03- Reasoning about the Human in the Loop

Lorrie Cranor

January 25, 2017

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

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

Today’s class

- Human in the Loop Framework
- Usable privacy and security studies 101
- Everyday usability
- Privacy illustrated

The Human in the Loop

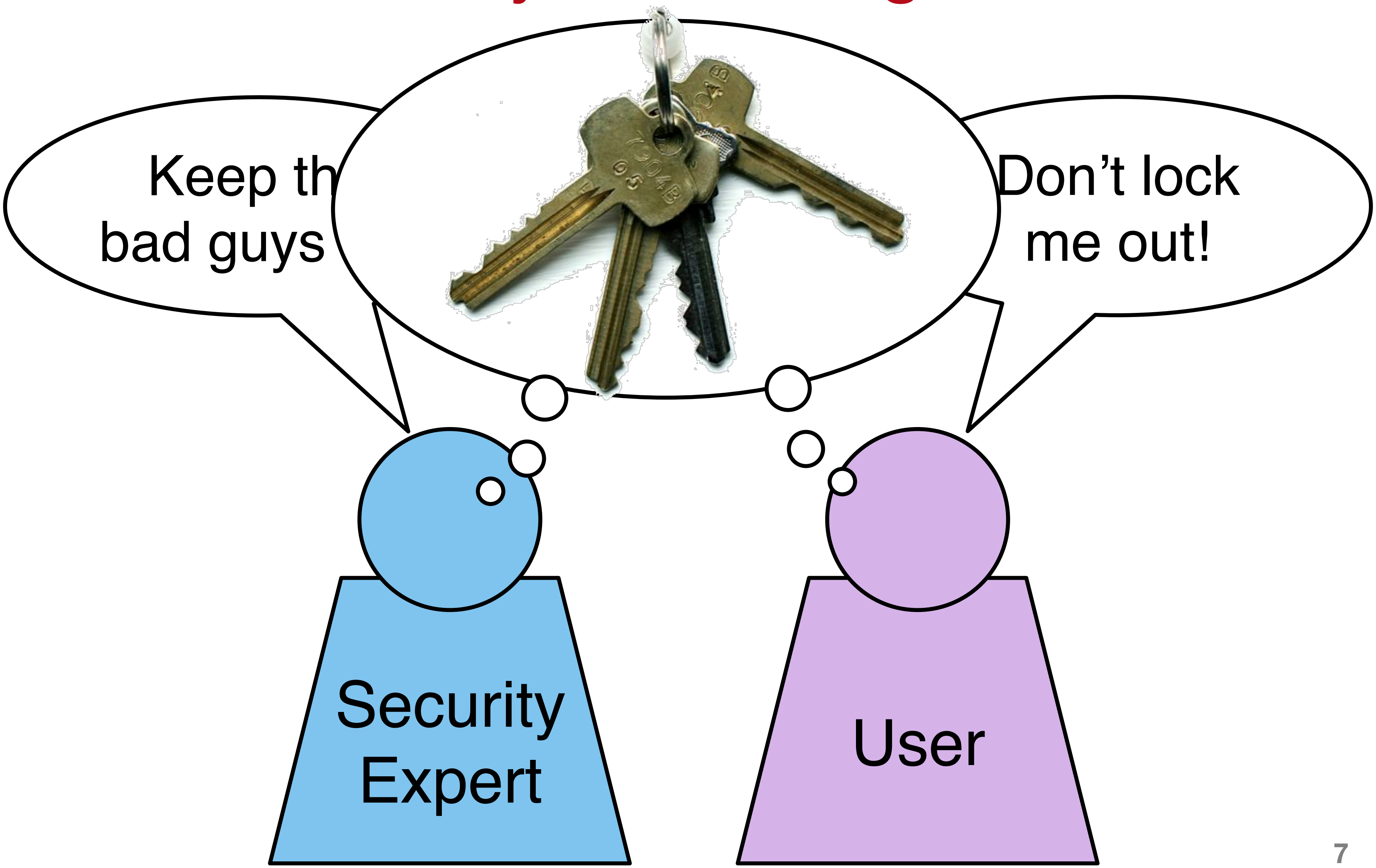
The human threat

- 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



Keep th
bad guys

