Privacy-by-ReDesign: Alleviating Privacy Concerns for Third-Party Applications

PI: Heng Xu | CNS-0953749 | College of Information Sciences and Technology | Pennsylvania State University

http://pal.ist.psu.edu/

In online social networks, the aggressive way of data access and transmission by third-party applications (apps) has made privacy concerns particularly salient. A heightened need for empowering user control for third-party apps arises due to the inability to monitor the data use by app providers within and outside of the social networking platform and the inherent uncertainty about their privacy practices. The approach of *Privacy by ReDesign* is employed to investigate whether users can more adequately represent their preferences for sharing and releasing personal information with two newly proposed designs.

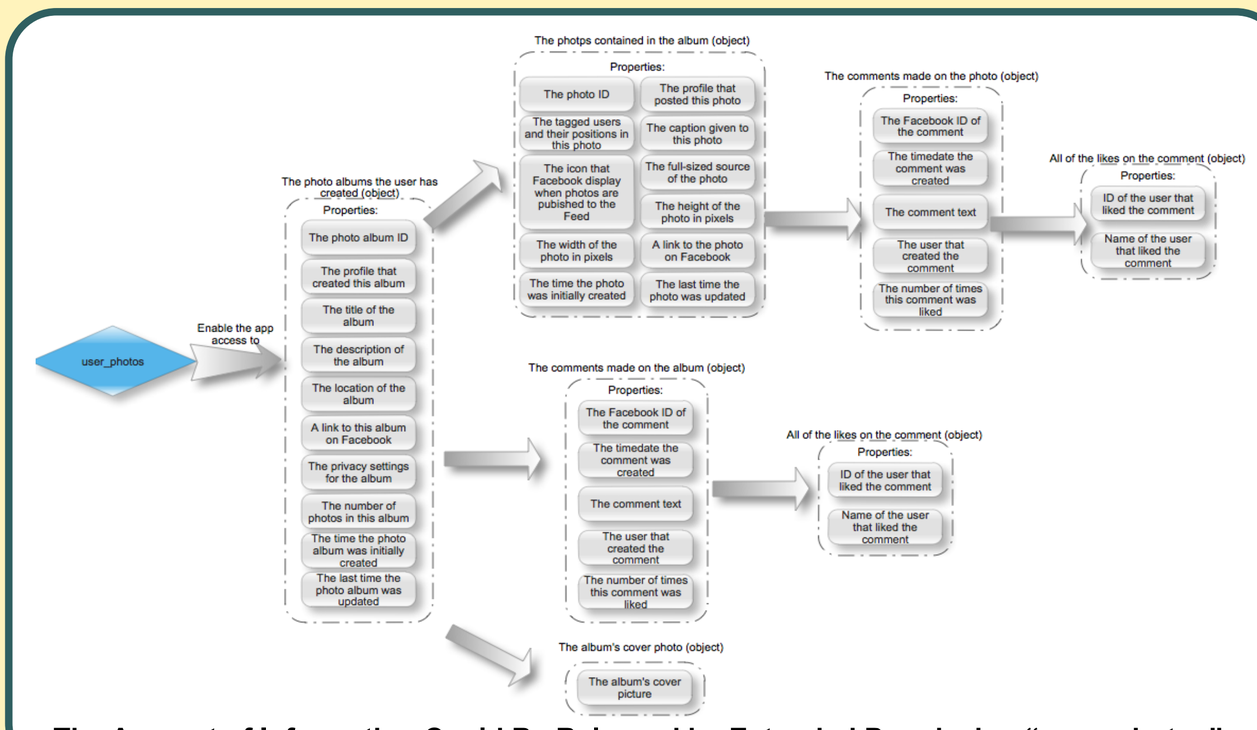
Apps' Problematic Data Practices

- Collect data from the most popular 1800 Facebook apps in Dec 2010
- There is no way for users to limit apps' data access or publishing

Users' Information Releasing Description.

