

# 03- Reasoning about the Human in the Loop

Lujo Bauer, Nicolas Christin,  
and Abby Marsh

January 20, 2016

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734  
*Usable Privacy and Security*

Carnegie  
Mellon  
University  
CyLab

**isr** institute for  
SOFTWARE  
RESEARCH

Engineering &  
Public Policy



# Today!

- Human in the Loop Framework
- Everyday usability
- Privacy illustrated

# The Human in the Loop

# The human threat

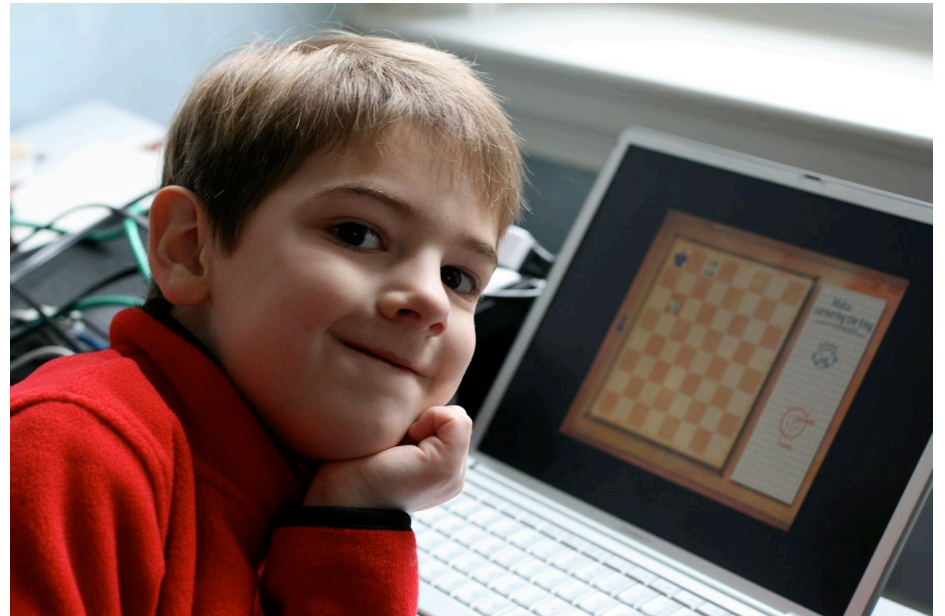
- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations



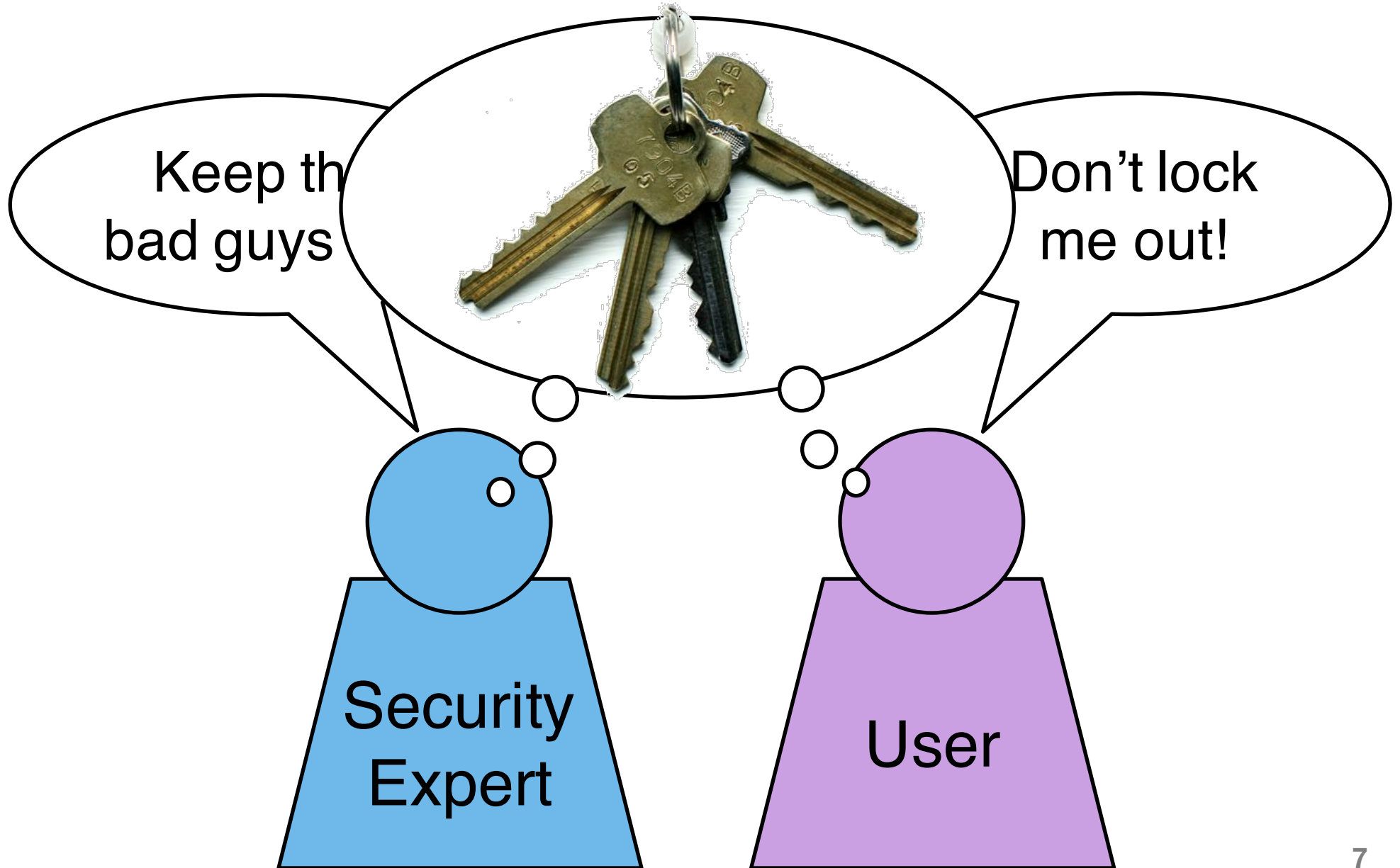
Are you capable  
of remembering  
a unique strong  
password for  
every account  
you have?



