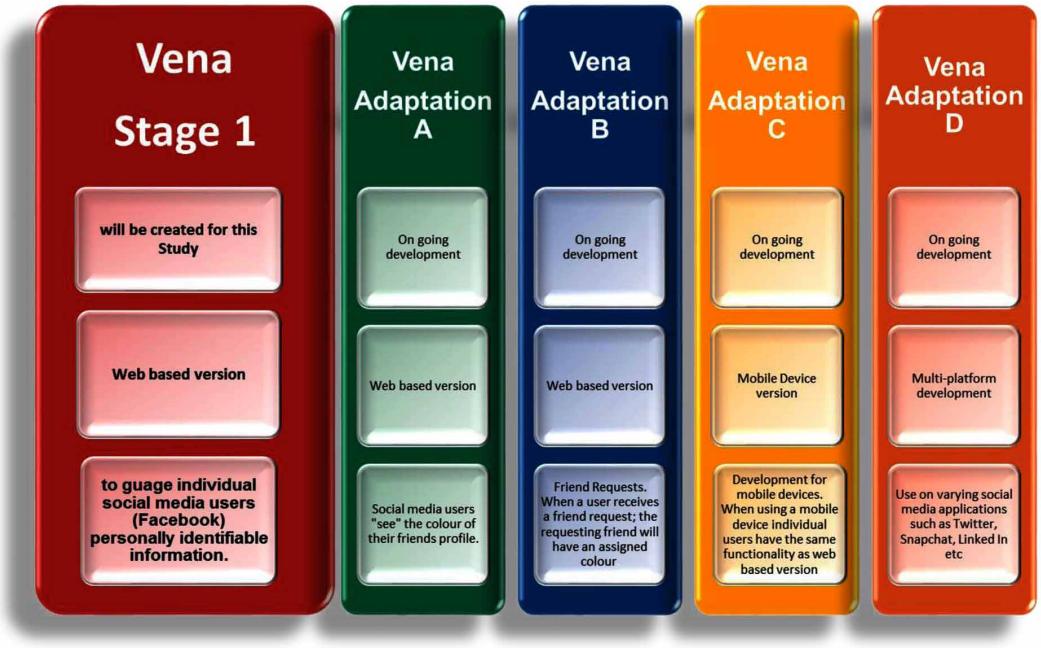

Table 8. Phases of tool development

Adaption	Description
A	Vena could be modified to read names from the friend list of the social media user and if the friend had Vena installed retrieve the number (risk value) and display a coloured dot beside the friends name. Thus replacing the user notification of the green dot as the indicator "I am online". Aiding in increasing social media literacy and the use of privacy preservation techniques when interacting with friends. Social media literacy is having the "proficiency to communicate appropriately, responsibly, and to evaluate conversations critically within the realm of socially-based technologies". Privacy preservation techniques are some simple strategies that can be employed to keep your information as private as possible. These techniques to untagging photos, Deletion of content, blocking Friendship requests and managing default privacy settings. Accessibility features will be added to allow those with low vision to access the extension. These features will be in line with those described in WCAG 2.0 (Web Content Accessibility Guidelines). These accessibility guidelines explain how to make web content available to all users of the world wide web. (W3C, 2016) In this phase of development consideration into the use of text instead of colour to assist those who use screen readers when using internet browsers. Other tools under consideration will include a tool developed by Vision Australia – Colour Contrast Analyser. This tool is primarily for checking foreground & background colour combinations to determine good colour visibility (Vision Australia, 2016). These features will be easily turned on or off through a toggle switch on Vena's Control Panel.
B	Of the development would see users who would have Vena installed making and receiving friend requests. When a social media user receives a friend request; the colour of the profile will be attached. Based on the colour a user can then accept or decline the request. Again this employs privacy preservation techniques.
C	Sees Vena going mobile; with over 655 million mobile only users record in the second quarter of this year. This version would have the same functionality as its web based counterpart.
D	The majority of social media applications have APIs to allow third party programmes to be developed. There would be nothing stopping the application of Vena on a host of differing social media applications.

