
User-Tailored Privacy by Design

Darcia Wilkinson, Saadhika Sivakumar , **David Cherry**,
Bart P. Knijnenburg, Elaine M. Raybourn , Pamela
Wisniewski , Henry Sloan



Introduction

Privacy:

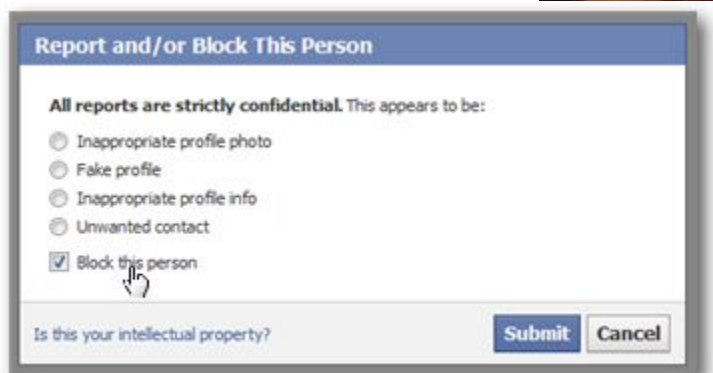
- *Prevent* information access
- Information distributed by individual
- System to *protect* user



Privacy: Beyond Information Access

Supporting user's preferred privacy management strategies:

Blocking



Report and/or Block This Person

All reports are strictly confidential. This appears to be:

- Inappropriate profile photo
- Fake profile
- Inappropriate profile info
- Unwanted contact
- Block this person

Is this your intellectual property?

Submit Cancel



Untagging

Withholding



Share this Photo

Share: On your own timeline (selected) Close Friends

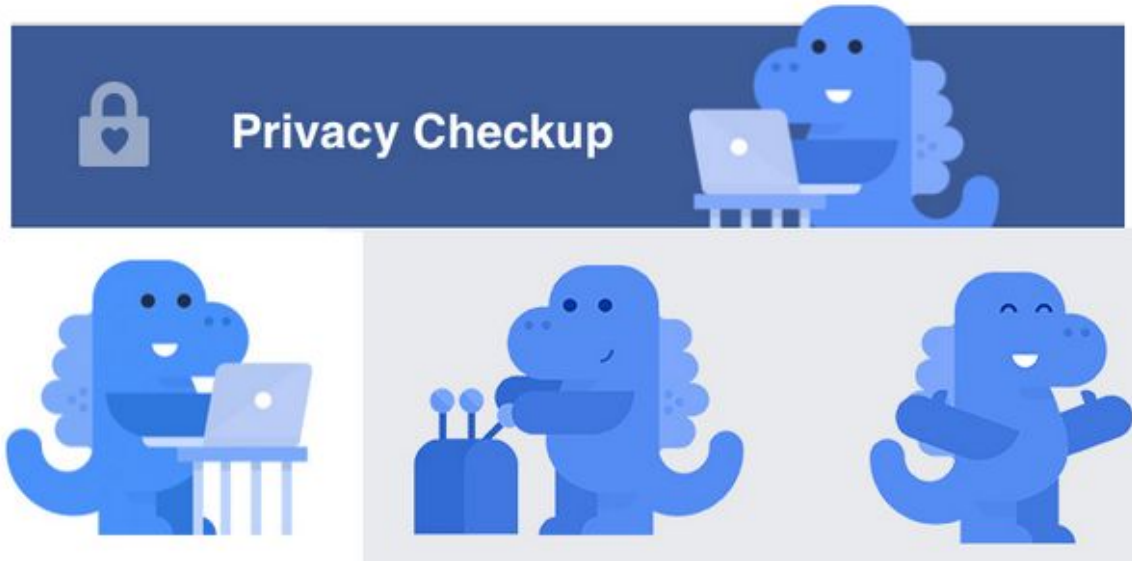
- ✓ On your own timeline
- On a friend's timeline
- In a group
- On your Page
- In a private Message

