VeilMe: An Interactive Visualization Tool for Privacy Configuration of Using Personality Traits

Conference Paper · April 2015

DOI: 10.1145/2702123.2702293

6 authors, including:

Liang Gou
VISA Research
31 PUBLICATIONS **316** CITATIONS
SEE PROFILE

Anbang Xu
IBM Research, Almaden
44 PUBLICATIONS **424** CITATIONS
SEE PROFILE

Michelle Zhou
Association for Computing Machinery
19 PUBLICATIONS **385** CITATIONS
SEE PROFILE

Huahai Yang
Juji, Inc.
33 PUBLICATIONS **427** CITATIONS
SEE PROFILE

VeilMe: An Interactive Visualization Tool for Privacy Configuration of Using Personality Traits

Yang Wang
University of California Davis
Davis, CA, USA
ywang@ucdavis.edu

Liang Gou
IBM Research - Almaden
San Jose, CA, USA
lgou@us.ibm.com

Anbang Xu
IBM Research - Almaden
San Jose, CA, USA
anbangxu@us.ibm.com

Michelle X. Zhou
Juji Inc.
Saratoga, CA, USA
mzhou@acm.org

Huahai Yang
Juji Inc.
Saratoga, CA, USA
huahai.yang@gmail.com

Hernan Badenes
IBM Argentina
Buenos Aires, Argentina
hdadenes@us.ibm.com

ABSTRACT

With the recent advances in using data analytics to automatically infer one's personality traits from their social media data, users are facing a growing tension between the use of the technology to aid self development in workplace and the privacy concerns of such use. Given the richness of personality data that can be derived today and the varied sensitivity of revealing such data, it is a non-trivial task for users to configure their privacy settings for sharing and protecting their derived personality data. Here we present the design, development, and evaluation of an interactive visualization tool, VeilMe, which helps users configure the privacy settings for the use of their personality portraits derived from social media. Unlike other privacy configuration tools, our tool offers two distinct advantages. First, it presents a novel and intuitive visual interface that aids users in understanding and exploring their own personality traits derived from their social media data, and configuring their privacy preferences. Second, our tool helps users to jump start their privacy settings by suggesting initial sharing strategies based on a set of factors, including the users' personality and target audience. We have evaluated the use of our tool with 124 participants in an enterprise context. Our results show that VeilMe effectively supports various user privacy configuration tasks, and also suggest several design implications, including the approaches to personalized privacy configurations.

Author Keywords

Visual Interface; Personality Traits; Privacy; Sharing Settings; Social Media

ACM Classification Keywords

H.5.2 Information Interfaces and Presentation: User Interfaces - *Interaction Styles*; K.4.1Computers and society: Public Policy Issues - *Privacy*

CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea

http://dx.doi.org/10.1145/2702123.2702293

INTRODUCTION

A person's personality traits—the patterns of individuals' thought, emotion, and behavior, together with the psychological mechanisms behind them—largely impact the person's life outcomes, including their performance in the workplace [9, 2, 30]. Recent advances in psycho-linguistics and machine learning have shown that such traits can now be automatically derived from one's linguistic signals, such as their online social media footprints [11, 37, 40].

Our current work is exploring the use of the derived personality traits to aid employees' self-awareness and self-development in the workplace. In particular, we focus on studying three types of personality traits and their impact on a person's professional life: Big 5 personality [40], human values [3] and fundamental needs [39]. Table 1 summarizes these three types of traits and their use in the workplace.

With the increasing power of gaining deeper insights into themselves, people not only begin to be aware of the potential benefits but have also expressed heightened privacy concerns about revealing these insights about themselves in the workplace. For example, a recent study shows that people perceive a number of benefits and risks of exposing their derived personality traits in the workplace, including self branding and potential misuse of such traits [13]. The users thus have expressed the need of tight controls over the use of such data. While some of their privacy preferences over these data are similar to those on handling their other personal data, such as personal communications (e.g., instant message, email) [24] and work locations [26], the users also want much finer-grained controls over their most intrinsic traits (e.g., exposing Big 5 personality traits but not motivations) due to the power *and* the imperfections of today's data analytics [13].

However, it is a non-trivial task for users to configure their privacy policies for the use of their personality data in the workplace for three main reasons. First, personality data is multi-dimensional and inherently complex for a user to comprehend, let alone setting the privacy policy for each trait. For example, the three types of personality traits that we focus on already include a total of 52 traits (Table 1) at three levels of abstraction. Second, since different personality traits influence a person's professional life differently [30], a user may

Big 5 Personality [40] (Workplace Use: work proficiency, training proficiency, and teamwork [2])	
Openness	Subtraits:*Imagination, Artistic interests, Emotionality, Adventurousness, Intellect, Liberalism*
Conscientiousness	Subtraits:*Self-Efficacy, Orderliness, Dutifulness, Achievement striving, Self-discipline, Cautiousness*
Extraversion	Subtraits: *Friendliness, Gregariousness, Assertiveness, Activity-level, Excitement-seeking, Cheerfulness*
Agreeableness	Subtraits: *Trust, Morality, Altruism, Cooperation, Modesty, Sympathy*
Neuroticism	Subtraits: *Anxiety, Anger, Depression, Self-consciousness, Immoderation, Vulnerability*
Needs [39] (Workplace Use: job incentives, collaboration [39])	
Ideals	a desire for perfection
Harmony	appreciating other people's feeling
Closeness	being connected to family and setting up home
Self-expression	discovering and asserting one's own identity
Excitement	upbeat emotions, and having fun
Curiosity	a desire to discover and grow
Values [3] (Workplace Use: motivations and commitment for jobs [4])	
Self-transcendence	showing concern for the welfare and interests of others
Conservation	emphasizing conformity, tradition, security
Self-enhancement	seeking personal success for oneself
Open-to-change	emphasizing stimulation, self-direction
Hedonism	seeking pleasure and sensuous gratification for oneself

Table 1: Three types of traits used in this work.

not know how to optimize the privacy configurations to balance the benefits and risks of sharing their personality data. Third, there are often many other factors affecting a user's privacy policies over their personality data, including the social groups who can access the data, the purpose of the data use, and the level of trait details to be disclosed.

To help a user effectively configure their privacy policies over the use of their complex personality data without being overwhelmed by the task, we have built an interactive visualization tool, VeilMe. It helps a user to understand, configure, and maintain the sharing preferences of their personality data in the workplace. To help a user jump start the privacy settings, it also suggests an initial set of privacy policies based on a number of factors, including the user's own personality and the privacy policies preferred by other with similar personalitiy.

