

Usable Privacy

Lorrie Faith Cranor

July 2009



CarnegieMellon

CyLab *Usable Privacy* and Security Laboratory
<http://cups.cs.cmu.edu/>

Privacy is hard to define

“Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”

Robert C. Post, *Three Concepts of Privacy*,
89 Geo. L.J. 2087 (2001).



Britney Spears: “We just need privacy”

“You have to realize that we're people and that we need, we just need privacy and we need our respect, and those are things that you have to have as a human being.”

— Britney Spears
15 June 2006
NBC Dateline



<http://www.cnn.com/2006/SHOWBIZ/Music/06/15/people.spears.reut/index.html>



*Only a
goldfish can
live without
privacy...*



Some definitions from the academic literature

- Personhood
- Intimacy
- Secrecy
- Contextual integrity
- Limited access to the self
- Control over information

} Most relevant to
“usable privacy”



Limited access to self



“Being alone.”

- Shane (age 4)

1890: “the right to be let alone”

- Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)

1980: “our concern over our accessibility to others: the extent to which we are **known to others**, the extent to which others have **physical access** to us, and the extent to which we are **the subject of others attention**.”

- Ruth Gavison, “Privacy and the Limits of the Law,” *Yale Law Journal* 89 (1980)



Control over information

“Privacy is the claim of individuals, groups or institutions **to determine for themselves** when, how, and to what extent information about them is communicated to others.”

“...each individual is continually engaged in a **personal adjustment process** in which he balances the desire for privacy with the desire for disclosure and communication....”

Alan Westin, *Privacy and Freedom*, 1967



Realizing limited access and control

- Limited access
 - Laws to prohibit or limit collection, disclosure, contact
 - Technology to facilitate anonymous transactions, minimize disclosure
- Control
 - Laws to mandate choice (opt-in/opt-out)
 - Technology to facilitate informed consent, keep track of and enforce privacy preferences



Privacy concerns seem inconsistent with behavior

- People say they want privacy, but don't always take steps to protect it
- Many possible explanations
 - They don't really care that much about privacy
 - They prefer immediate gratification to privacy protections that they won't benefit from until later
 - They don't understand the privacy implications of their behavior
 - The cost of privacy protection (including figuring out how to protect their privacy) is too high



Privacy policies

- Inform consumers about privacy practices
 - Consumers can decide whether practices are acceptable, when to opt-out
- Most policies require college-level skills to understand, long, change without notice
 - Few people read privacy policies
- Existing privacy policies are not an effective way to inform consumers or give them privacy controls



Cost of reading privacy policies

- What would happen if everyone read privacy policy for each site they visited once each month?
- Time = 244/hours year
- Cost = \$3,534/year
- National opportunity cost for time to read policies: \$781 billion

A. McDonald and L. Cranor. The Cost of Reading Privacy Policis. I/S: A Journal of Law and Policy for the Informaiton Society. 2008 Privacy Year in Review Issue. <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>



Privacy policy format study

- Participants answered reading-comprehension and opinion questions about privacy policies in various formats
- People could accurately answer questions where they could find answer by scanning or key word
 - Does Acme use cookies? (98%)
- People had trouble with questions that required more reading comprehension
 - Does this policy allow Acme to put you on an email marketing list? (71%)
 - Does this policy allow Acme to share your email address with a marketing company that might put you on their email marketing list? (52%)
- Even well-written policies are not well-liked and difficult to use
- Layered notices don't appear to help much

A.M. McDonald, R.W. Reeder, P.G. Kelley, and L.F. Cranor. A comparative study of online privacy policies and formats. Privacy Enhancing Technologies Symposium 2009. <http://lorrie.cranor.org/pubs/authors-version-PETS-formats.pdf>



Requirements for meaningful control

- Individuals must understand what options they have
- Individuals must understand implications of their options
- Individuals must have the means to exercise options
- Costs must be reasonable
 - Money, time, convenience, benefits