# Security is a secondary task



# Concerns may not be aligned



# Grey

- Smartphone based access-control system
- Used to open doors in the Carnegie Mellon CIC building
- Allows users to grant access to their doors remotely

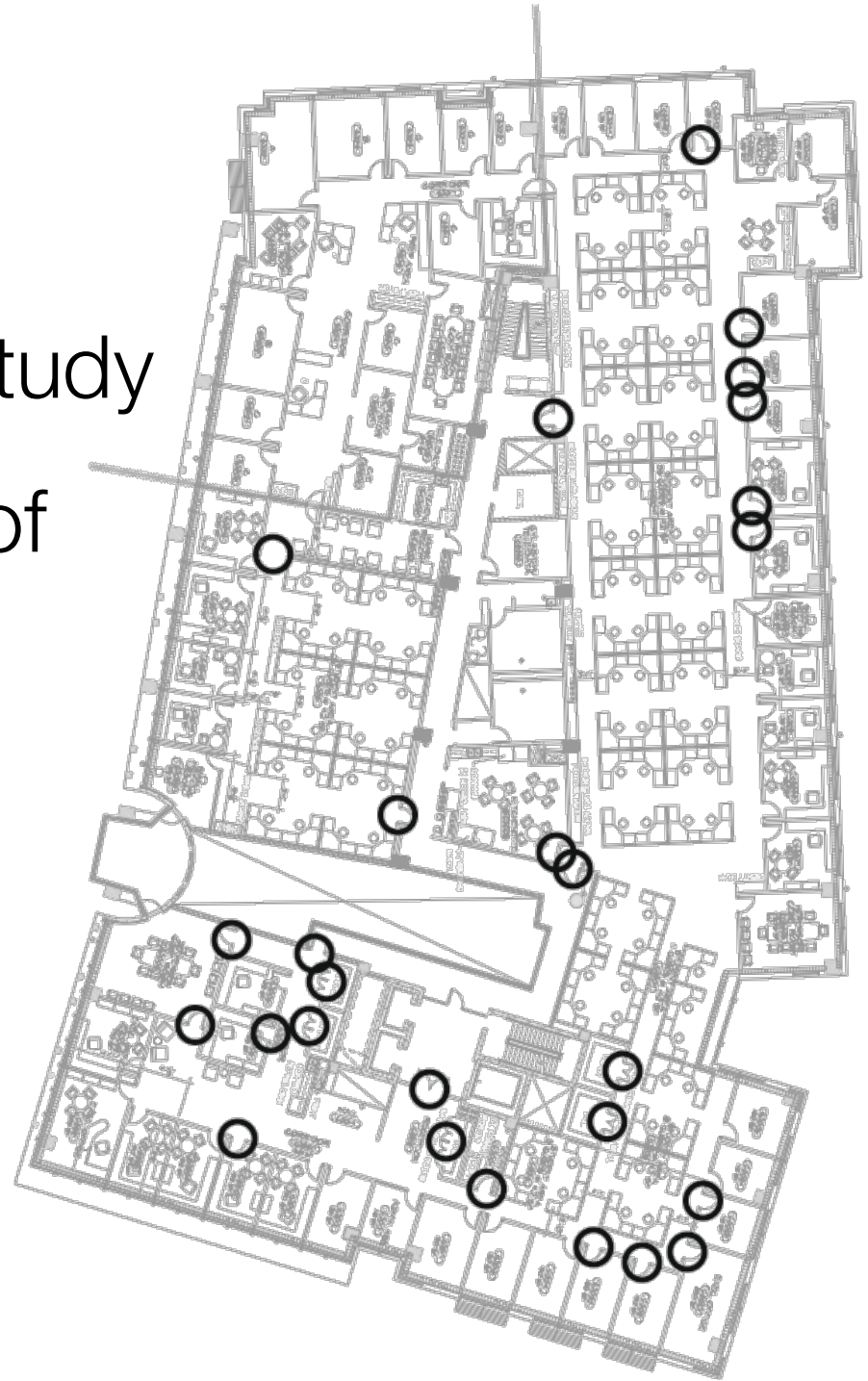


L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, and K. Vania. **A User Study of Policy Creation in a Flexible Access-Control System.** CHI 2008. <http://www.robreeder.com/pubs/greyCHI2008.pdf>

L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vania. **Lessons Learned from the Deployment of a Smartphone-Based Access-Control System.** SOUPS 2007. [http://cups.cs.cmu.edu/soups/2007/proceedings/p64\\_bauer.pdf](http://cups.cs.cmu.edu/soups/2007/proceedings/p64_bauer.pdf)

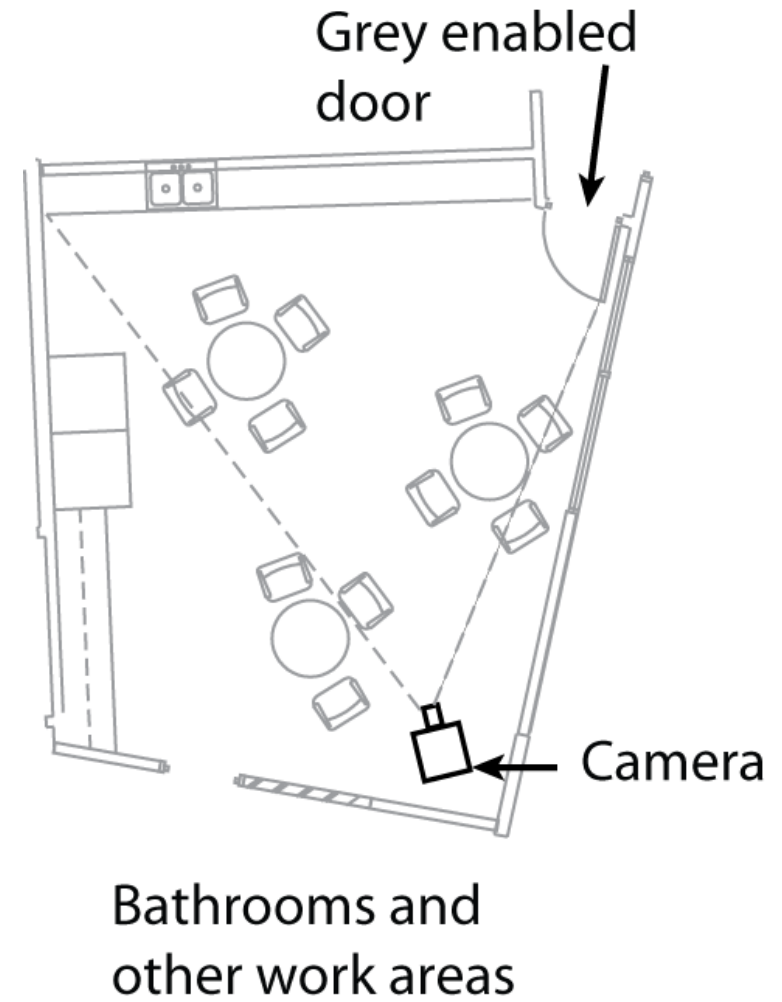
# Data collection

- Year long interview study
- Recorded 30 hours of interviews with Grey users
- System was actively used: 29 users x 12 accesses per week

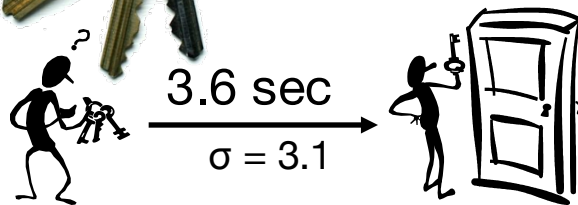


# Users complained about speed

- Users said Grey was slow
- But Grey was as fast as keys
- Videotaped a door to better understand how doors are opened differently with Grey and keys



# Average access times



Getting  
keys

3.6 sec  
 $\sigma = 3.1$



Stop in  
front of  
door

5.4 sec  
 $\sigma = 3.1$



Door  
opened

5.7 sec  
 $\sigma = 3.6$



Door  
Closed

**Total  
14.7  
sec**

$\sigma = 5.6$



Getting  
phone

8.4 sec  
 $\sigma = 2.8$



Stop in  
front of  
door

2.9 sec  
 $\sigma = 1.5$



Door  
opened

3.8 sec  
 $\sigma = 1.1$



Door  
Closed

**Total  
15.1  
sec**

$\sigma = 3.9$



“I find myself standing outside and everybody inside is looking at me standing outside while I am trying to futz with my phone and open the stupid door.”