Compared to existing tools for privacy management and policy authoring and configuration (e.g., [16, 33, 31, 29, 23, 7, 26]), our work offers three unique contributions. First, it introduces a novel but simple visual interface that helps users to effectively explore and understand their personality traits. Second, it supports intuitive visual metaphors and fluid visual interactions that allow users to easily configure their privacy policies involving a number of parameters *simultaneously* based on the "social distance" of target audience. Third, it incorporates several strategies to help users configure their initial privacy policies, which further reduces the users' efforts in their privacy configuration tasks.

To evaluate the effectiveness of VeilMe, we have deployed the tool in a large IT company and conducted a study with 124 participants. Our results are encouraging. It demonstrates the helpfulness of our tool in support of users' privacy configuration tasks over their own personality data. The study has also enriched our understanding on how people use such a tool in the real world and suggested several important design implications, including the effective use of different visual metaphors in configuring privacy policies.

The rest of paper is organized as follows. We first give a brief introduction to the related work, and then present the design rationales and details of VeilMe. Finally, we describe our study design and results, and discuss design implications learned from our study.

RELATED WORK

Personality Modeling on Social Media

There are many research efforts in modeling and analyzing people's traits from various data sources. For example, some work attempts to predict Big 5 personality from essays and conversation scripts [22] and emails [34]. There is also a rich body of work on predicting personal traits from social media, such as extracting an individual's demographics and political orientation from Twitter [28], and inferring one's emotional states from Twitter [6]. Some other efforts use social behavior to predict Big 5 personality [1]. Golbeck et al. show how to predict Big 5 personality from social media [12] by using both linguistic and social behavior signals.

In this work, we used three personality models rooted in psycho-lingusitic analysis, including a Big 5 personality model [40] and a model of human values [3] built with LIWC dictionary [37], a model of fundamental needs with a self-constructed dictionary [39]. We implemented the three models in our system with people's twitter data, and the model implementation is beyond the focus of this work.

Privacy about Personal Data

On the other hand, researchers in HCI community show extensive interests in understanding users' privacy preferences of different personal data [15]. Many work has been done to understand personal data including personal communications (e.g., instant message, email, and social media) [24], and location-based activities [18]. Occasionally, there are some work examining the relation among people's privacy and their personality traits. For example, it is showed that people's trust and risk propensity impact their privacy concerns [35], and certain dimensions of Big 5 personality traits influence one's privacy concerns [17, 19]. A recent study shows that people's sharing preferences of such traits are related to several factors in the workplace, including social groups who can access the traits, the control of trait granularity, the trait properties of types and values, and the context of benefits and risks [13].

To sum up, this work of system and visual interface design is grounded in and guided by these studies. Especially, it leverages the results from this work [13] by supporting flexible control over various factors of social groups, trait types and values, trait granularity under in the workplace context.

Interactive User Interface for Privacy Settings

With increasing attention on privacy issues around personal data, some tools have been proposed to assist users to comprehend and configure privacy settings in a networked environment. Some visual interfaces are designed to help people understand their privacy settings. For example, the Facebook audience preview allows users to preview how the individual friends or public to see their profile [16]. Schlegel et. al. used a visual metaphor of eyes to show the amount of personal information accessed by others [33].

Besides supporting the comprehension of privacy settings, other tools are provided for configuring and maintaining such settings. Two notable interactive visualization tools were proposed for security policies configuration. Rode et. al. used a circled pie chart like visualization to show access activity of system files and configure the access policy [31], while Reeder et al. presented an expandable matrix interface to achieve a similar purpose [29] and found this interface is complementary with Facebook audience view [20]. While these tools majorly focus on security and access control on file systems, other tools were proposed for sharing settings of personal data. PViz uses a bubble chart based visual interface to support sharing settings for Facebook and suggests automatically generated social groups to reduce configuration efforts [23]. A similar Venn Diagram interface is used for social network policy configuration for different social groups [7]. MySpace utilizes interactive visualization of physical workplaces to support configuring access policies about availability and location in workplace [26].

To conclude, the visual interface in this work is inspired by above work, but differentiates itself in several ways. This work considers the uniqueness of sharing personality portrait in the workplace setting, such as complicated structure of personality portraits, multiple levels of sharing control on social groups, trait types and values. It is difficult to apply above tools address this problem. Also, this design proposes intuitive visual metaphors to help users understand their personality portraits and configure sharing preferences of portraits.

Privacy Policies Generation

While user interface attempts to help users specify their privacy settings, many other work focuses on generating meaningful privacy preferences for users. These efforts usually take two strategies: rule based and machine learning based approaches. The rule based ones identify important factors impacting sharing, such as information content, social relationship, context, and time, to generate sharing policies for different users or user groups [32, 27]. Meanwhile, some work introduces machine learning techniques to predict a user's sharing preferences with various features, such as social network information [8], sensitivity and visibility of the shared information [21].

In this work, we experimented both rule based and machine learning based strategies which are intergrated into our visual interface as the default sharing settings. Personality traits were used as additional features to predict the sharing preferences in our model. The goal here is to find a good default settings strategy to reduce users' efforts to adjust the sharing settings over complicated personality portraits.

VEILME

In this section, we introduce the design goals, implementation details and strategies of generating initial privacy settings in VeilMe.

Design Goals

To help users with the privacy settings for their personality portraits, VeilMe should meet following design goals:

DG1 ***It should provide an intuitive visual representation for personality portrait***. A user needs to fully understand her personality portrait before she can configure the privacy settings for such traits. In our case, a personality portrait includes multiple dimensions (e.g., "Big 5", "Needs", etc.) and a hierarchical structure (there are sub-traits under Big 5 traits). The goal is to design a scalable visualization of such a personality portrait with a capability of an overview and detail-on-demand.

DG2 ***It should help users to be aware of their privacy settings***. According to previous literature, it is critical for users to have the awareness of WHAT information (personality traits) can be accessed, by WHOM (social groups), and with HOW MUCH detail (trait sharing granularity). The visual interface should provide users a quick overview of such information.

DG3 ***It should enable users easily control of their sharing preferences***. It is a non-trivial task to configure the sharing preferences for personality portrait. Users need to control all three factors in a privacy setting: 1) multiple social groups who may access the traits; 2) the personality traits with a multi-dimensional hierarchical structure; 3) sharing granularity of traits. Thus, the system should provide an intuitive user interface for users to easily control these factors.