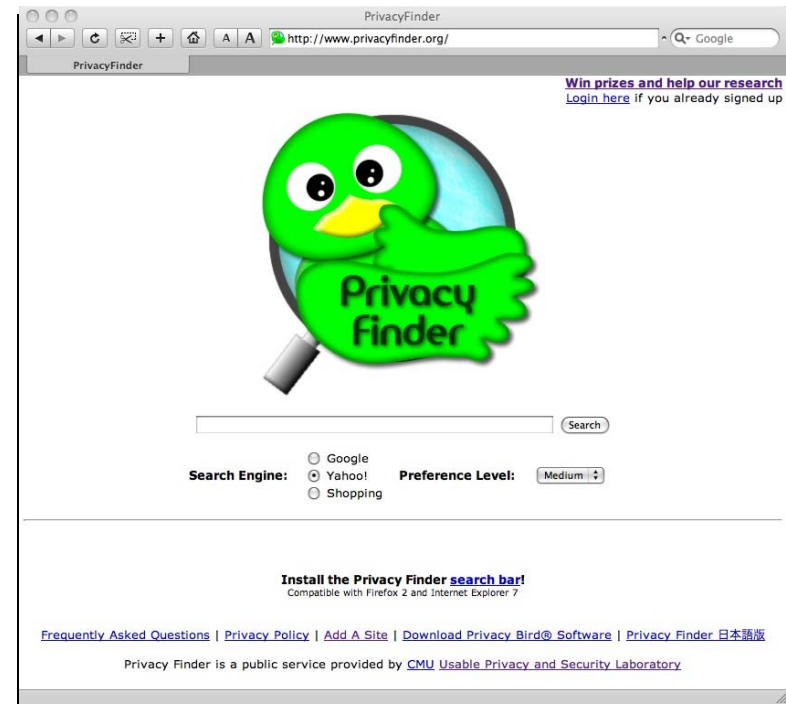


Impact of privacy information on decision making

- Studies demonstrate that when readily accessible and comparable privacy information is presented in search results, many people will pay more for better privacy

J. Tsai, S. Egelman, L. Cranor, and A. Acquisti. **The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.** WEIS 2007.
<http://weis2007.econinfosec.org/papers/57.pdf>

S. Egelman, J. Tsai, L. Cranor, and A. Acquisti. 2009. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. CHI2009.
<http://www.guanotronic.com/~serge/papers/chi09a.pdf>



<http://privacyfinder.org/>



Nutrition labels for privacy

- Standard easy-to-read format
 - Makes it easy to find info and compare policies
- Work in progress: Iterating on design and conducting user studies

P. Kelley, J. Bresee, L. Cranor, and R. Reeder. A “Nutrition Label” for Privacy. SOUPS 2009.
<http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf>

The Acme Policy					
types of information this site collects	how we use your information			who we share your information with	
	marketing	telemarketing	profiling	other companies	public forums
contact information	opt out	opt out		opt in	
cookies	opt out	opt out		opt in	
preferences	opt out	opt out		opt in	!
purchasing information	opt out	opt out		opt in	
social security number & gov't ID					
your activity on this site	opt out	opt out		opt in	!

Information not collected or used by this site: demographic, financial, health, location.

Access to your information
 This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
 Please email our customer service department

acme.com
 5000 Forbes Avenue
 Pittsburgh, PA 15213 United States
 Phone: 800-555-5555
 help@acme.com

!	we will collect and use your information in this way		we will not collect and use your information in this way
opt out	by default, we will collect and use your information in this way unless you tell us not to by opting out	opt in	by default, we will not collect and use your information in this way unless you allow us to by opting in



Questions: privacy communication

- How do we communicate meaningfully about how technology impacts privacy?
 - Behavioral advertising
 - Social networks
 - Deep packet inspection
 - Log files
 - Location sharing
- How do we help people understand privacy risks that may seem distant or not relevant to them today?
 - We have nothing to hide until it is too late
- Will different types of privacy communications be necessary for people of different cultures? Age? Gender?



Privacy in a location finding service

The screenshot displays the Locaccino web application. At the top, a red header contains the "LOCACCINO" logo and navigation links: HOME, PRIVACY SETTINGS, FRIENDS' VIEWS, LOCATOR, INVITE, and HELP. Below the header, a banner encourages users to join a study for \$30. The main interface features a map of Pittsburgh. On the left, a sidebar shows "Your location" (online at 10:50 PM) and a "Search for a friend" list with names like Chuck Cranor, Dena Tsamitis, Heng Xu, Kami Vaniea, Lorrie Cranor, Patrick Kelley, Christa Jones, and David Pierpont. A pop-up window for "Lorrie Cranor" is open, showing her profile picture, address (Near: 5344 Northumberland St, Pittsburgh, Pennsylvania 15217), and a "Show in Google Maps" button. The map shows various streets and landmarks like Schenley Park Golf Course.