Data Category	No. of apps request for the data	Total times of user information are requested by apps
Access my basic information	1305	857,821,274
Send me email	454	238,991,048
Post to my wall	670	137,473,280
Access my profile information*	148	178,912,316
Access my data any time	76	17,450,664
Manage my pages	8	237,067
Access my photos and videos	128	43,227,008
Access my friends information	148	68,436,680
Access posts in my News Feed	66	30,635,352
Online Presence	16	4,003,824
Access my family & relationship	28	6,617,296
Access Facebook Chat	8	1,739,160
Send me SMS messages	10	1,195,720

* User information accessed by this category may vary based on different app requests.



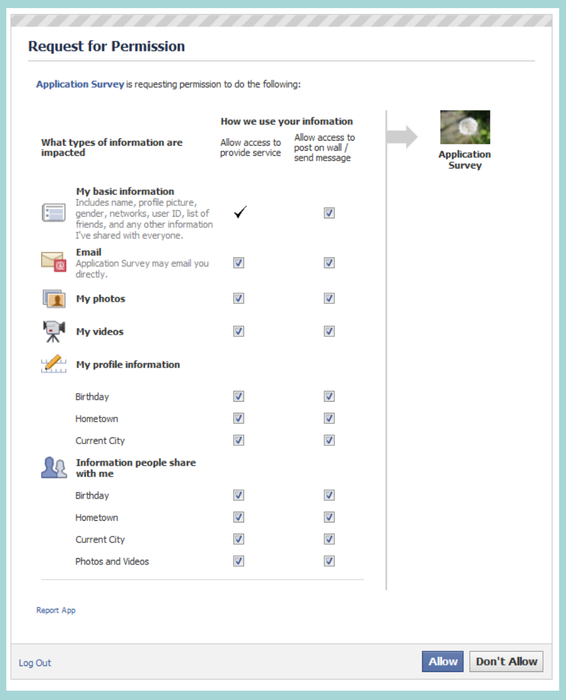
The Amount of Information Could Be Released by Extended Permission "user_photos"

Proposed New Designs

Design Principles:

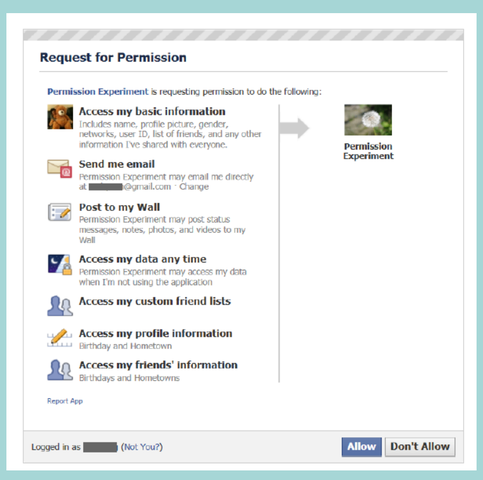
• [*Control*] The privacy authentication dialogue should provide options for a user to control an app's information access and use before adding the app to the user's Facebook profile.

• [*Awareness*] The privacy authentication dialogue should provide alert signals for a user when an app asks for the user's sensitive private information such as date of birth and address.

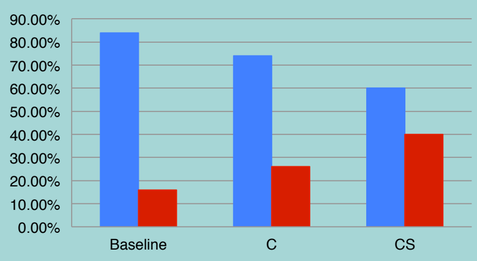


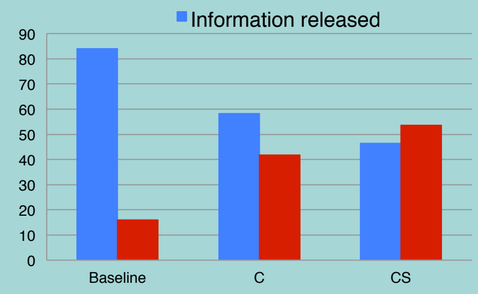
Proposed Design for Empowering Control (C)