DG4 ***It should provide a personalized initial privacy setting***. As mentioned above, it is a tedious process to adjust the sharing preferences of the multi-dimensional hierarchical portraits for various social groups. It would be beneficial to provide a personalized initial default privacy setting to reduce users' efforts on setting adjustment.

User Interface

The user interface of VeilMe is shown in Figure 1. Panel A and B show a user's twitter profile and her latest tweets. Panel C in the middle left shows the visualization, PersonalityGenome, to support interactive exploration of one's personality portrait. On the right is the privacy setting panel (Panel D), where a user can configure her sharing preferences of the personality portrait.

PersonalityGenome Visualization (DG1)

One key component of the VeilMe is to visualize the derived personality portrait for interactive exploration. As mentioned before, the portrait data is both multi-dimensional and hierarchical. It consists of three main trait types: *Big 5 Personality*, *Needs* and *Values* (see Table 1). Within each type, a group of

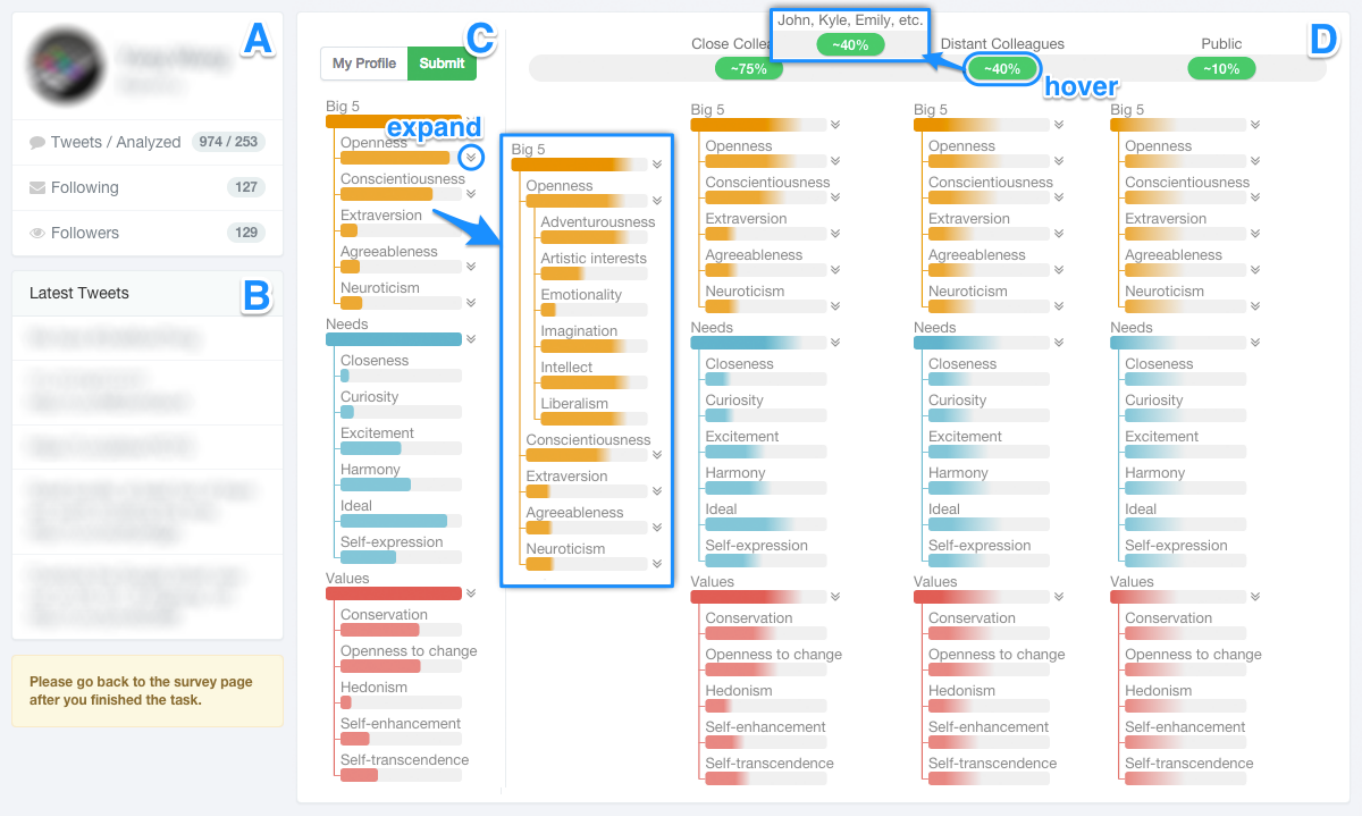


Figure 1: The screenshot of the VeilMe interface. Panel A & B: user's twitter profile and the latest tweets; C: portrait exploration panel; D: privacy setting panel. User can click to expand to reveal traits with sub-traits. When hovering a social distance knob, the input audience names of that group will be shown for user engagement. (Refer to the PDF document for better image quality.)

five to six traits are computed with percentile scores against the population. Furthermore, traits in the *Big 5* type contains sub-traits that constitutes a hierarchical structure.

To visualize this multi-dimensional hierarchical data model, we conducted three design sessions with 10 targeted users and tried three visualization mock-ups including a bar chart, node-link tree and radial space filling tree visualization. With the feedback of balancing functionality and aesthetics, we designed *PersonalityGenome*, a visualization inspired by a genome sequence, as shown in Figure 1 panel C. In this visualization, personality traits are piled together as a genome-like bar sequence. Each bar corresponds a trait. The sub-traits are grouped under a leading bar (indicates the parent trait) with links among them showing the hierarchical structure. Different trait types are colored differently. The length of a filled bar reveals the percentile score of each trait, which is also explicitly shown as text overlay on top. A label of trait name is placed over each bar. A control button on the right of a bar can be used to fold and unfold a trait group. A tooltip popup for a bar displays the definition of the corresponding trait.

Interactive Visualization for Sharing Settings (DG2 & DG3)

The SocialDistance Metaphor

In VeilMe, we incorporated a *SocialDistance* metaphor to achieve effective and efficient privacy control. The design rationale is as follows: people have different self-disclosing tendencies towards different social groups, and the *distance* (denoted as d_{sg}) between a person and a social group impacts her sharing willingness [24, 13]. For example, people tend to share more personal information with family members and close friends, but less to the public. Therefore, in our design, we semantically encode the distance of a social group to control how much information will be disclosed to that group.