<http://locaccino.org/>



Privacy rules

LOCACCINO

HOMEPRIVACY SETTINGSFRIENDS' VIEWSLOCATORINVITEHELP!

My Rules

Add New Rule

Family any time

Locaccino demo

Locaccino team

On campus

People I work with

SOUPS2009

Seattle

Washington, DC

Rule Editing

CancelSave changesDelete

Rule name





People I work with

Who

Who can see my location?

New Locaccino Friend ListClick for all lists and networksShow all





Faculty



and 22 more...

Remove | Edit





Locaccino team



and 7 more...

Remove | Edit

PhD students



and 3 more...

Remove | Edit

When

When can they see my location?

☐ I can be seen all the time

☒ I can be seen part of the time...

☐ Sun

☒ Mon

☒ Tue

☒ Wed

☒ Thu

☒ Fri

☐ Sat

From: 8:00 am

To: 6:00 pm

☐ All day

Where

Where can they see my location?

e.g. my friends can see my location only when I'm in the Carnegie-Mellon University campus

☒ I can be seen in all locations

☐ I can be seen in these locations...

CancelSave changes

Carnegie Mellon

CyLab Usable Privacy and Security Laboratory

<http://cups.cs.cmu.edu/>

18

Feedback

LOCACCINO

HOME

PRIVACY SETTINGS

FRIENDS' VIEWS

LOCATOR


INVITE

Who asked to view me


Who can view me right now

Unhappy? Go to Privacy Settings and fix your rules


Friends who can view your current location



Chuck Cranor




Judy Ackerman




Seth Carlson


Friends who cannot view your current location




Vassilis Kosta...




Heng Xu




Christa Jones




Marvin Sir




Jason Hong




Paul Drielsma




Steve Sheng




Joe Locac




Lujo Bauer




Jialiu Lin



Patrick Kelley



Heidi Brayer



Kursat Ozenc

LOCACCINO

HOME

PRIVACY SETTINGS

FRIENDS' VIEWS

LOCATOR

INVITE

HELP












Who asked to view me

Who can view me right now

Show records from:

All records

Please indicate how comfortable you are with each of the viewing records
☒ Very uncomfortable | ☐ Uncomfortable | ☐ Comfortable | ☐ Very Comfortable
 Unhappy? Go to Privacy Settings and fix your rules

	Friend	Time	Location	Outcome	Feedback
	Paul Drielsma	11:35 AM, Thu, Jun 11	Cambridge, Massachusetts 02142 [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Steve Sheng	11:08 PM, Wed, Jun 10	[map]	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Eran Toch	4:58 PM, Wed, Jun 10	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Steve Sheng	4:40 PM, Wed, Jun 10	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Jay Springfield	4:11 PM, Wed, Jun 10	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Kami Vaniea	12:51 PM-12:52 PM, Wed, Jun 10	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Patrick Kelley	12:50 PM-12:51 PM, Wed, Jun 10	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Kami Vaniea	11:21 AM, Wed, Jun 10	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Eran Toch	4:52 PM, Tue, Jun 9	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Paul Drielsma	4:34 PM, Tue, Jun 9	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Kami Vaniea	2:12 PM-2:13 PM, Tue, Jun 9	Carnegie Mellon University [map]	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Carnegie Mellon

CyLab Usable Privacy and Security Laboratory

<http://cups.cs.cmu.edu/>

19

Privacy configuration

- How do we simplify the creation of privacy rules?
- How do we allow people to easily set their privacy preferences up front for a range of applications?
- How do we help people realize when adjustments to these settings are needed and adjust them easily (or automatically?)



Privacy conflicts

- How do we balance the need to store information with the need to discard information to protect privacy?
 - Information used to provide feedback to users, automate privacy configuration, improve application functionality
- How do we balance the need to store access data for audit purposes with the need to protect employee privacy?
- How do we balance the need to discard information to protect privacy with the needs of law enforcement?
- Can we use technology to preserve privacy and enable all of the above?



Evaluating informed consent UIs

- Typical UI metric is successful completion of task
- Informed consent experiences result in fewer people completing task
- What metrics should we use?



Anonymity tools

- Anonymity tools typically hide users in cover traffic or send traffic via a circuitous route
- Users typically give up speed, convenience, functionality for anonymity
- Turning anonymity tools on and off is cumbersome and requires user action
- Can we provide anonymity without deteriorating user experience?