Write

Share Photo Cancel

Privacy By Design

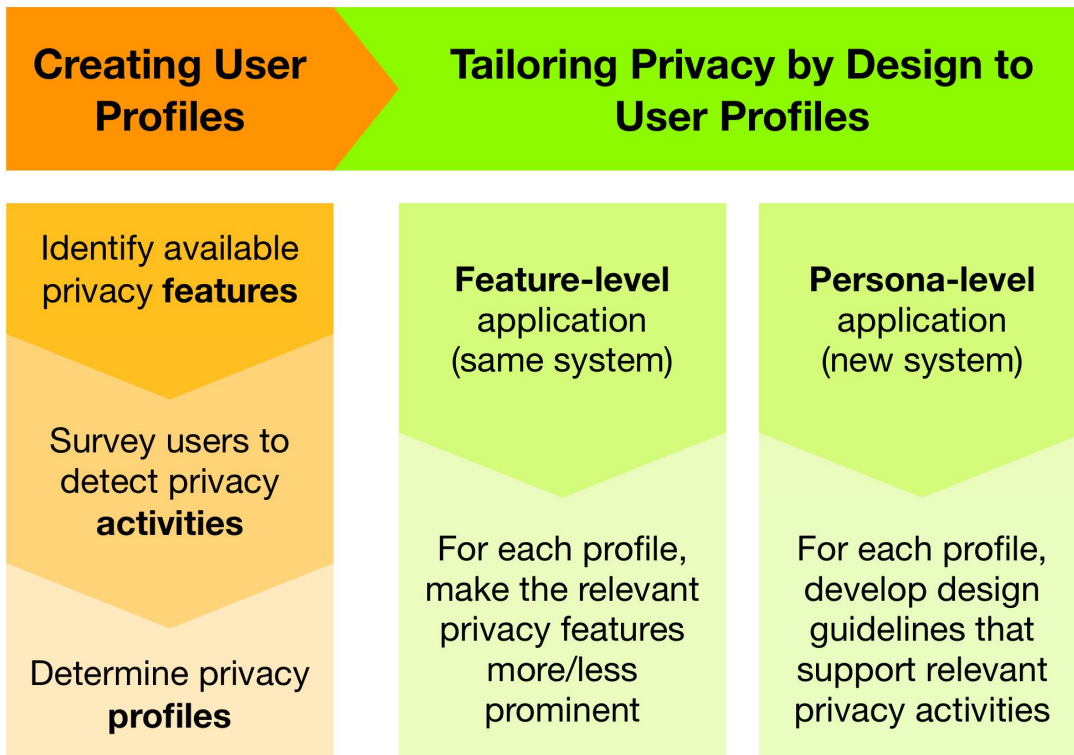
- Privacy addressed early in system development
- Tries to avoid privacy problems
- Criticism is...it doesn't address variations of all users



User Tailored Privacy

- System supports users' management strategies
- Tailors user interface for privacy features
- Including:
 - Withholding information
 - Restricting chat
 - Selectively sharing

User-Tailored Privacy by Design Framework



Profiling Facebook Users' Privacy Behavior

Supporting user's preferred privacy management strategies:

Profiling Facebook Users' Privacy Behaviors

Pamela Wisniewski
College of Information Sciences and
Technology
The Pennsylvania State University
pam@pamspam.com

Bart P. Knijnenburg
Department of Informatics
University of California, Irvine
bart.k@uci.edu

Heather Richter Lipford
Department of Software and
Information Systems
UNC Charlotte
heather.lipford@unc.edu

ABSTRACT

Social Network Sites (SNSs) such as Facebook offer a plethora of privacy controls, but users rarely exploit all of these controls, nor do they do so in a similar manner. In this paper, we analyze distinct *profiles* of users' privacy management strategies on Facebook (including but also going beyond information disclosure behavior). We cluster the self-reported privacy behaviors of 308 Facebook users based on the privacy settings and features available in Facebook's user interface. We extrapolate six distinct privacy profiles, which include: 1) *Privacy Maximizers*, 2) *Selective Sharers*, 3) *Privacy Balancers*, 4) *Self-Censors*, 5) *Time Savers/Consumers*, and 6) *Privacy Minimalists*. Creating such profiles will enable deeper exploration of privacy concerns and behaviors, as well as expose opportunities for personalization of privacy settings, recommendations, and training.