As depicted in Figure 1 panel D, we applied the *SocialDistance* metaphor to two levels: 1) the position of social groups on the screen; and 2) the degree of faithfulness for each PersonalityGenome to be shared.

Social groups with different distance d_{sg} are visualized as draggable slider knobs. User can easily drag a knob to adjust the social distance of a specific group; consequently, the faithfulness of her portrait to that group will change accordingly: more faithful is dragged leftward, and more fuzzy is dragged rightward.

Under each social group, an obfuscated copy of the original PersonalityGenome is presented to show how users in that group will perceive of the subject's portrait. We adopted the idea of *k-Anonymity*, a frequently used method in privacy-

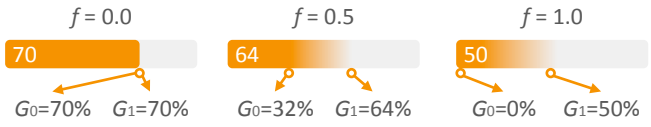


Figure 2: An example of obfuscating a single trait. The fuzziness are, from left to right, 0.0, 0.5 and 1.0, respectively, resulting different $P_{\text{obfuscated}}$ values and gradients.

preserving data mining [36], to develop the *kNN-Anonymity* model for obfuscation of one's PersonalityGenome. The obfuscated portrait can be obtained as:

$$P_{\text{obfuscated}} = kNNA(P_{\text{derived}}, f) \tag{1}$$

where P_{derived} is the derived personality portrait from social footprints and f the injected fuzziness value corresponding to user's interactions. Given a person-specific portrait P_{derived}, The *kNNA* function amalgamates the portraits of the user's k nearest neighbors yielding a obfuscated portrait $P_{\text{obfuscated}}$, from which the user cannot be re-identified. The number k is mapped from f ($k \in [0, n-1] \leftarrow f \in [0, 1]$) and f is determined by the amount of adjustment on UI. f also controls the level of blurriness,

$$G_0 = P_{\text{obfuscated}} * (1 - f), G_1 = P_{\text{obfuscated}} \tag{2}$$

where G_0 and G_1 are the starting and ending position of the gradient control, respectively. An example of the obfuscation is shown in Figure 2.

One extreme of the *kNN-Anonymity* model is, for example, when $k = 0$, the produced portrait $P_{\text{obfuscated}}$ is the exact portrait P_{derived} of the subject. On the other extreme, when k equals to the number of the population n, $P_{\text{obfuscated}}$ becomes an "averaged" portrait of the whole population.

Multiple Control Levels of Trait Obfuscation

In VeilMe we provide multiple levels of control to adjust the obfuscation of a portrait. Users can either drag the knob to adjust the obfuscation for the whole personality portrait at the social distance level, or click and slide on each trait to adjust the obfuscation individually.

To help users with fast configuration, we also introduced a hierarchical interlocking mechanism. If the obfuscation of a trait is changed explicitly and the resulting obfuscation is different from previous, that specific trait will be locked and its fuzziness will not change until user explicitly unlock it. Otherwise, if not locked, fuzziness of finer grained controls will be overridden by that of its parental traits'. An example of the hierarchical interlocking mechanism is explained in Figure 3. Beside locking, we also allow users to hide traits to prevent from being shared completely.

Strategies for Initial Privacy Settings (DG4)

In our study, we explored different strategies of providing useful initial settings to reduce users' efforts. We examined three strategies: 1) a conservative approach, 2) a rule-based approach and 3) a prediction-based approach.

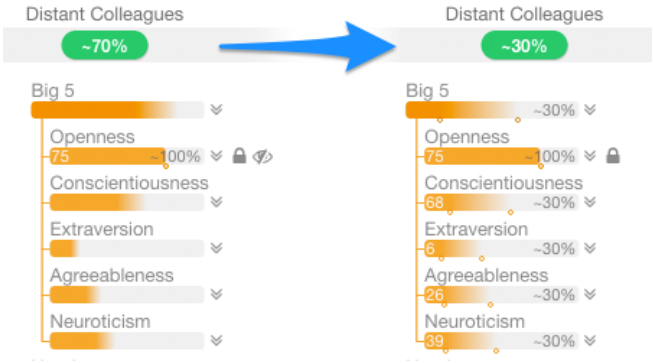


Figure 3: An example of obfuscation and hierarchical interlocking. On the left, the *Distant Colleagues* knob is placed with an overall faithfulness of 70% (30% obfuscation), the child traits inherit the obfuscation level except that obfuscation of trait *Openness* is explicitly changed and locked to 0 (faithfulness 100%). When the knob is dragged rightward to faithfulness 30%, all traits except the locked one are changed.

In the **conservative** approach, we disclosed the least information for all groups with a "privacy pragmatists" assumption [38]. In this approach, all social groups are placed at the far-end on the social distance slider. Traits in PersonalityGenome maintain the lowest level of fidelity. This conservative approach can serve as a baseline when compared with others.

The **rule-based** approach was built upon an observation from previous studies that people tends to share most with close friends and colleagues, but least with the public [24, 13]. From a survey with 224 people of their sharing willingness for different groups [13], we generated an initial settings rule for three default social groups ("close colleagues", "distant colleagues" and "public") with initial faithfulness of 90%, 50% and 10%, respectively.

Lastly in the **prediction-based** approach, we predicted one's sharing willingness for her individual traits towards different social groups based on the derived personality portraits. Again, with sharing willingness ratings from 224 people, we built a kernel (Nadaraya-Watson) regression model for each social group:

$$\mathcal{M}(x) = E[Y|X = x] = \frac{\sum_i^n f(i,x) y_i}{\sum_i^n f(i,x)} \tag{3}$$

where $X_{n \times m}$ is the input portraits ($n = 224$: # of subjects, $m = 16$: # of traits), $Y_{n \times m}$ the output sharing willingness, and $f(i, x)$ a Gaussian kernel with the bandwidth of 0.1.

The model $\mathcal{M}$ can be interpreted as an estimator of weighted average of k nearest neighbors of an incoming portrait. In our study, $k = 7$ gives the highest prediction power (cross-validated) with $R^2 = 0.61$. To prevent potential over-fitting due to limited training samples ($n = 224$) and relative large number of traits ($m = 16$), we applied L1-norm SVM for feature selection, yielding a smaller feature size ($m' = 5$) with marginal drop in prediction accuracy ($R^2 = 0.57$).