REFERENCES

W3C. (2016). Web Content Accessibility Guidelines (WCAG) 2.0. Retrieved from https://www.w3.org/TR/WCAG20/

Advisor, P. (2016). Best web browser 2016: Chrome vs Firefox vs Edge vs Safari vs IE and more. Plus: Opera adds VPN, ad blocker and low-power mode. Retrieved from http://www.pcadvisor.co.uk/feature/software/best-web-browser-2016-internet-3635255/

Anderson, A. (1997). *Media, Culture and the Environment*. University of Plymouth: Routledge.

Anthony Tony Cox, L. (2008). What's wrong with risk matrices? *Risk Analysis*, *28*(2), 497–512. doi:10.1111/j.1539-6924.2008.01030.x PMID:18419665

Australia, S. (1985). AS 1318-1985 SAA Industrial Safety Colour Code.

Australia, S. (2004). HB436:2004. *Handbook: Risk Management Guidelines:Companion to AS*, *NZS4360*, 2004.

Australia., S. (2004). AS/NZS ISO 4360:2004 Risk management.

Australia., S. (2009). AS/NZS ISO 31000:2009 Risk management—Principles and guidelines.

Australia, V. (2016). Colour Contrast Analyser. Retrieved from https://www.visionaustralia.org/businessandprofessionals/digitalaccessconsulting/resources/toolstodownload/colour-contrast-analyser

Baresch, B., Knight, L., Harp, D., & Yaschur, C. (2011). Friends who choose your news: An analysis of content links on Facebook. *Paper presented at the ISOJ: The Official Research Journal of International Symposium on Online Journalism*, Austin, TX.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*. Retrieved from http://firstmonday.org/article/view/1394/1312_2

Boyd, D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. MacArthur foundation series on digital learning–Youth, identity, and digital media.

Buccafurri, F., Fotia, L., Lax, G., & Saraswat, V. (2016). Analysis-preserving protection of user privacy against information leakage of social-network Likes. *Information Sciences*, *328*, 340–358. doi:10.1016/j.ins.2015.08.046

Buglass, S. L. B., & Jens, F.; Betts, Lucy R.; Underwood, Jean D.M. (2015). When 'friends' collide: Social heterogeneity and user vulnerability on social network sites. *Computers in Human Behavior*, 2015, 62–72.

Cardona, O. D. (2004). The need for rethinking the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management. In *Mapping vulnerability: Disasters, development and people* (p. 17).

Caron, X., Bosua R., Maynard, S.B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law and Security Review*, 32(1), 4 - 15.

Cox, L. A. Jr. (2009). *Risk analysis of complex and uncertain systems* (Vol. 129). Springer Science & Business Media. doi:10.1007/978-0-387-89014-2

Donoghue, A. M. (2001). The design of hazard risk assessment matrices for ranking occupational health risks and their application in mining and minerals processing. *Occupational Medicine*, *51*(2), 118–123. doi:10.1093/occmed/51.2.118 PMID:11307687

Dumas, G., Serfass, D. G., Brown, N. A., & Sherman, R. A. (2014). The Evolving Nature of Social Network Research: A Commentary to Gleibs (2014). *Analyses of Social Issues and Public Policy (ASAP)*, *14*(1), 374–378. doi:10.1111/asap.12055

Folkenflik, R. (2011). Anonymous was a writer. *LATimes.* Retrieved from http://articles.latimes.com/2011/dec/27/opinion/la-oe-1227-folkenflik-anonymous-20111227

Fox-Glassman, K. T. W., Elke U. (2016). What makes risk acceptable? Revisiting the 1978 psychological dimensions of perceptions of technological risks. *Journal of Mathematical Psychology*. doi:10.1016/j.jmp.2016.05.003

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information*, *2*(1), 140–165. doi:10.3390/info2010140

Gadd, S., Keeley, D., & Balmforth, H. (2003). *Good practice and pitfalls in risk assessment*. Health & Safety Laboratory.

GLOBAL, S. (2011). AS 2700-2011 Colour standards for general purposes.

Gundecha, P., Barbier, G., Tang, J., & Liu, H. (2014). User Vulnerability and its Reduction on a Social Networking Site. *Journals of Transactions on Knowledge Discovery from Data*.