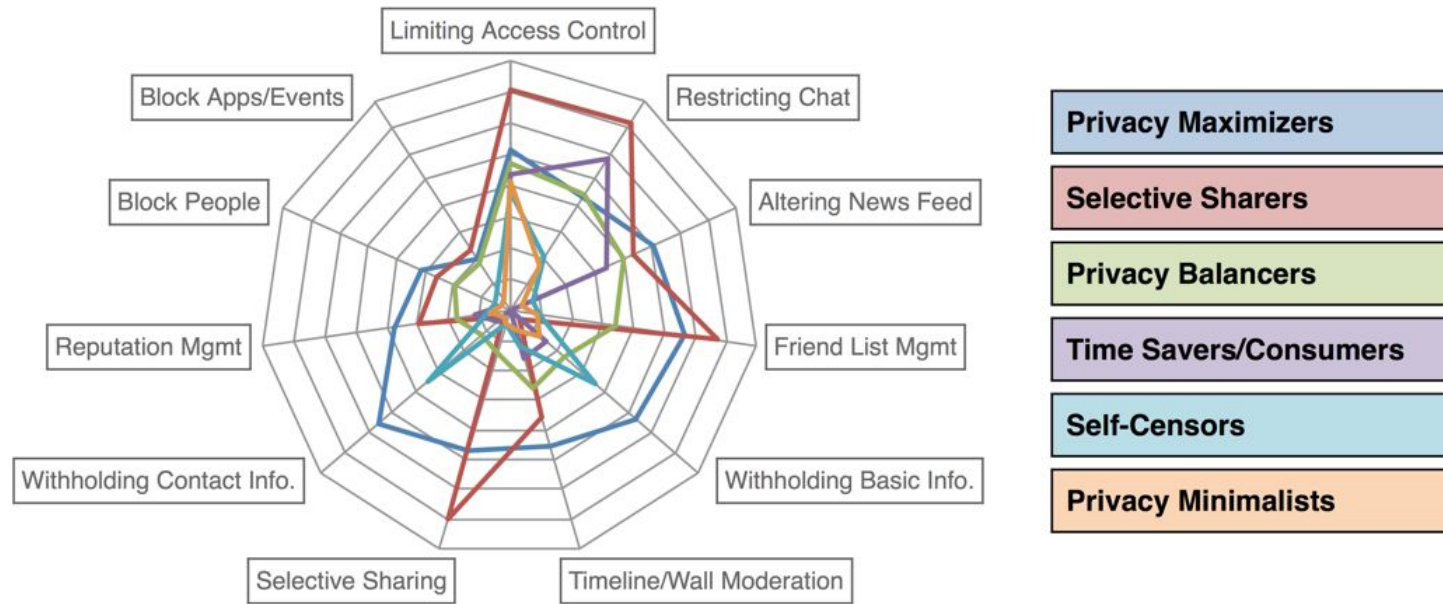
1. INTRODUCTION

Privacy is a major concern of Social Network Site (SNS) users [13], even though most SNSs provide users with a variety of mechanisms to control how they interact and share information with one another. Users' efficacy in privacy management is hampered by their bounded rationality [1] and their limited motivation to control their privacy [4, 6]. Thus, understanding and exploiting *all* the mechanisms necessary to manage every aspect of a user's privacy on an SNS such as Facebook is a

different interface features available for regulating interpersonal privacy [23]. By doing this, we were able to build a theoretical framework to better understand the various types of interpersonal privacy boundaries that SNS users manage [21, 23]. In many cases, we found that the ability to manage various types of interpersonal boundaries was directly dependent on the interface features available within the SNS for doing so. Therefore, for the purposes of this paper, we define *privacy behaviors* as the privacy features and/or settings that Facebook users leverage in order to manage interpersonal privacy boundaries. On Facebook, managing one's personal user profile information, the content displayed or posted onto one's Timeline or Wall, the content that filters into one's News Feed from one's friends, or even whom one chooses to friend or unfriend are all examples of interpersonal boundary decisions that SNS users can combine to form a strategy for regulating their interpersonal privacy boundaries.

A variety of research has examined individuals' use of various privacy controls, and their relationships with privacy concerns, demographics, or other behaviors and outcomes. For example, Stutzman et al. [17] examined the factors which contributed to Facebook users' decisions on whether or not to set their Facebook profiles to "Friends Only." Ellison et al. [5] found a positive relationship between Facebook users' use of advanced privacy settings (such as changing privacy settings from the default and

Privacy Behaviors on Facebook



The six privacy management strategies uncovered by Wisniewski et al.