EVALUATION

The purpose of the evaluation is to examine how VeilMe meets the design goals mentioned above. This objective can be attained by addressing three questions: Q1) how well the system supports the privacy configuration for sharing personality traits; Q2) what configuration strategies emerge from users' interaction with our system; Q3) how different initial sharing settings affect users' configuration and interaction.

Participants

We invited 1,240 colleagues who have Twitter presence (200+ tweets) as required for extracting personalities. We had 151 completed responses, 124 of which are valid after filtering out unqualified responses based on three criteria (time spent on the tutorials, time spent on the tasks, and one test question for system understanding). Among the valid responses, we had 43 responses for the conservative setting, 40 for the rule-based setting, and 41 for the prediction-based setting. As for demographics, almost half of the participants were from the United States (44.2%), with the rest from Europe (31.4%) and other parts of the world (25.4%), ranging from 25 to 55 in age, most are male (69%), which is representative of a large enterprise or alike. The study took less than 30 minutes to complete and we drew a lottery with $50 Amazon gift card out of 50 people as the compensation for the study.

Procedure

The study consists of two parts: 1) personality portrait exploration, and 2) trait sharing configuration. Each part includes an interactive tutorial, experimental tasks and questions. The whole study was navigated through an online survey.

Personality Portrait Exploration

First, the participants were given the background of the study and the context of personality used in the workplace. Then, they were asked to login with their twitter credentials and the system would lively derive their personality portraits from their tweets. After that, the participants were provided with an interactive tutorial that go through their portraits, and were asked to explore the visualization of their portraits. They were asked to answer three questions about their portrait, including the trait values at both top level (e.g., "Closeness" in Needs) and sub-trait level (e.g. "Cheerfulness" under "Extraversion"), and a trait with maximum score in a trait category. They were also asked to rate how well the results matched their self-assessment. These questions were used to examine how the visualization helped the participants to understand their profile and also to engage them to explore the traits before configuring the sharing preferences. The first question was also used as test questions to filter qualified participants for later analysis.

Trait Sharing Configuration

Before the participants moved to trait sharing tasks, they were solicited for their opinions about the potential benefits and risks of using such personality traits in the workplace. They were first asked to rate the overall benefits and risks identified from previous study [13] (only the top four potential benefits/risks were used) on a 7-likert scale, followed by a task to mark all possible benefits and risks for each trait on top level (not for the sub-traits). With these questions, we want participants to reflect the benefits and risks before they actually used the system to configure their sharing preferences. After answering the benefit and risks questions, the participants were navigated to the sharing preferences setting page. Similarly, an interactive tutorial was popped up to help them go through the interface. At the end of the tutorial, the participants were asked to name three close colleagues and distance colleagues and the input names will be shown on each social group when hovered. The purpose of naming audience they know is to mimic real use scenarios and to engage them to the sharing tasks. The participants were also instructed that the target audience will see the same veiled portrait as they set in the UI, and their preferences will be recorded and used as-is in future deployments.

		Type	Description
Measures	Interaction Log	#Clicks	number of interactions
		ΔChange	amount of value change
		Accuracy	logged vs. reported
	Ctrl. Pref. Rating	PR_{sd}	prefer social dist. level
		PR_{tr}	prefer trait level
	Usability Rating	UR1	easy to explore
		UR2	easy to configure
		UR3	initial setting helpful
		UR4	privacy awareness
		UR5	overall easy to use
Factors	Initial Setting	IS_{con}	conservative setting
		IS_{pred}	prediction-based setting
		IS_{rule}	rule-based setting
	Control Level	CL_g	social distance level
		CL_t	trait level
	Social Group	SG_{cls}	close colleagues
		SG_{dis}	distant colleagues
		SG_{pub}	public

Table 2: Measurements and factors used in the study.

Next, the participants were asked to play with the visual interface and configure their sharing preferences that they feel most conformable. Upon submitting their setting, the participants were asked about their sharing preferences at three levels of social groups, trait categories, and individual traits. The questions include reporting the values of faithfulness for the shared portraits, 7-likert preference rating for adjustment at the two control levels, as well as their comments about their ratings. At last, the participants were asked to answer five usability questions of on a 7 Likert scale (see Figure 4).

Experimental Conditions

To evaluate how different initial setting strategies influence users' sharing preferences, we employed three types of initial settings (*conservative*, *rule-based*, and *prediction-based*) in VeilMe as experimental conditions. The participants were randomly assigned to one of these three conditions to start with and were asked to finish the study described above.

Measures

We used two types of measurements including participants' interaction logs and their subjective ratings (summarized in

Task	Exploration		Configuration		
Questions	Q1	Q2	Q1	Q2	Q3
Accuracy	95.16%	97.99%	93.55%	94.35%	92.74%

Table 3: The accuracy for the trait exploration and the sharing configuration questions.

Table 2). For interaction logs, we counted the number of effective interactions[1] (henceforth referred to as #Clicks) at two control levels (CL) across three default social groups (SG). We also calculated the actual amount of effective change (henceforth referred to as ΔChange). For the subjective ratings, we examined two categories including the adjustment preference ratings (PR) and general usability ratings (UR). The same set of measurements were collected under all three initial settings (IS).

RESULTS AND ANALYSIS

In this section, we report the results of our study and interpret them to answer the evaluation questions proposed earlier. Before diving into these results, we first examined the model performance, and found that the derived traits closely matched the participants' own perception with the means of all self-assessment ratings above 3 (somewhat) out of 5 (perfect). Specifically, we obtained average ratings of 3.45 (sd = 1.21), 3.21 (sd = 1.14), 3.28 (sd = 1.39) for Big 5 personality, values, and needs (more performance discussion in [40, 3, 39, 13]).

Q1: How Helpful VeilMe Is

To answer this question, we assessed the accuracy of the traits exploration and the sharing configuration tasks, and analyzed the usability ratings. Regarding the task accuracies, we compared the values recorded in the system logs and users' answers and found an average accuracy of over 90% was achieved (refer to Table 3), regardless of the initial settings. This indicates the VeilMe interface can effectively support the exploration of the participants' personality portrait and the configuration of their sharing preferences.