Proposed Design for Promoting Awareness (CS)



Original Design on Facebook (Baseline)

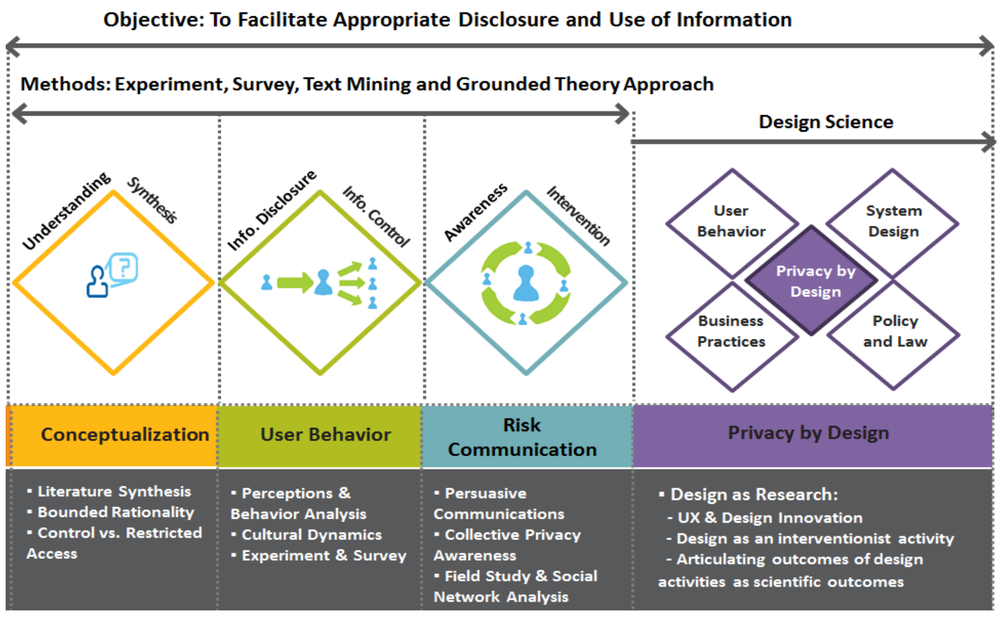




50 Facebook users were recruited per treatment from MTurk

I (Baseline)	Current Facebook privacy notice
II (C)	Check-box design (for Empowering Control)
III (CS)	Check-box and Signal design (for Promoting Awareness)

Research Framework



Contributors:

Na Wang, Jens Grossklags, Pan Shi, Saijing Zheng, Tamara Dinev, and H. Jeff Smith

Selected Publication:

Wang, N., Grossklags, J. and Xu, H. (2013). "An Online Experiment of Social Applications' Privacy Authorization Dialogues," Proceedings of CSCW, San Antonio, TX.

Xu, H., Wang, N., and Grossklags, J. (2012). "Privacy-by-ReDesign: Alleviating Privacy Concerns for Third-Party Applications," Proceedings of ICIS, Orlando, FL.

Shi, P., Xu, H., Erickson, B. L., and Zhang, C. (2012). "See Friendship: Interpersonal Privacy Management in a Collective World," Proceedings of AMCIS, Seattle, WA.

Zheng, S., Shi, P., Xu, H., and Zhang, C. (2012). "Launching the New Profile on Facebook: Understanding the Triggers and Outcomes of Users' Privacy Concerns," Proceedings of TRUST, LNCS 7344, pp. 325–339.

Xu, H. (2012). "Reframing Privacy 2.0 in Online Social Networks," University of Pennsylvania Journal of Constitutional Law, Vol. 14, No. 14, pp. 1077-1102.

Smith, H. J., Dinev, T., and Xu, H. (2011). "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly, Vol. 35, No. 4, pp. 989-1015.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

PAL@Penn State
Penn State Privacy Assurance Lab (PAL)