Six Facebook Privacy Profiles

Selective Sharers

Self-Censors

Time Savers



Privacy Maximizers

Privacy Balancers

Privacy Minimalists

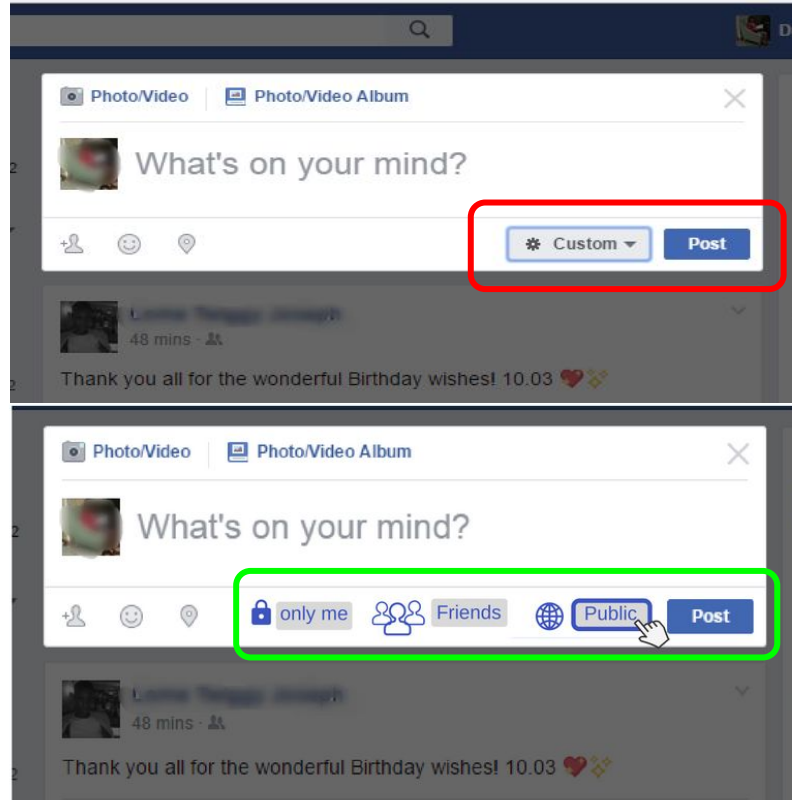
Six Facebook Privacy Profiles

Selective Sharers

require a more restrictive default sharing setting

More prominent design of capabilities for:

- **selective sharing**
- friend list management
- blocking apps
- blocking people in their notification window



Six Facebook Privacy Profiles

Selective Sharers

require a more restrictive default sharing setting

More prominent design of capabilities for:

- selective sharing
- **friend list management**
- blocking apps
- blocking people in their notification window



Six Facebook Privacy Profiles

Self-Censors

benefit from their info being set to “only me” by default

Users in this profile may:

- “Only me” default setting for basic and contact information
- Reduce interface clutter

The screenshot shows the 'About' section of a Facebook profile. The right-hand column contains various information fields, each with a lock icon to its right, indicating that the information is set to 'Only Me'. A green rectangular box highlights these lock icons. The fields include:

CONTACT INFORMATION	
Address	100 Brown Street New York, NY, United States 10026
Email	2 emails hidden from Timeline
+ Add a mobile phone	
+ Add a public key	

WEBSITES AND SOCIAL LINKS	
Websites	http://www.cnn.com/
Social Links	www.instagram.com/janedoe (Instagram)

BASIC INFORMATION	
Birth Date	September 2
Birth Year	1988
Gender	Female
Religious Views	50%sanaton 30%boddha, 20%christian
Political Views	Non-party

This screenshot shows a Facebook video post. A red rectangular box highlights the privacy settings for the video, which are set to 'Friends', 'Following', and 'Message'.

This screenshot shows the same Facebook video post as above. A green rectangular box highlights the 'Message' privacy setting, which is currently selected.

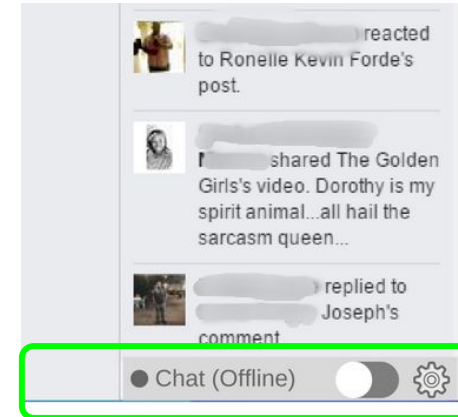
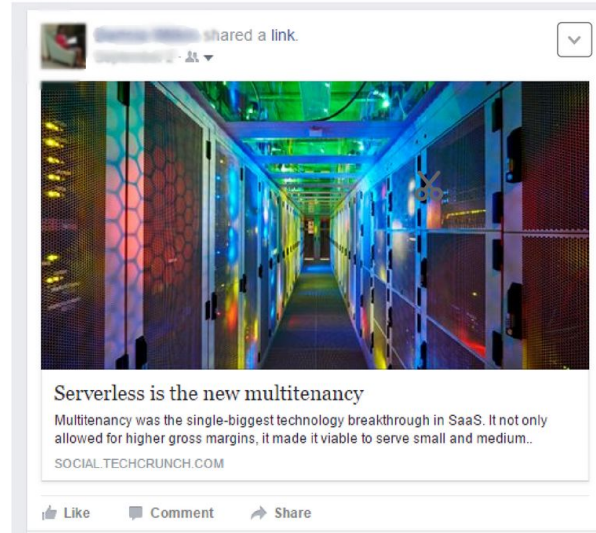
Six Facebook Privacy Profiles