More questions

- As today's youth grow up with their lives online, will they come to expect less privacy?
- As we increasingly tradeoff privacy for convenience and functionality, are we doomed to a slow erosion of privacy that eventually leaves us with minimal expectations of privacy?
- Can “usable privacy” be designed into technology to provide convenience and functionality without sacrificing privacy?





Cylab Usable Privacy and Security
Laboratory

<http://cups.cs.cmu.edu/>

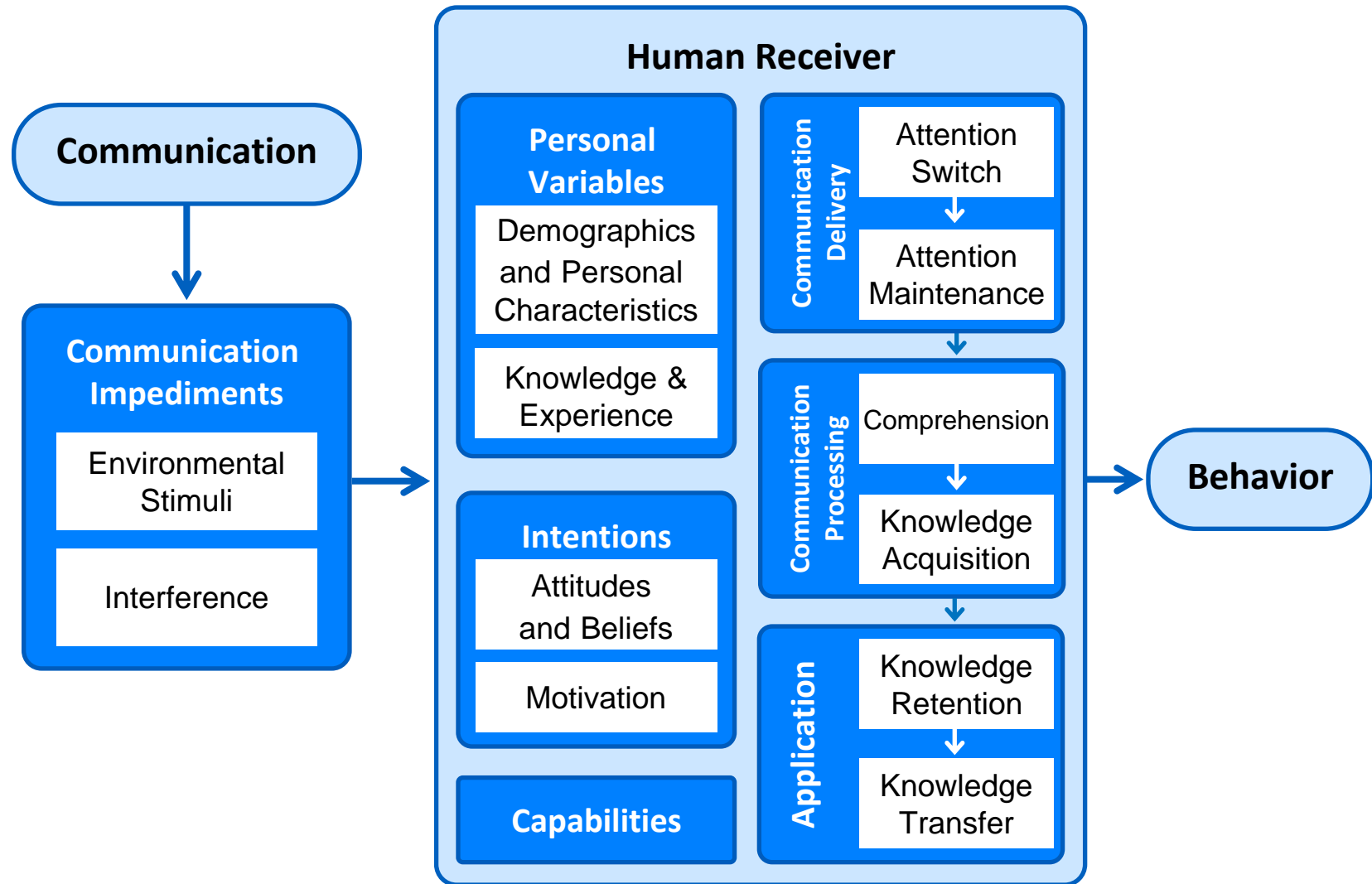
Carnegie Mellon

The human in the loop framework

- A model of all the ways that humans may fail to perform the actions expected of them when using a secure system



Human-in-the-loop framework



Human threat identification and mitigation process

