

Online Social Networks: Enhancing user trust through effective controls and identity management



Ryan Galpin

University of Fort Hare



University of Fort Hare
Together in Excellence

Prof Stephen Flowerday

University of Fort Hare



Recipient of the
**Supreme Order
of Baobab**
(Gold)

Overview

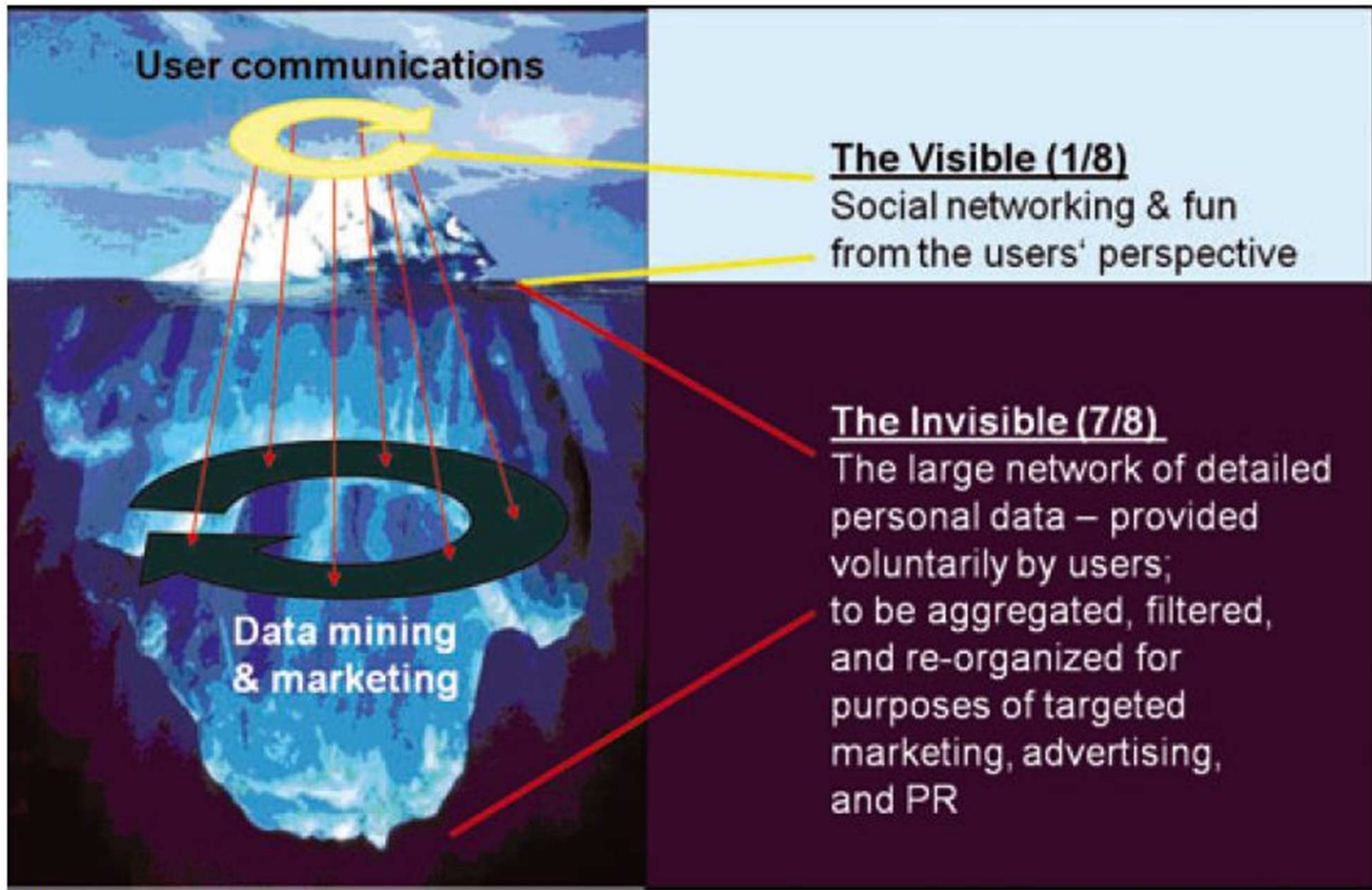
- Introduction
- Current Vulnerabilities and Risks
- Challenge of Increasing User Trust
- Identity Management within Online Social Networks
- Evaluating Current Controls
- Social Networking Control Set
- Conclusion