# Nobody wants to have to reboot their door

## DOOR

An exception 06 has occurred at 0028:C11B3ADC in VxD DiskTSD(03) + 00001660. This was called from 0028:C11B40C8 in VxD voltrack(04) + 00000000. It may be possible to continue normally.

- \* Press any key to attempt to continue.
- \* Press CTRL+ALT+RESET to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue

# Unanticipated uses can bolster acceptance

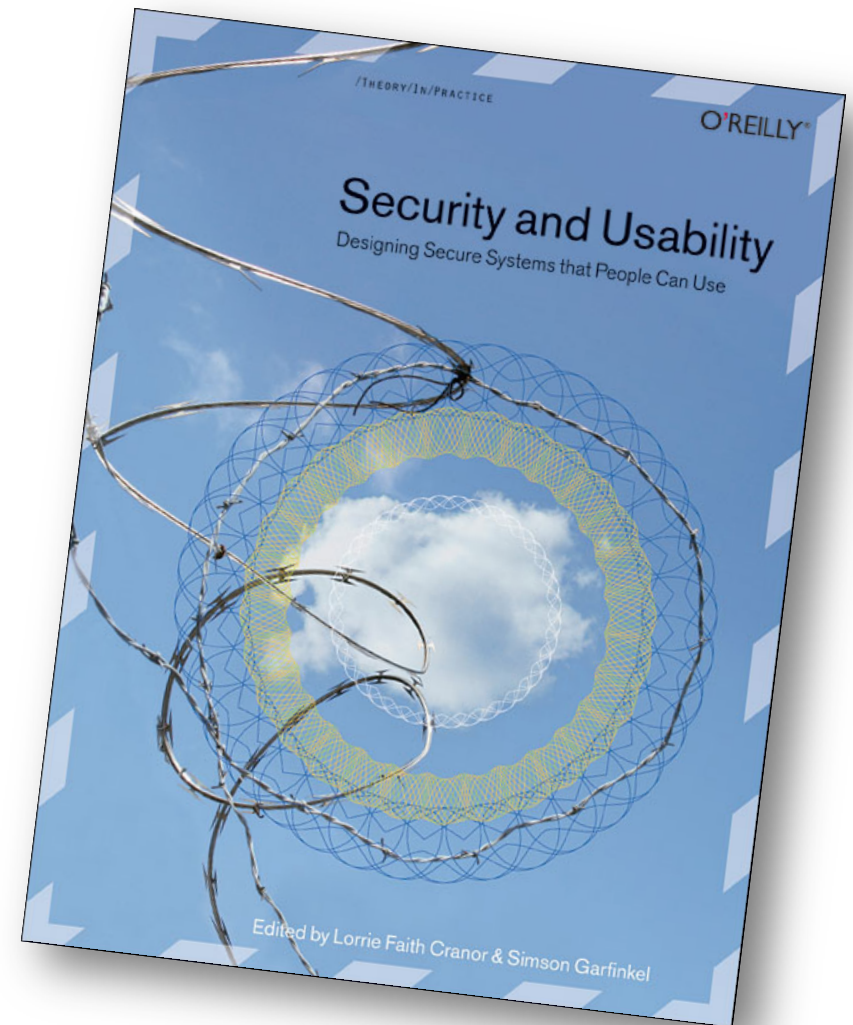


# Convenience always wins



# How can we make secure systems more usable?

- Make it “just work”
  - Invisible security
- Make security/privacy understandable
  - Make it visible
  - Make it intuitive
  - Use metaphors that users can relate to
- Train the user



# Try to better understand humans in the loop

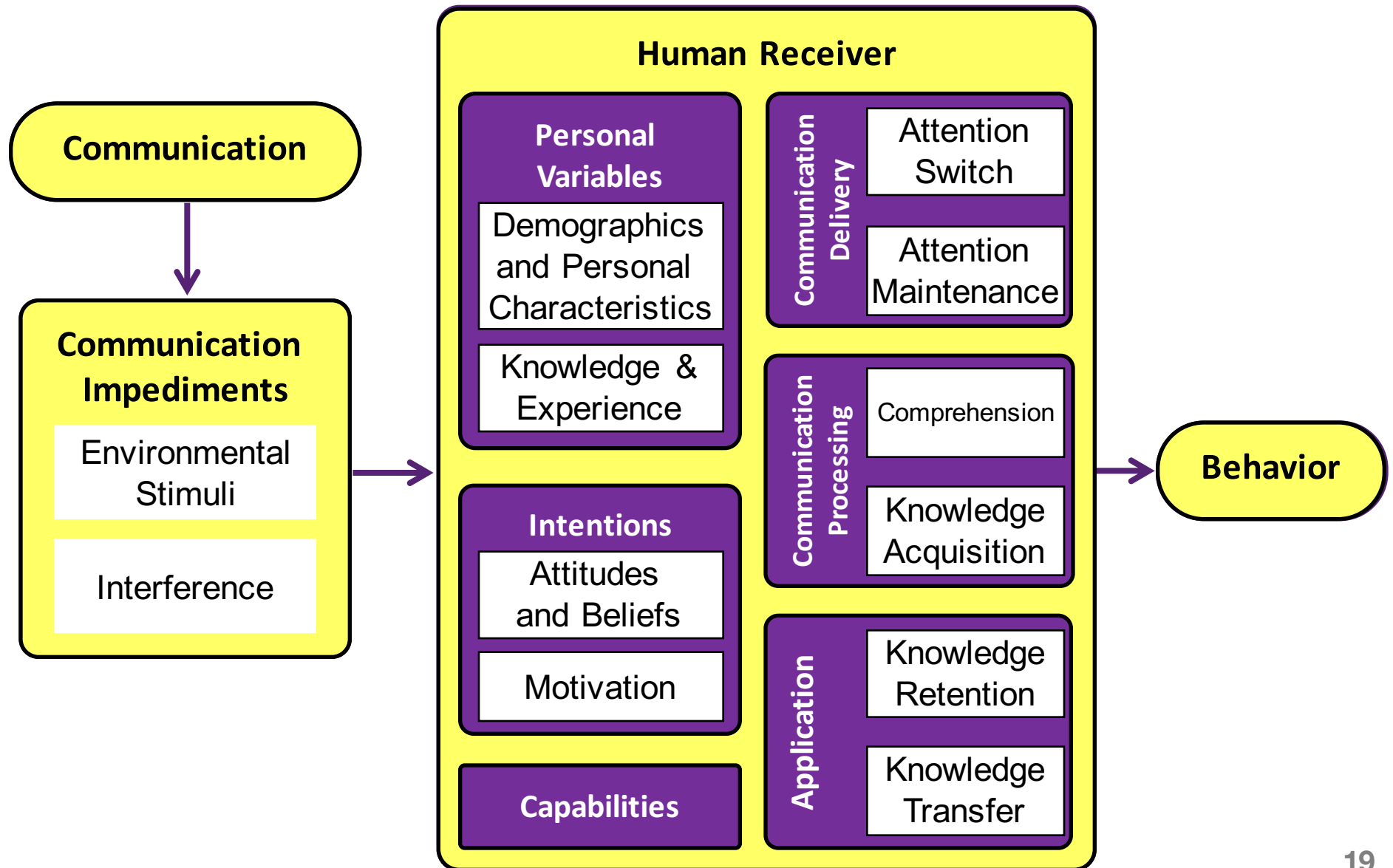
- Do they know they are supposed to be doing something?
- Do they understand what they are supposed to do?
- Do they know how to do it?
- Are they motivated to do it?
- Are they capable of doing it?
- Will they actually do it?