As for the usability ratings, VeilMe received around 5 out of 7 for the overall easy-to-use ratings based on the 124 responses (shown in Figure 4). Easy-to-explore obtained the highest ratings of over 5.5 and easy-to-configure also had good ratings of over 5, while privacy-awareness got the lowest ratings around 4.5. Under different initial settings, we did not observe significance for the above ratingss. Notably, we found there is a discrepancy in the ratings for the helpfulness-of-the-initial-settings ($F_{1,122} = 7.29, p = 0.008$), and the rule-based strategy received the highest ratings ($\mu = 5.11, sd = 1.8$). We will discuss this in detail later in Q3.

Q2: How Users Interact with VeilMe

We examined the interaction patterns that the participants adopted from two aspects: control levels (CL) and social groups (SG), with different initial settings (IS) strategies.

[1]Effective interactions is defined as the total number of interactions divided by the number of visual elements (i.e. social distance knobs and trait bars) users interacted with.

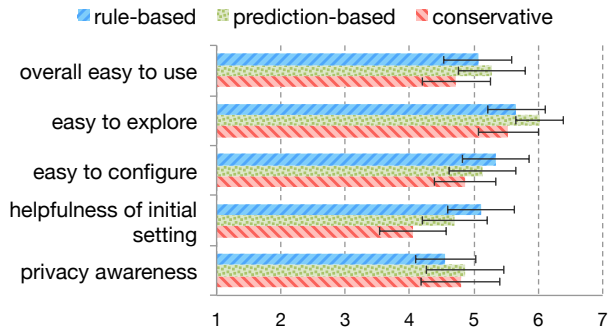


Figure 4: Usability ratings of VeilMe.

	CL×IS			SG×IS		
Measure	Factor	F	p-value	Factor	F	p-value
#Clicks	CL	9.05	0.003***	SG	5.15	0.006***
	IS	0.94	0.391	IS	1.81	0.163
	CL×IS	0.35	0.708	SG×IS	1.02	0.394
ΔChange	CL	1.06	0.347	SG	5.12	0.006***
	IS	1.04	0.308	IS	0.18	0.830
	CL×IS	3.91	0.021*	SG×IS	0.48	0.750
Pref. Rating	CL	8.09	0.005**			
	IS	4.16	0.017*		N/A	
	CL×IS	0.26	0.773			

Table 4: ANOVA analyses of control levels (CL) and social groups (SG) over initial settings (IS).

Interaction Patterns with Control Levels

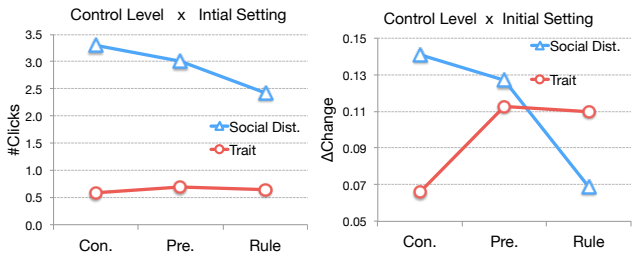
We first investigated how the participants interacted with both CLs to determine whether it is impacted by the initial settings.

The left part of Table 4 shows two-way ANOVA results for three measurements (#Clicks, ΔChange and preference ratings) over two factors (CL and IS). We can see there is significant difference for #Clicks ($F_{(1,244)} = 9.12, p = 0.003$) at the two control level, but no difference for ΔChange. As shown in Figure 5 (a), we can observed that the participants had more interactions at the social distance level (CL_g). This indicates the participants tend to use the social group knob to configure their sharing preferences rather than adjusting each traits individually.

We also compared the subjective ratings of user's preferences over each CL. We found there is main effect of CL ($F_{1,122} = 8.09, p = 0.004$) and participants preferred controlling at the social distance level (PR_{sd}, $\mu = 4.69, sd = 2.0$) than at the trait level (PR_{tr}, $\mu = 3.86, sd = 1.97$), which is consist with the findings from log data and shows that users prefer to use the higher level controls.

Participants' comments also shared the same conclusion that fewer efforts are needed at CL_g. For example, one participant commented: "*I found it easiest to do a quick broad brush setting, rather than having to tinker with each trait, which was fiddly and time consuming.*" Interestingly, someone pointed out preferring to control at CL_g is to keep her portrait consistent: "*I think it's better to share consistently across all the traits so I did not adjust at the finer grained level*".

Interaction Patterns with Social Groups



(a) #Clicks (b) ΔChange

Figure 5: Interaction plots over two factors of control level and initial setting for (a)#Clicks and (b)ΔChange.

We also studied whether the participants' interactions vary on different social groups. On the right of Table 4 we show two two-way ANOVA results for both #Clicks and ΔChange over factors of SG and IS. We can observe significances for both #Clicks and ΔChange at different SGs ($F_{2,363} = 5.15$, $p = 0.006$ and $F_{2,363} = 5.13$, $p = 0.006$, respectively). Post-hoc Tukey tests show that the #Clicks on SG_{cls} (close colleagues, $\mu = 5.18$) is significantly greater than the #Clicks on SG_{dis} (distant colleagues, $\mu = 3.49$) and SG_{pub} (public, $\mu = 3.18$) with $p = 0.032$ and $p = 0.008$ respectively. Similar results were observed for ΔChange: the ΔChange on SG_{cls} ($\mu = 0.58$) is significantly larger ($p = 0.007$ and $p = 0.04$) than that of SG_{dis} ($\mu = 0.21$) and SG_{pub} ($\mu = 0.282$).

This indicates that participants tend to adjust their preferences for closer social groups. One explanation is that people care more about their personal images presented to people that are close to them (SG_{cls}). Therefore they tend to think carefully and interact more on SG_{cls}. For example, one participant commented, "*Social Groups represent people I would like to interact. It seems easier to set (preferences) by the groups which are familiar for me*".

Q3: How the Initial Settings Work

Lastly we focused on how different ISs help the participants to configure their sharing preferences from two aspects: (1) the overall perceived helpfulness of the participants; and (2) the impact of IS strategies on their interaction patterns.

First, there was a significant impact of IS over participant's perceived helpfulness of the tool ($F_{1,122} = 7.29, p = 0.008$), as mentioned above with Figure 4. The helpfulness ratings of IS_{rule} (the rule-based strategy, $\mu = 5.11, sd = 1.8$) is better than IS_{con} (the conservative strategy, $\mu = 4.1, sd = 1.8$) indicated by a post-hoc test ($p = 0.009$).