Introduction

- Online social networking currently one of the most popular Internet activities
 - More than two-thirds of global on-line population visit and participate
 - Monthly avg of 32% of worldwide Internet users visiting Facebook (Alexa.com)
- Establishment of trust and the protection of users becomes an ongoing challenge
 - threat of misuse and privacy intrusions by malicious users
- Online environment characterized by anonymous interactions
 - Virtual Persons
 - connection between multiple users in the environment and the true identity of the individual they represent
- Social networks are a targeted platform
 - sexual offenders , cyber bullying, identity theft and harassment
- Misrepresentation
 - Inexperienced and adolescent users





Challenge of Increasing User Trust

- Trust in an online environment
 - Basic pre-conditions to electronic based interactions
- Information available to users
 - Determined by the level of trust and trustworthiness within these services
 - User evaluation and decision on accepted reflections of reality
- Unique social screening ability
- Trust in People
 - Varying levels of uncertainty during interactions between individuals
 - Uncertainty Reduction Theory
 - Reducing uncertainty – increasing predictability
- Trust in systems
 - Assess levels of user trust and adequacy of controls
 - Effect on user confidence
- Goal of reducing uncertainty and increasing trust
 - Effective system of controls needed
 - limit uncertainty, increasing confidence and trust
 - Preventative, Detective and Corrective



Identity Management (IDM) within Online Social Networks

- IDM defined
 - identification, authentication and authorization of information, as well as the use of this information to authenticate and properly authorize principals in a computer network or distributed system
- “One to many” service provider relationship
- Challenge of implementation of IDM within the confines of service provider environment
 - Users are able to create multiple user profiles or accounts that can be accessed within one online service
 - Systems and processes need to be implemented that can manage these users and achieve a satisfactory level of user-to-profile linking.



Identity Management (IDM) within Online Social Networks

- Commonly exhibited models within organizations and service providers worldwide
 - Isolated User Identity Model (ISUIM)
 - Most commonly used : Single user – single set of login credentials
 - Federated User Identity Model (FUIM)
 - Federated domain of service providers (SP's)
 - Allow identities from different SP domains recognition across all domains
 - Common User Identity Model (CUIM)
 - single authority/entity acts as exclusive user credentials provider for all SP's
 - Single Sign-On Identity Model (SSOIM)
 - Users authenticated by one service provider, resulting in authentication across several other SP's



Identity Management (IDM) within Online Social Networks

- Current evidence of Identity Management by service providers
- Facebook Connect - 2008
 - Trusted Authentication
 - Real Identity
 - Single Sign-On model
- MySpace Data Availability - 2008
 - Personalized Internet browsing
- Shortfalls still exist
 - Accurately authenticate users
 - Manage multiple profiles



Evaluating Current Controls

- Penetration testing methodology
 - Key system areas and controls/processes evident
 - Identify problem areas
- Experiment designed and conducted
 - Test areas linked to problem area
 - Assessed for possible vulnerabilities
- Profile creation and interaction
 - Fictitious user profiles created by researcher in both Facebook and MySpace environments
 - Conduct daily activities
 - Specific character role
 - Detailed test log to document findings



Evaluating Current Controls

Assessment Area	Assessment Items
Age Controls	<ul style="list-style-type: none"> • Age Verification during profile creation • Ability to search users by age • Ability to send underage users friend requests • Ability for underage users to interact with adults • Search groups where teen activity would be high
Privacy Controls	<ul style="list-style-type: none"> • Default setting when creating a profile • Ease of use – changing of privacy settings • Public versus Private profile settings
Profile Controls	<ul style="list-style-type: none"> • Management of friends • Blocking/Reporting of unwanted users
Identity Management – Service Provider	<ul style="list-style-type: none"> • Multiple profiles created by single user • Multiple profiles share same password • Identity Management • All created profiles linked to a blocked user
Administrator Effectiveness	<ul style="list-style-type: none"> • Treatment of reported/blocked users • Feedback from reporting/blocking requests



Evaluating Current Controls

- Age Controls
 - Effective in isolation
 - Inconsistent application of rules
- Privacy Controls
 - Adequate and effective
- Profile Controls
 - Effective for management of friends
 - Reporting/Blocking of users ineffective – no evidence of identity management
- Identity Management – Service Provider
 - No evidence of identity management processes
 - Inability to manage multiple profiles by single individuals
- Administrator Effectiveness
 - Effective when performing blocking
 - Ineffective in management of blocked users