# Human-in-the-loop framework

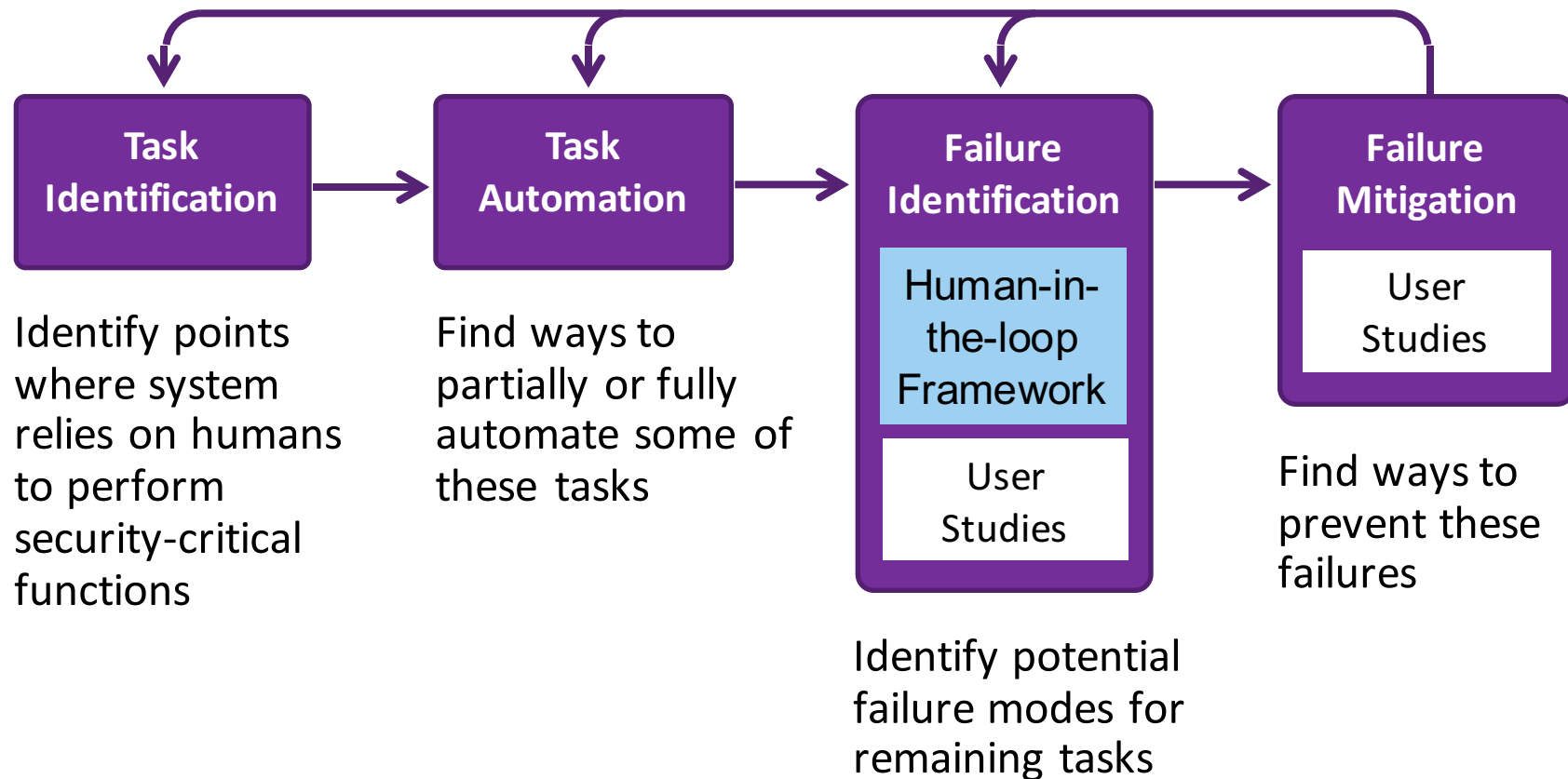
- Based on Communication-Human Information Processing Model (C-HIP) from Warnings Science
- Models human interaction with secure systems
- Can help identify human threats