Secondly, we did not observe any main effect of IS over the participants' interactions (#Clicks and ΔChange) for both CL and SG. (see Table 4). However, we found there is an interaction effect between CL and IS with $F_{2,242} = 3.91$ and $p = 0.008$ for ΔChange. As depicted in the interaction plot in Figure 5 (b), we can see that participants made more changes at CL_g (social distance level) with IS_{con} (conservative strategy), but made more changes at the CL_t (trait level) with IS_{rule} (rule-based strategy).

The above results from both log data and ratings echo each other and show that our rule-based initial setting worked the best in terms of least efforts for sharing preference configuration, especially at CL_g. However, surprisingly, we did not find that IS_{rule} (prediction-based strategy) performed better than the other two strategies. Also, We did not observe significant patterns between the initial and final settings.

DISCUSSION

In this section, we discuss several important design implications that we have learned from our study, and indicate current limitations in our work and some future research directions.

Effective Use of Visual Metaphors in Aiding Configuration

Traditionally, privacy policy configuration has been supported through the use of basic UI elements, such as buttons and check-boxes. Our study results suggest that it is beneficial to utilize the power of visual metaphors in such a task, especially when the task involves complex parameters. For example, we observed that our participants enjoyed using our "social distance knobs" visual interaction metaphor to rapidly adjust their settings by controlling a number of parameters *simultaneously*. This metaphor is semantically intuitive for our participants to grasp as the "draggable knob" helps them easily control how much to reveal "who I am" to different social groups. Since a metaphor-based design gauges people's cognitive capability for new and complicated tasks with existing knowledge from another and often familiar domain [5], we can extend our work by considering the use of additional visual metaphors. For example, we may design a "social sieve" visual metaphor to reveal the associated benefits and risks when particular pieces of information are filtered by the "sieve". This way a user will have an immediate understanding on what benefits can be gained and what are at risk if s/he chooses to share certain pieces of data. Also we should be careful some caution with visual metaphors, such as interaction constraints imposed by metaphor affordance [5].

Social Groups as a Configuration Proxy

Configuring privacy policies over each personality trait is a tedious task. We observed that our users use "social groups" as a proxy to configure their privacy policies. In particular, they adjust their privacy settings as a whole for each group based on their social distance to the group, instead of specifying policies for each individual traits. This observation echos the concept of "privacy tension of social boundaries" [25], which states that disclosure boundaries exits among different social groups. While configuring privacy policies at the group level has certainly simplified a user's task, flexibility must be provided to support fine-grained controls and adjustments, e.g. allowing users to split and merge different social groups for more customized settings.

Moreover, special design attention should be paid to the support of different social groups. In our study, we found that our participants made more adjustments about their privacy settings for their "closer" social groups, since they clearly cared more about how their socially "closer" groups perceive their personality traits. This observation implies that we may need to provide different controls to support the privacy policy settings for different groups, e.g., finer-grained controls over groups that have "strong-ties" with the user [10].

Approaches to Personalizing Initial Privacy Settings

To help users jump start their privacy configurations, our current system experimented several approaches to suggest the initial settings to users. While our study shows that providing an initial configuration is helpful, it also reveals that some of the approaches worked better than others. In our case, our simple rule-based approach that suggested initial settings based on a few parameters at a high level worked better than our prediction-based approach that made suggestions based on a prediction model involving a number of fine-grained parameters including the user's personality. These initial settings also directly impacted users' interaction behavior and task performance in our study. This observation seems consistent with the findings in other's work (e.g, [26]), which suggests a template-based approach of sharing settings but does not elaborate whether the granularity of the template would make a difference.

Although a simpler approach demonstrated to be more effective in our study, it does not mean a simpler approach would always work better in the future. A more sophisticated approach can still win if the factors used and their effects can be better modeled. For example, our current prediction-based approach was developed using a small training data set, and the model prediction may be over-fitted and did not predict the preferences accurately enough for new users. While this is a hard problem beyond the scope of this paper, this type of approaches can be greatly improved with more training data and carefully chosen mathematical models. Moreover, we envision a mixed-initiative approach [14], which combines the power of both machines and humans and supports a continuous learning loop involving both sides. The system will first make initial suggestions that users will be willing to adjust, and the users will teach the system to update its prediction model through their behavior and feedback.

Limitations and Future Work

Through our study, we have also observed several limitations in our current work. First, previous studies indicate that privacy control is a long and interactive process within a context [25]. Our current work focused only on understanding participants' interaction behavior during a short time period and have not studied how a temporal context would impact users' behavior in a system like ours. Second, people's privacy concerns are influenced by their trust with the system [13], people might have configured their privacy policies differently if they know more about the quality of a system like ours. However, our current system does not provide users much information to help them assess the quality of our personality analytics, e.g., the evidence showing how the traits are derived and how accurate the derived portraits are. Without such information, our understanding of users' privacy preferences over their personality data is limited. Thus, making our system more transparent by providing users with more information on how the personality traits are derived and the quality of the analytics is one of our future tasks. Our study also revealed several user-desired features that we currently do not support. For example, people want to use the consequences resulted from their privacy policies to guide their behaviors on social media.

CONCLUSION

In this paper, we reported the design, development and evaluation of an interactive visualization tool, VeilMe, to help users configure their privacy preferences of personality portraits derived from social media. VeilMe considers several factors of social groups, personality traits, disclosure level and initial settings in the workplace context. It also employs novel and intuitive visual metaphors to help the exploration of personality portraits, and the comprehension and configuration of sharing preferences. The evaluation results showed that VeilMe can effectively support the sharing configuration, and suggest several design implications including using visual metaphors to aid sharing configuration tasks, using social groups as an efficient configuration proxy, and design tradeoff of approaches for personalized sharing settings.