Hayward, S. (2011). Literary Camouflage. Retrieved from http://www.wsj.com/articles/SB10001424052702303657404576359331656789852

Hogan, B. (2012). *PSEUDONYMS AND THE RISE OF THE REAL-NAME WEB A Companion to New Media Dynamics* (pp. 290–308). Chichester: Blackwell Publishing Ltd.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27. doi:10.1111/j.1539-6924.1981.tb01350.x PMID:11798118

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(15), 5802–5805. doi:10.1073/pnas.1218772110 PMID:23479631

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Paper presented at the2nd ACM workshop on Online social networks*. doi:10.1145/1592665.1592668

Lu, S., Ham, J., & Midden, C. (2016, April 5-7). Red Radiators Versus Red Tulips: The Influence of Context on the Interpretation and Effectiveness of Color-Based Ambient Persuasive Technology. In A. Meschtscherjakov, B. De Ruyter, V. Fuchsberger, M. Murer, & M. Tscheligi (Eds.), Persuasive Technology: 11th International Conference, PERSUASIVE 2016, Salzburg, Austria (pp. 303-314). Cham: Springer International Publishing. doi:10.1007/978-3-319-31510-2_26

Ni, H., Chen, A., & Chen, N. (2010). Some extensions on risk matrix approach. *Safety Science*, *48*(10), 1269–1278. doi:10.1016/j.ssci.2010.04.005

Oeldorf-Hirsch, A., & Sundar, S. S. (2015). Posting, commenting, and tagging: Effects of sharing news stories on Facebook. *Computers in Human Behavior*, *44*, 240–249. doi:10.1016/j.chb.2014.11.024

Organisation, I. S. (2009). AS/NZS ISO 31000:2009 Risk management—Principles and guidelines.

Organisation, I. S. (2011). ISO 3864-1:2011(E) Graphical symbols — Safety colours and safety signs Part 1: Design principles for safety signs and safety markings.

Organisation, W. H. (2009). Semi-quantitative risk characterization. In *Risk characterization of microbiological hazards in food*. Geneva: World Health Organisation.

Pickering, A., & Cowley, S. P. (2010). Risk matrices: Implied accuracy and false assumptions. *Journal of health and safety research and practice*, 2(1).

Radu, L.-D. (2009). Qualitative, semi-quantitative and, quantitative methods for risk assessment: case of the financial audit. *Analele Stiintifice ale Universitatii" Alexandru Ioan Cuza" din Iasi-Stiinte Economice*, 56, 643-657.

Raghunathan, B. (2013). *The Complete Book of Data Anonymization: From Planning to Implementation*. CRC Press.

Rowe, W. D. (1977). *An Anatomy of Risk John Wiley & Sons*. New York, NY.

Sanghera, P., & Thornton, F. (2007). How to cheat at deploying and securing RFID. Burlington: Syngress Publishing Inc.

Sar, R. K., & Al-Saggaf, Y. (2014). Contextual integrity's decision heuristic and the tracking by social network sites. *Ethics and Information Technology*, *16*(1), 15–26. doi:10.1007/s10676-013-9329-y

Smith, E. D., Siefert, W. T., & Drain, D. (2009). Risk matrix input data biases. *Systems Engineering*, *12*(4), 344–360. doi:10.1002/sys.20126

Social Media Research Foundation. (2015). *Social Media Importer*. Retrieved from http://socialnetimporter.codeplex.com/

Stutzke, R. D. (2005). *Estimating software-intensive systems: projects, products, and processes*. Pearson Education.

Sundar, S. S. (2008). Self as source: Agency and customization in interactive media.

Thornton, F., & Sanghera, P. (2011). How to cheat at deploying and securing RFID. Syngress.

van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press. doi:10.1093/acprof:oso/9780199970773.001.0001

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: Challenges and opportunities. *IEEE Network*, *24*(4), 13–18. doi:10.1109/MNET.2010.5510913

Zhu, X. G. J. (2011). Privacy Preserving Data Mining. In P. K. Funatsu (Ed.), *Privacy Preserving Data Mining*. New Fundamental Technologies in Data Mining.