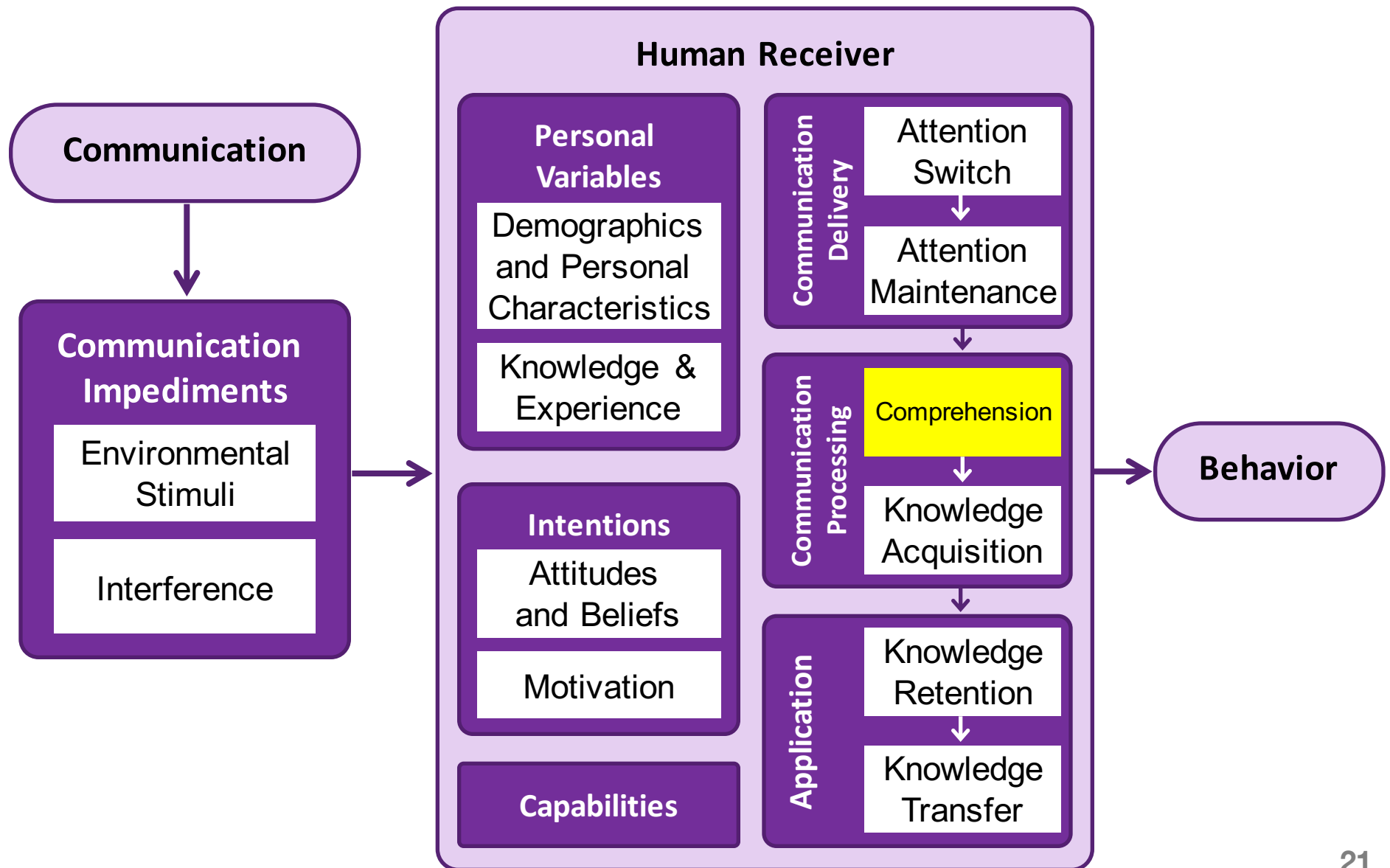
# Human-in-the-loop framework

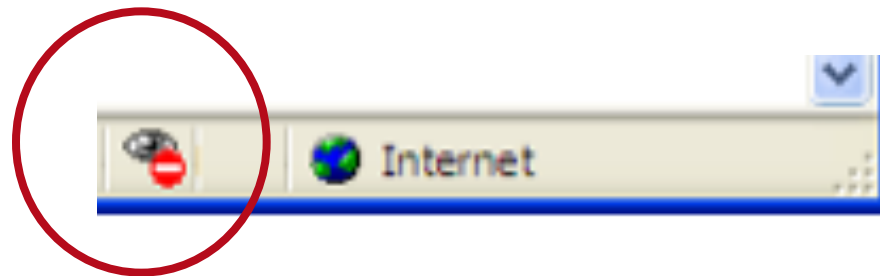


# Human threat identification and mitigation process



# Human-in-the-loop framework





Internet Explorer cookie flag



Privacy policy  
**matches** user's  
privacy preferences



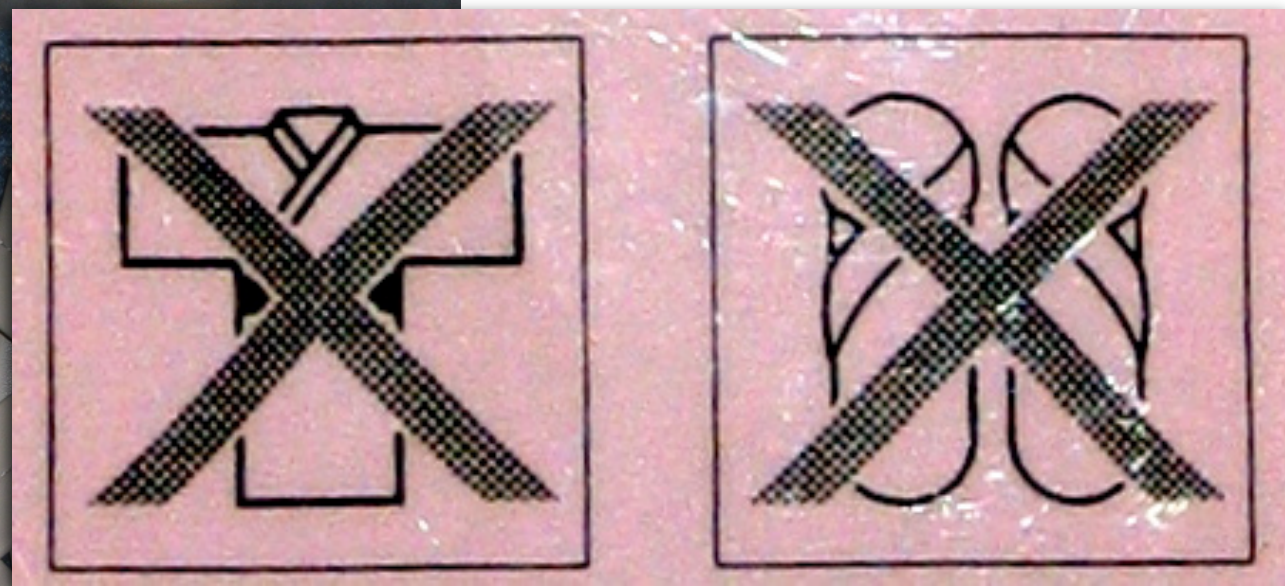
Privacy policy  
**does not match**  
user's privacy  
preferences

OPERATOR SPECIALTY COMPANY, INC.



Moving Gate Can Cause  
Serious Injury or Death





# Warnings





What to do about hazards?