Time Savers

require more prominent News Feed moderation features

Users in this profile may:

- Prefer to read information without messages or updates
- Alter news feeds through deleting content
- Edit their own posts and stories
- Create custom friends lists



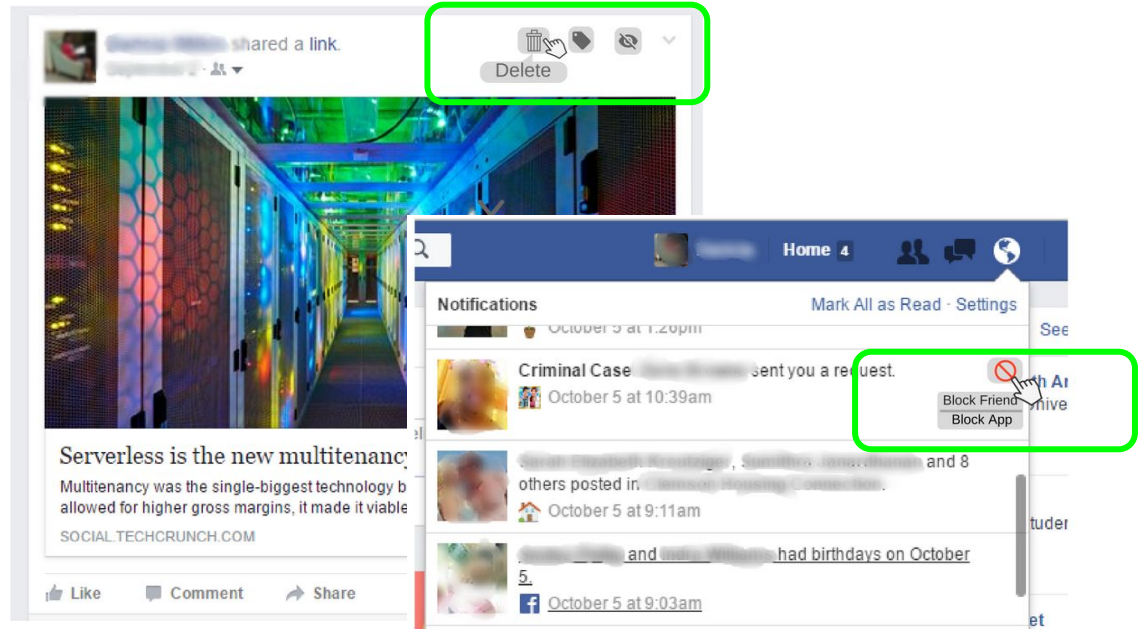
Six Facebook Privacy Profiles

Privacy Maximizers

require all of the functionalities previously described

Users in this profile may:

- Utilize all available privacy features
- Moderate posts
- Blocks apps, events, people
- Restrict chat accessibility



Six Facebook Privacy Profiles

Privacy Balancers

require more prominent controls to alter their News Feed and timeline

Users in this profile may:

- Show moderate levels of privacy management
- Prefer certain features over others



Six Facebook Privacy Profiles

Privacy Minimalists

Users in this profile may:

- Show lowest levels of privacy concerns
- Use interfaces as they are
- Little to no changes in privacy settings

Overview of the UTPbD solution for TLA

Self-Censors	Require functionality to share their information and training outcomes w/ applications and people
Selective Shares	Require mechanisms for the selection of learning material, and highly restricted forms of sharing learning outcomes
Time Savers	Should be able to opt out of active notifications and social features
Privacy Maximizers	Require all of the functionality described above
Privacy Balancers	Require mechanisms for curation, blocking, and avoiding direct interaction
Privacy Minimalists	Require systems that allow them to maximally benefit from their adaptive and social functionalities

Future Work

Current approach:

- Observe privacy management behaviors and make features easily accessible

Alternative methods:

- Highlight features that **fit within profile** but they are **not being used**
- Highlight features that **do not fit within profile** and are **not being used**
- Automate features