REFERENCES

1. Adali, S., and Golbeck, J. Predicting personality with social behavior. In *Proc. of ASONAM 2012*, IEEE Computer Society (2012), 302–309.
2. Bellotti, V., and Sellen, A. Design for privacy in ubiquitous computing environments. In *Proc. of ECSCW '93*, Kluwer Academic Publishers (1993), 77–92.
3. Chen, J., Hsieh, G., Mahmud, J. U., and Nichols, J. Understanding individuals' personal values from social media word use. In *Pro. of CSCW'14* (2014), 405–414.
4. Cohen, A. A value based perspective on commitment in the workplace. *International Journal of Intercultural Relations 33*, 4 (2009), 332–345.
5. Cormac, E. R. M. *A Cognitive Theory of Metaphor*. MIT Press, 1990.
6. De Choudhury, M., Counts, S., and Horvitz, E. Predicting postpartum changes in emotion and behavior via social media. In *Proc. of SIGCHI '13* (2013), 3267–3276.
7. Egelman, S., Oates, A., and Krishnamurthi, S. Oops, i did it again: Mitigating repeated access control errors on facebook. In *Proc. of SIGCHI '11*, ACM (2011), 2295–2304.
8. Fang, L., and LeFevre, K. Privacy wizards for social networking sites. In *Proc. of WWW '10*, ACM (2010), 351–360. 00179.
9. Funder, D. C. *The personality puzzle.* WW Norton & Co, 1997.
10. Gilbert, E., and Karahalios, K. Predicting tie strength with social media. In *Proc. of SIGCHI '09*, ACM (2009), 211–220.
11. Golbeck, J., Robles, C., Edmondson, M., and Turner, K. Predicting ersonality from twitter. In *Privacy, security, risk and trust in SocialCom '11* (2011), 149–156.
12. Golbeck, J., Robles, C., and Turner, K. Predicting personality with social media. In *Proc. CHI'11 EA*, ACM (2011), 253–262.

13. Gou, L., Zhou, M. X., and Yang, H. KnowMe and ShareMe: Understanding automatically discovered personality traits from social media and user sharing preferences. In *Proc. of SIGCHI '14*, ACM (2014), 955–964.

14. Horvitz, E. Principles of mixed-initiative user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '99, ACM (New York, NY, USA, 1999), 159–166. 00675.

15. Iachello, G., and Hong, J. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction 1*, 1 (2007), 1–137.

16. Inc., F. Facebook audience preview, 2014.

17. Junglas, I. A., Johnson, N. A., and Spitzmller, C. Personality traits and concern for privacy: an empirical study in the context of location-based services. *Eur. J. of Info. Sys. 17*, 4 (2008), 387–402.

18. Knijnenburg, B. P., Kobsa, A., and Jin, H. Preference-based location sharing: are more privacy options really better? In *Proc. of SIGCHI '13*, ACM (2013), 2667–2676.

19. Korzaan, M., Brooks, N., and Greer, T. Demystifying personality and privacy: An empirical investigation into antecedents of concerns for information privacy. *Journal of Behavioral Studies in Business 1* (2009), 1–17.

20. Lipford, H. R., Watson, J., Whitney, M., Froiland, K., and Reeder, R. W. Visual vs. compact: A comparison of privacy policy interfaces. In *Proc. of SIGCHI '10*, ACM (2010), 1111–1114.

21. Liu, K., and Terzi, E. A framework for computing the privacy scores of users in online social networks. *ACM Trans. Knowl. Discov. Data 5*, 1 (Dec. 2010).

22. Mairesse, F., Walker, M. A., Mehl, M. R., and Moore, R. K. Using linguistic cues for the automatic recognition of personality in conversation and text. *J. Artif. Intell. Res.(JAIR) 30* (2007), 457–500.

23. Mazzia, A., LeFevre, K., and Adar, E. The PViz comprehension tool for social network privacy settings. In *Proc. of SOUPS '12*, ACM (2012), 13:1–13:12.

24. Olson, J. S., Grudin, J., and Horvitz, E. A study of preferences for sharing and privacy. In *Proc. of CHI '05 EA*, ACM (2005), 1985–1988.

25. Palen, L., and Dourish, P. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, ACM (New York, NY, USA, 2003), 129–136.

26. Patil, S., and Lai, J. Who gets to know what when: Configuring privacy permissions in an awareness application. In *Proc. of SIGCHI '05*, ACM (2005), 101–110.

27. Patil, S., Schlegel, R., Kapadia, A., and Lee, A. J. Reflection or action?: How feedback and control affect location sharing decisions. In *Proc. of SIGCHI '14*, ACM (2014), 101–110.

28. Pennacchiotti, M., and Popescu, A.-M. A machine learning approach to twitter user classification. In *ICWSM* (2011).

29. Reeder, R. W., Bauer, L., Cranor, L. F., Reiter, M. K., Bacon, K., How, K., and Strong, H. Expandable grids for visualizing and authoring computer security policies. In *Proc. of SIGCHI '08*, ACM (2008), 1473–1482.

30. Roberts, B. W., Kuncel, N. R., Shiner, R., Caspi, A., and Goldberg, L. R. The power of personality: The comparative validity of personality traits, socioeconomic status, and cognitive ability for predicting important life outcomes. *Persp. on Psy. Sci. 2*, 4 (2007), 313–345.

31. Rode, J., Johansson, C., DiGioia, P., Filho, R. S., Nies, K., Nguyen, D. H., Ren, J., Dourish, P., and Redmiles, D. Seeing further: Extending visualization as a basis for usable security. In *Proc. of SOUPS '06*, ACM (2006), 145–155.

32. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiq. Comput. 13*, 6 (2009), 401–412.

33. Schlegel, R., Kapadia, A., and Lee, A. J. Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In *Proc. of SOUPS '11*, ACM (2011), 14:1–14:14.

34. Shen, J., Brdiczka, O., and Liu, J. Understanding email writers: Personality prediction from email messages. In *User Modeling, Adaptation, and Personalization*. Springer, 2013, 318–330.

35. Smith, H. J., Dinev, T., and Xu, H. Information privacy research: An interdisciplinary review. *MIS quarterly 35*, 4 (2011), 989–1016.

36. Sweeny, L. k-anonymity: A model for protecting privacy. *Int. J. Unc. Fuzz. Knowl. Based Syst. 10*, 05 (2002), 557–570.

37. Tausczik, Y. R., and Pennebaker, J. W. The psychological meaning of words: LIWC and computerized text analysis methods. *J. of Lang.and Soc. Psy. 29*, 1 (2010), 24–54.

38. Westin, A. F., Maurici, D., Business, P. . A., LLP, P. W., and Associates, L. H. a. *E-commerce & Privacy: What Net Users Want*. Privacy & American Business, 1998.

39. Yang, J., and Li, Y. Identifying user needs from social media. Tech. rep., IBM Tech. Report, 2013.

40. Yarkoni, T. Personality in 100,000 words: A large-scale analysis of personality and word use among bloggers. *J. of Res. in Personality 44*, 3 (2010), 363–373.