Best solution: remove hazard



Next best: guard against hazard









If all else fails: warn

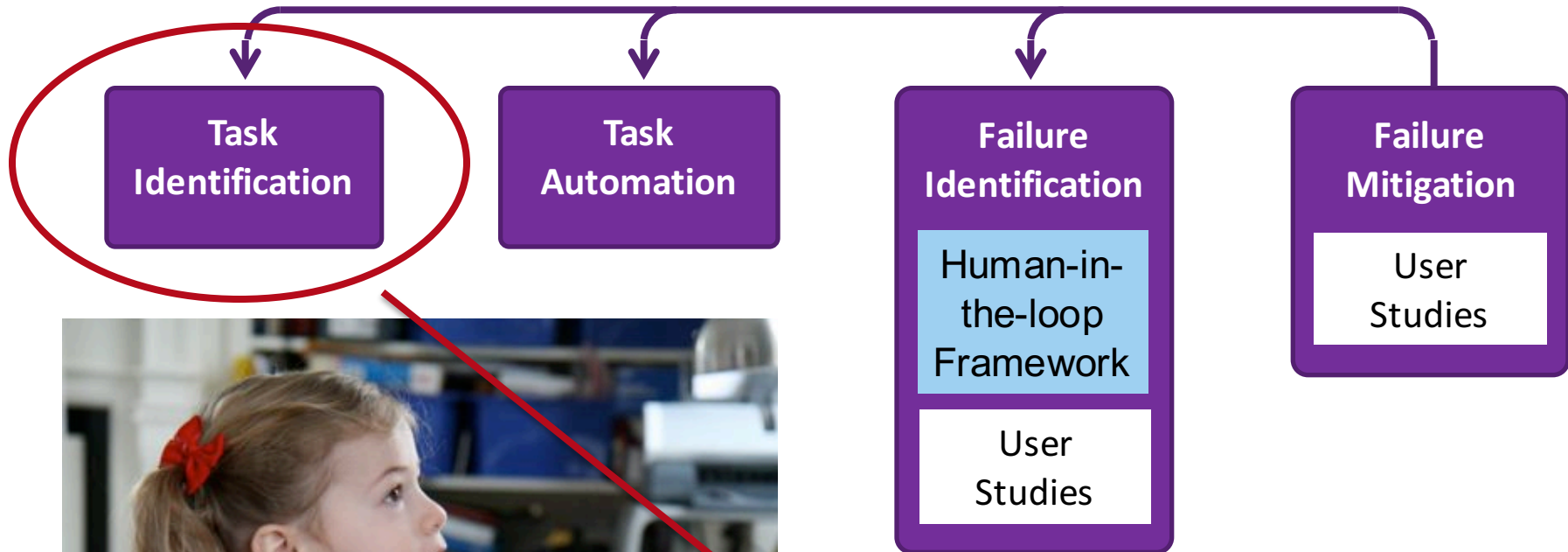


CAUTION

CAUTION

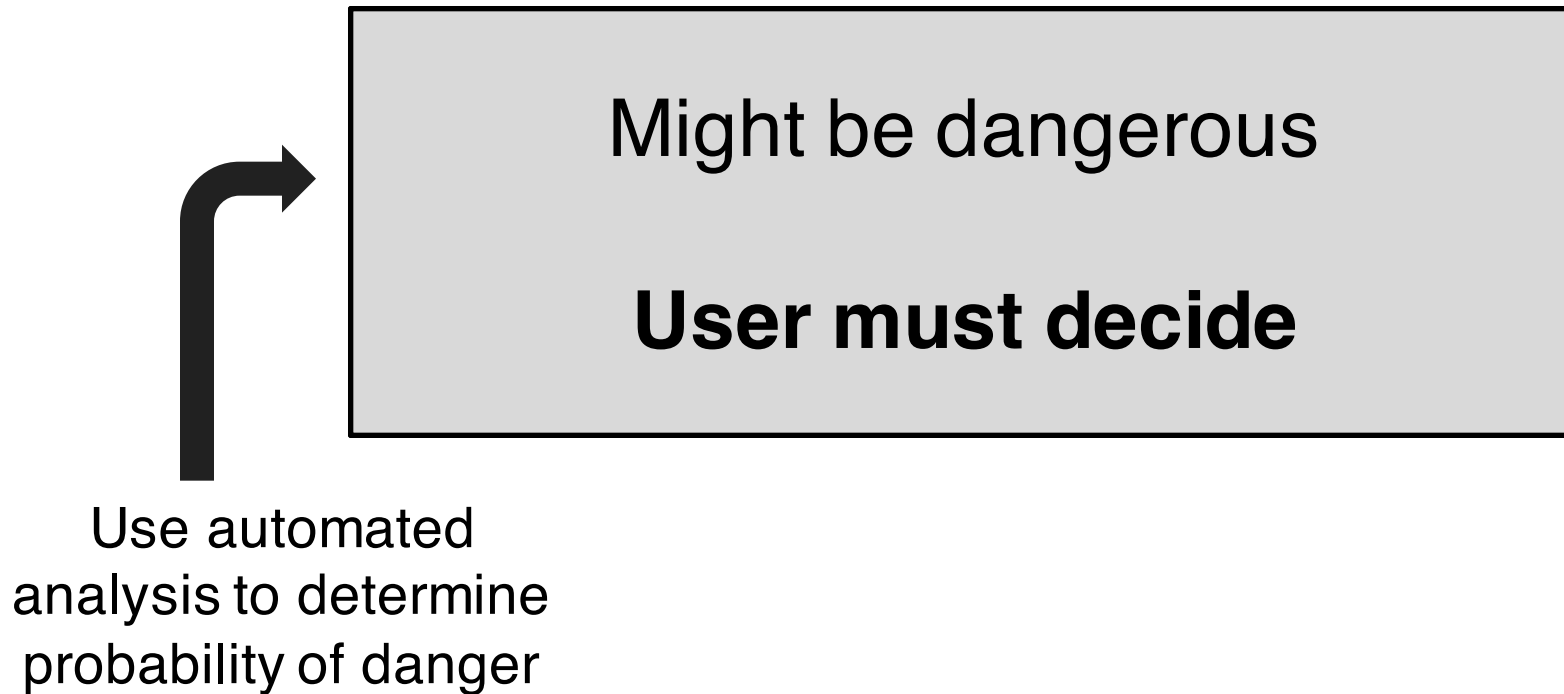
CAUTION  UNEVEN SURFACES

# Human threat mitigation for warnings



Determine whether task I am trying to complete is sufficiently risky that I should stop

# Automate and change tasks to reduce need for user involvement



# Support user decision



Improve warnings

Help user decide by asking question  
user is qualified to answer

# Bad question

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

Don't go there

Go there anyway

*I don't know what a phishing site is.*

*I really want to go to this site.*

*Of course I will go there anyway!*



# Better question

You are trying to go to evilsite.com. Do you really want to go there or would you rather go to yourbank.com?

Go to yourbank.com

Go to evilsite.com

*Of course I want to go to  
yourbank.com!*



# Everyday usability



Life vest below center armrest  
Fasten seat belt while seated



and the *Journal of Management* (1997).

IN QUESTO LOCALE È

A circular red sign with a diagonal slash over a cigarette, indicating 'No Smoking'.

RAUCHEN  
VERBOTEN  
NO SMOKING

Reproduction and posting of articles is prohibited without the written consent of the publisher. For more information, contact the publisher at 1000 Lakeshore Drive, Suite 100, Oak Brook, IL 60171, USA. Tel: 630/584-1000. Fax: 630/584-1001. E-mail: [info@elsevier.com](mailto:info@elsevier.com). Web: <http://www.elsevier.com>. Copyright © 2005 Elsevier Inc. All rights reserved.

Dasgupta and Stiglitz (1980) argument on patents

La dipendenza è un'emozione. Ma non è solo un'emozione. È un'emozione che si nutre di paura, di ansia, di rabbia, di dolore, di vergogna, di disperazione. È un'emozione che si nutre di tutti questi sentimenti, che li fa crescere, che li fa diventare una parte di noi. È un'emozione che si nutre di tutti questi sentimenti, che li fa crescere, che li fa diventare una parte di noi.







Please leave me on.

I will turn the light and fan off  
automatically after 4 minutes  
of detecting no movement.



