

Towards Privacy Standards Based on Empirical Data

Serge Egelman

Erika McCallister

Previous Privacy Standards

- P3P had highly granular privacy options
- Major web browsers supported it
- >25% of the most popular websites supported P3P
- Great success?



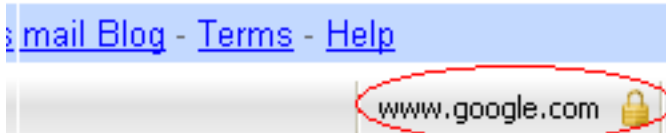
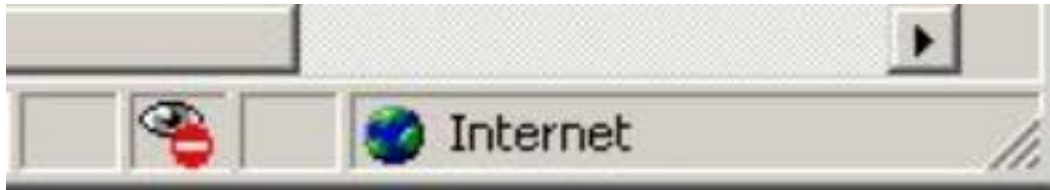
P3P is too granular!



How about SSL?

- Most users don't understand when a website is encrypted
- Most users don't understand what most SSL errors mean
- There are only two failure modes:
 - Site is not properly encrypted
 - Site is not trusted

\$#! My Browser Says



Firefox



Opera

UI Is Critical

- Interface needs to be consistent
- So how do we do this?
 - Will users make more informed decisions when impact is clearer?
 - Is informed consent currently being obtained when sites request data?
- We need data!

Quid Pro Quo

CNN Social is requesting permission to do the following:



Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.



CNNMoney.com

CNN Social



[Report App](#)

Logged in as Serge Egelman ([Not You?](#))

Allow


Don't Allow

Nom, nom,
nom!



Informed Consent?

CNN Social is requesting permission to do the following:

 **Access my basic information**

- Name: Serge Egelman
- Profile Picture
- Gender: Male
- Networks:
 - National Institute of Standards & Technology
 - Carnegie Mellon
 - UVA
 - Microsoft
- User ID: serge.egelman (767455623)
- List of Friends: [Link](#)
- Any other information I've shared with everyone

[Report App](#)

Logged in as Serge Egelman (Not You?)

[Allow](#) [Don't Allow](#)