Social Networking Control Set

Control Group	Control Name	Control Description	Control Type
Age Controls	• Email registration	<ul style="list-style-type: none"> • Service providers must log all email addresses that fail the initial age verification control at profile creation. • To ensure effectiveness, email address and username and surname must be logged to prevent the same user with a new email address variation from registering. 	Preventative
	• Underage Communication	<ul style="list-style-type: none"> • If contact is attempted between an adult user and an underage user, the adult must input the younger user's email address as confirmation. 	Preventative
	• Underage User Privacy	<ul style="list-style-type: none"> • All underage users must be protected by the service providers' administrators by default, and cannot make changes to privacy settings. 	Preventative
	• Group Age	<ul style="list-style-type: none"> • Service providers and group creators must apply recommended age restrictions to these various groups. • No adults should be able to search or find groups relating to teen interests and likes. 	Preventative Detective
	• User Search Age	<ul style="list-style-type: none"> • Service providers must either remove ability to search for users by age completely or make the youngest search age 18 year olds. 	Preventative
Privacy Controls	• Profile Privacy Settings	<ul style="list-style-type: none"> • Service providers must exhibit strong controls that protect the users' privacy and ensure users are protected by default. 	Preventative
Profile Controls	• Friend Request	<ul style="list-style-type: none"> • Service providers must ensure that the controls in place to manage user profiles are effective and easy to use. • Adult users should not be able to send friend requests to underage users without email address as confirmation. 	Preventative
	• Messaging	<ul style="list-style-type: none"> • Messaging controls must be in place to ensure that only friends can send and receive messages between each other. 	Preventative
	• User reporting and Blocking	<ul style="list-style-type: none"> • When a user requests to report another user, this must be enforced immediately. • Blocked users must not find complainant's profile through a user search. • It is proposed that the blocked user's name and profile details be flagged so that they cannot simply create a new profile with similar details. 	Corrective
Identity Management Controls	• User Verification	<ul style="list-style-type: none"> • Effective user verification process to be part of registration process. Must include submission of government issued identification document or similar. • Documents to be submitted for profile activation; else a status must appear on profile as "unconfirmed". This acts as a warning that the identity of the profile is unconfirmed. 	Preventative
	• Profile Linking	<ul style="list-style-type: none"> • Service providers are encouraged to create automated processes that filter created profiles for various triggers. • These filters act as triggers for investigation. Investigations could request identity verification or similar means to confirm the individual and remove profile alerts. 	Detective Corrective



Social Networking Control Set

Profile Controls	<ul style="list-style-type: none"> • Friend Request 	<ul style="list-style-type: none"> • Service providers must ensure that the controls in place to manage user profiles are effective and easy to use. • Adult users should not be able to send friend requests to underage users without email address as confirmation. 	Preventative
	<ul style="list-style-type: none"> • Messaging 	<ul style="list-style-type: none"> • Messaging controls must be in place to ensure that only friends can send and receive messages between each other. 	Preventative
	<ul style="list-style-type: none"> • User reporting and Blocking 	<ul style="list-style-type: none"> • When a user requests to report another user, this must be enforced immediately. • Blocked users must not find complainant's profile through a user search. • It is proposed that the blocked user's name and profile details be flagged so that they cannot simply create a new profile with similar details. 	Corrective
Identity Management Controls	<ul style="list-style-type: none"> • User Verification 	<ul style="list-style-type: none"> • Effective user verification process to be part of registration process. Must include submission of government issued identification document or similar. • Documents to be submitted for profile activation; else a status must appear on profile as "unconfirmed". This acts as a warning that the identity of the profile is unconfirmed. 	Preventative
	<ul style="list-style-type: none"> • Profile Linking 	<ul style="list-style-type: none"> • Service providers are encouraged to create automated processes that filter created profiles for various triggers. • These filters act as triggers for investigation. Investigations could request identity verification or similar means to confirm the individual and remove profile alerts. 	Detective Corrective



Conclusion

- Several areas where controls and effective IDM processes are needed
- Open to exploitation, in turn reducing effect on levels of trust exhibited by users in the system and in other users
- Proposed set of controls aimed to provide an effective means to enhance user trust through their implementation and management
- User trust and confidence for both the system and other users are market requirements, and implementation of an effective set of controls can assist in achieving them



Questions



University of Fort Hare
Together in Excellence