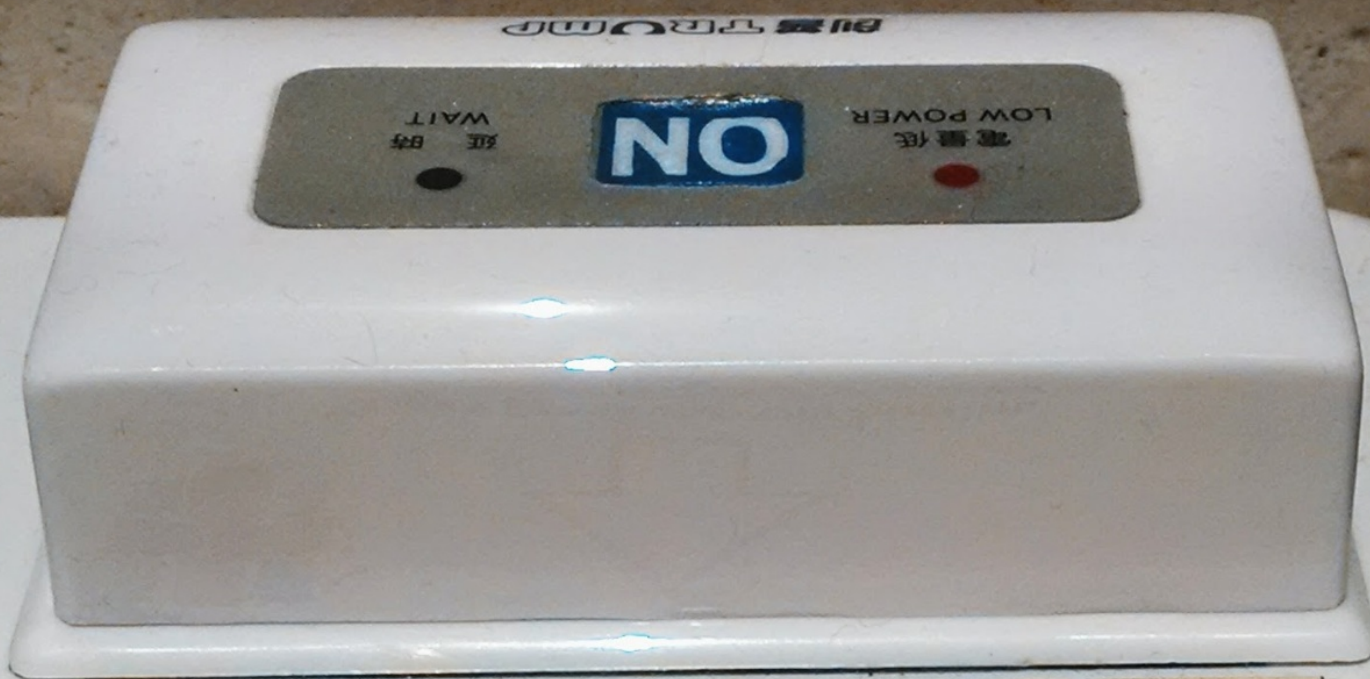
I will turn on automatically  
when someone walks in.











杀菌  
消毒



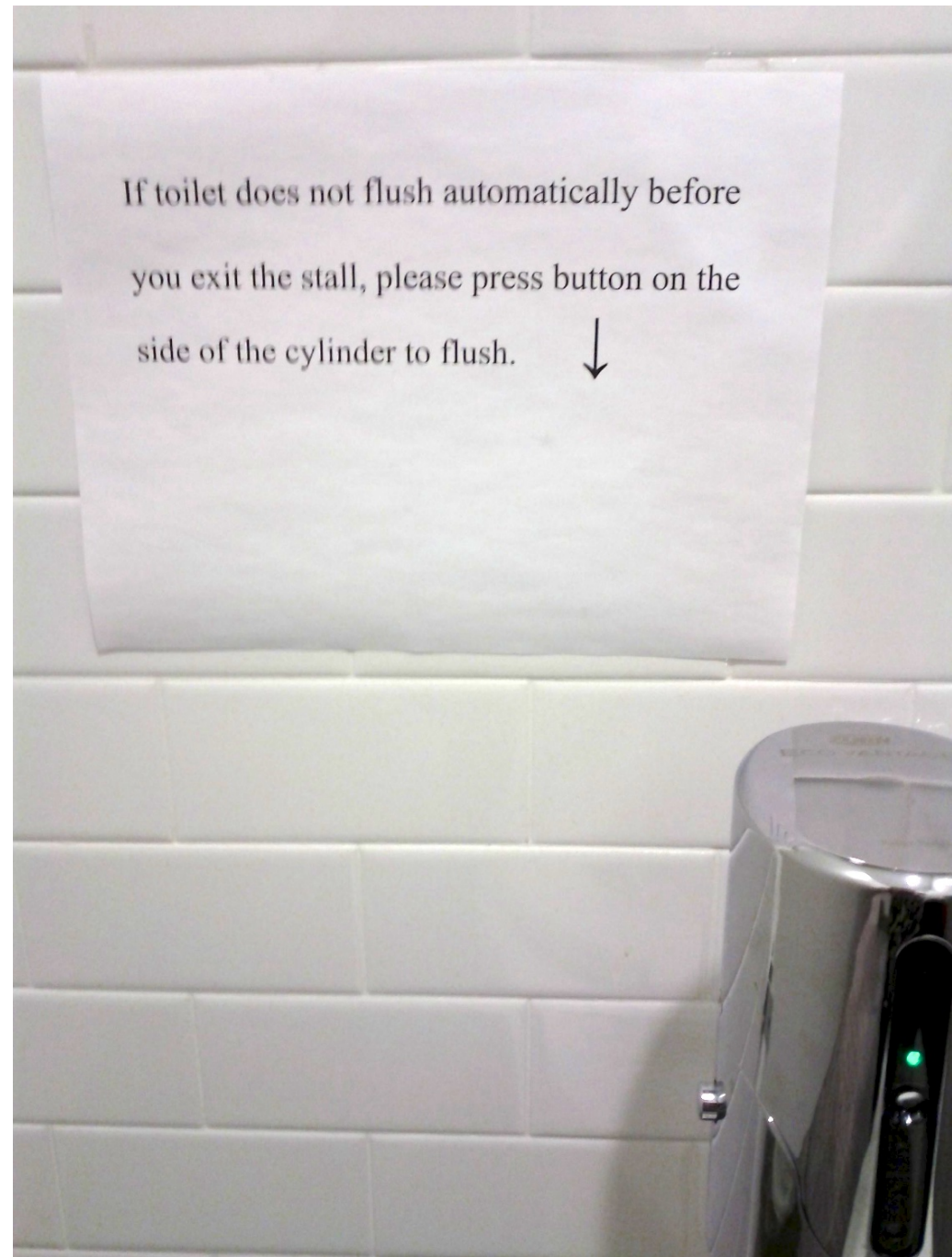
Please press the ON button.

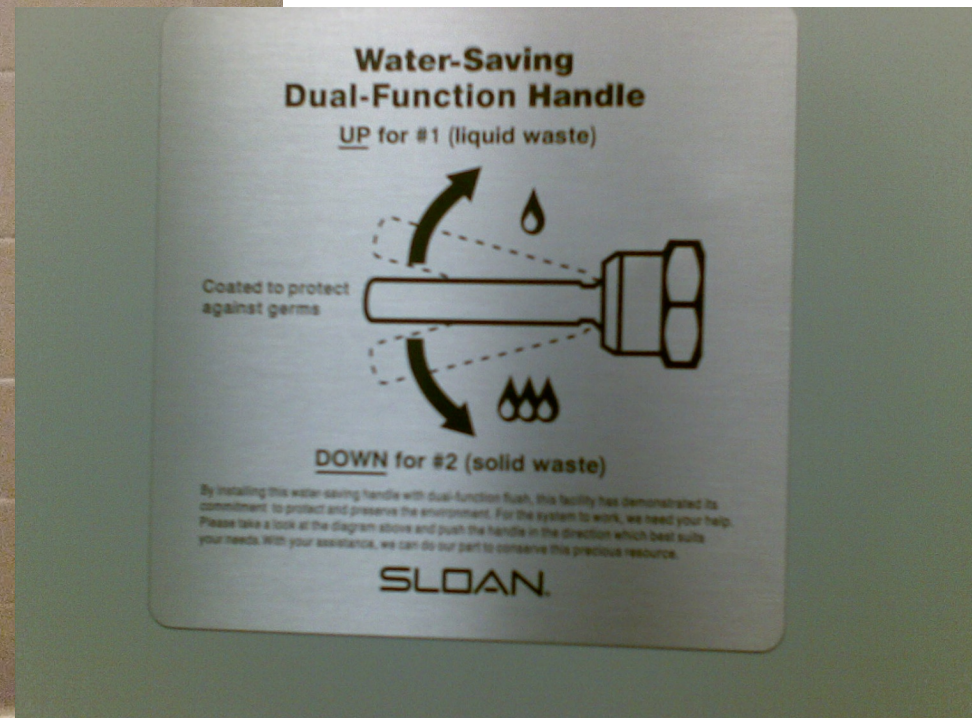
更换一次性便洁套，请按ON键

PLEASE NOTE THAT  
THIS FACILITY IS NOT  
EQUIPPED WITH AN  
AUTOMATIC FLUSHING  
SYSTEM.  
PLEASE FLUSH PRIOR  
TO LEAVING THE  
STALL.

THANK YOU FOR YOUR COOPERATION,

**CBRE**  
CB RICHARD ELLIS



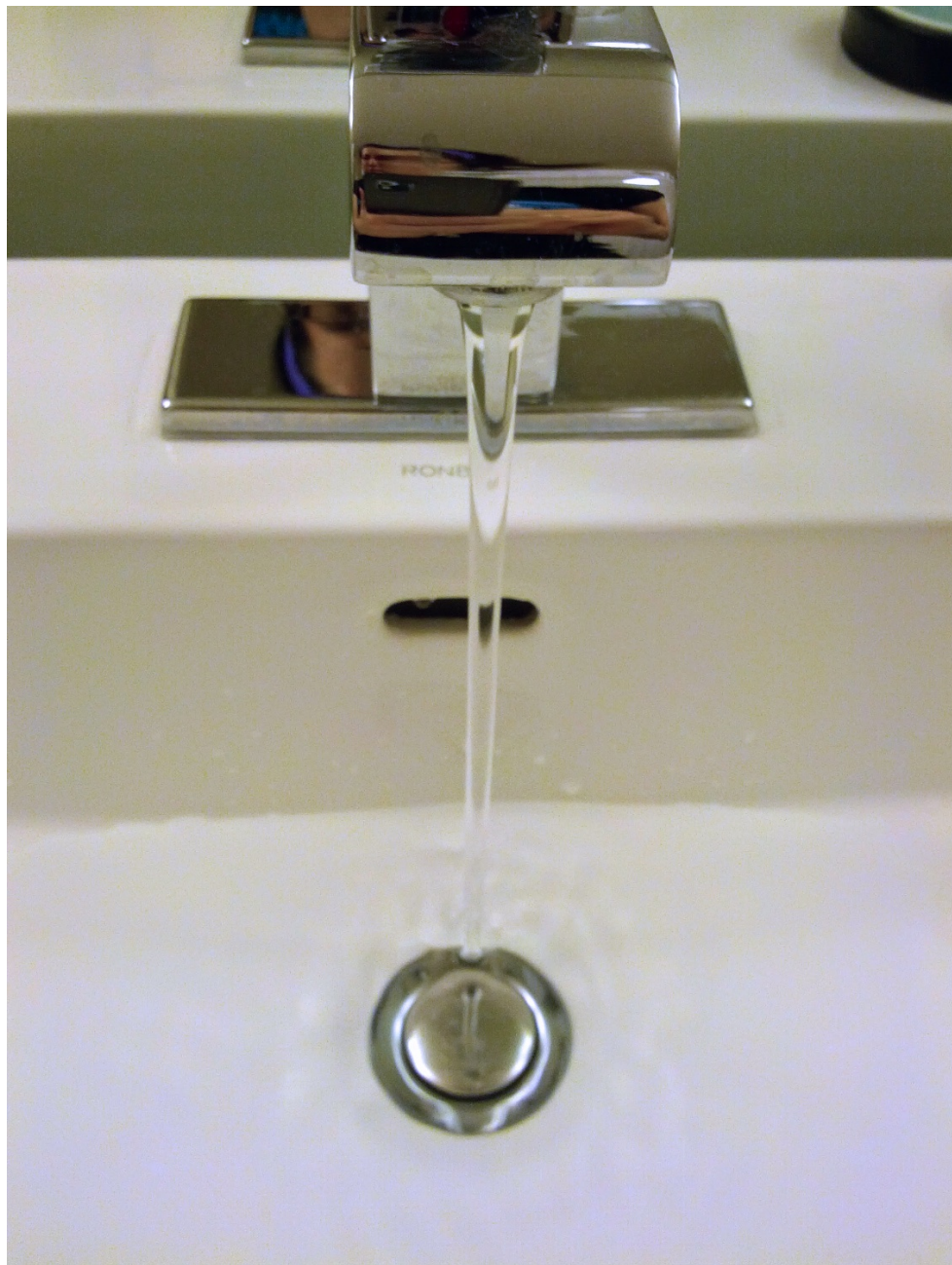














This bathtub has been treated with snash  
2000 anti-slip substance for your safety

אמבטיה זו עברה טיפול סנאש 2000  
למניעת החלקה לביטחונך האישי



סנאש שיווק בינלאומי בע"מ SNASH int Markating  
טל. 972-3-5748483







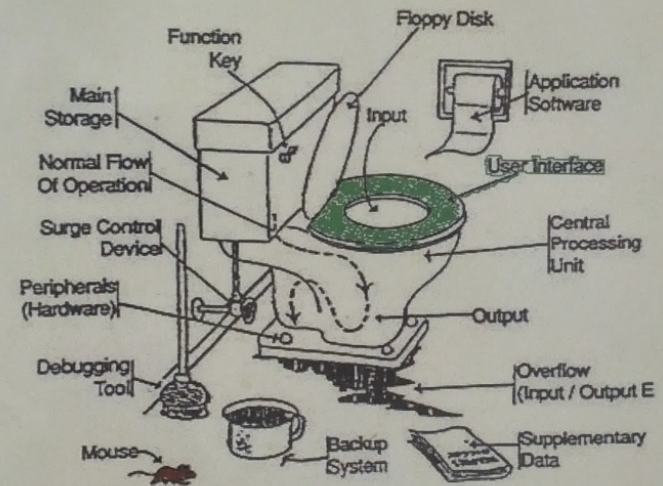
IF THIS RESTROOM IS  
IN NEED OF ATTENTION,

PLEASE CALL:  
225-4141

PLEASE USE THE FOLLOWING  
IDENTIFIER FOR THIS RESTROOM:  
C2B1

HOUSE SUPERINTENDENT'S OFFICE

Please make an effort to keep this bathroom clean for everyone who uses it. No trash on the floor, clean up after yourself and please be neat.



Please clean the **user interface** when your application is completed.

Thank you.



## IMAGES OF PRIVACY

**What does privacy mean to you?** We asked people to draw what privacy means to them. We went into schools to ask children of different ages, and we asked adults across the United States to contribute their images of privacy. Now we're asking people around the world to add to our collection. Explore the drawings here:

[abstract](#) [ads](#) [age20-29](#) [age30-39](#) [age40-49](#)

[age50-59](#) [age60-69](#) [age90-99](#) [alone](#) [alone/private space](#)

[anonymous](#) [away from family](#) [bank statement](#) [basement](#) [bathing](#)

[bathroom](#) [bedroom](#) [big brother](#) [blanket](#) [bow](#) [box](#) [brain](#) [browser](#)