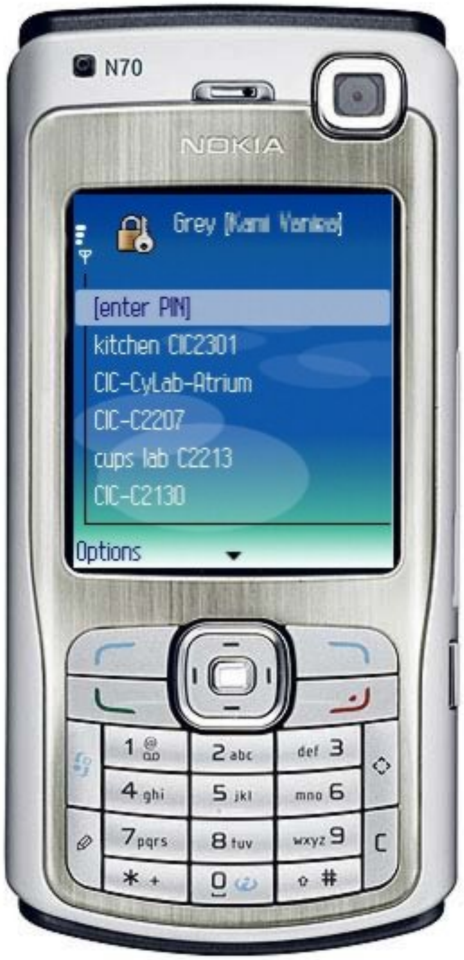
Don’t lock
me out!

Security
Expert

User

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

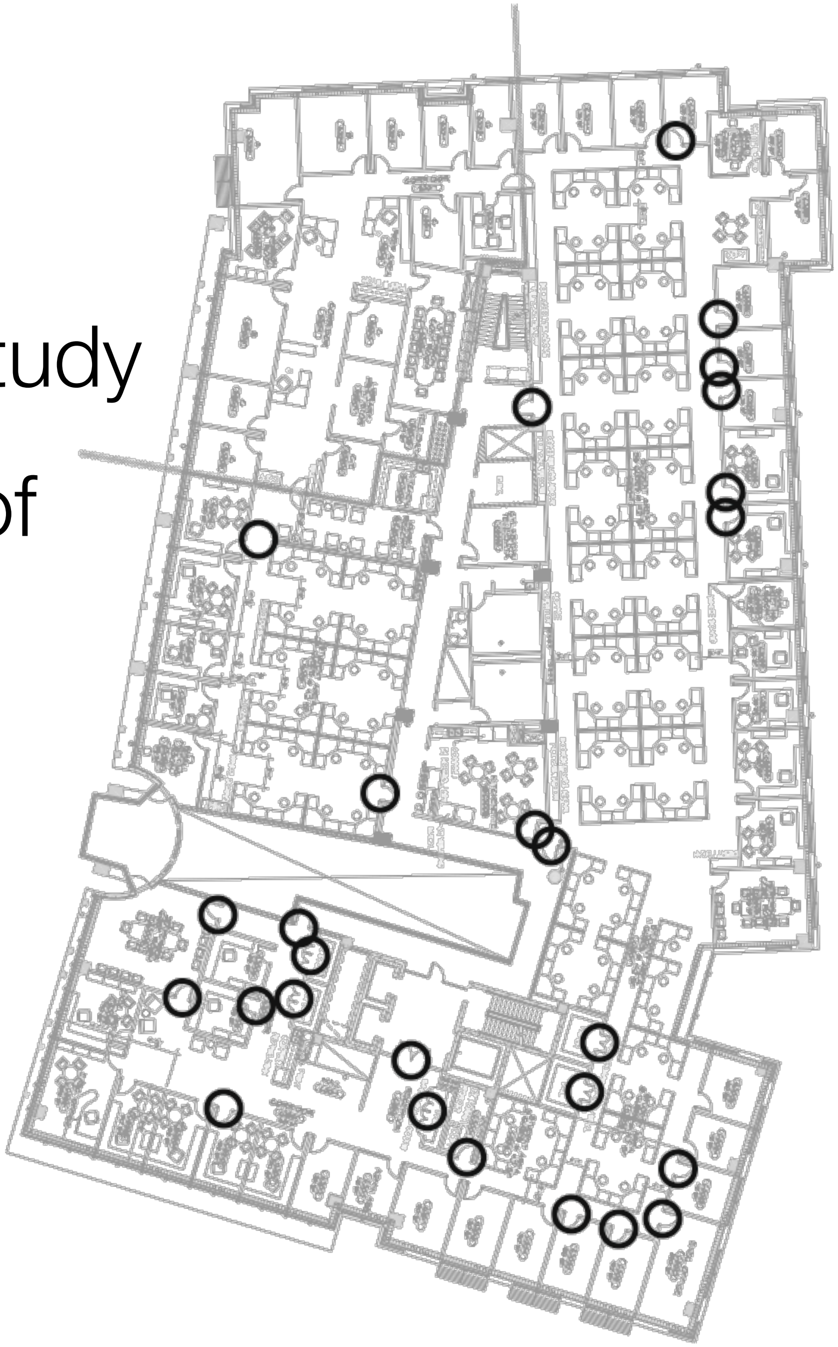


L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, and K. Vaniea. A User Study of Policy Creation in a Flexible Access-Control System. CHI 2008. http://www.robreeder.com/pubs/greyCHI2008.pdf

L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. 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

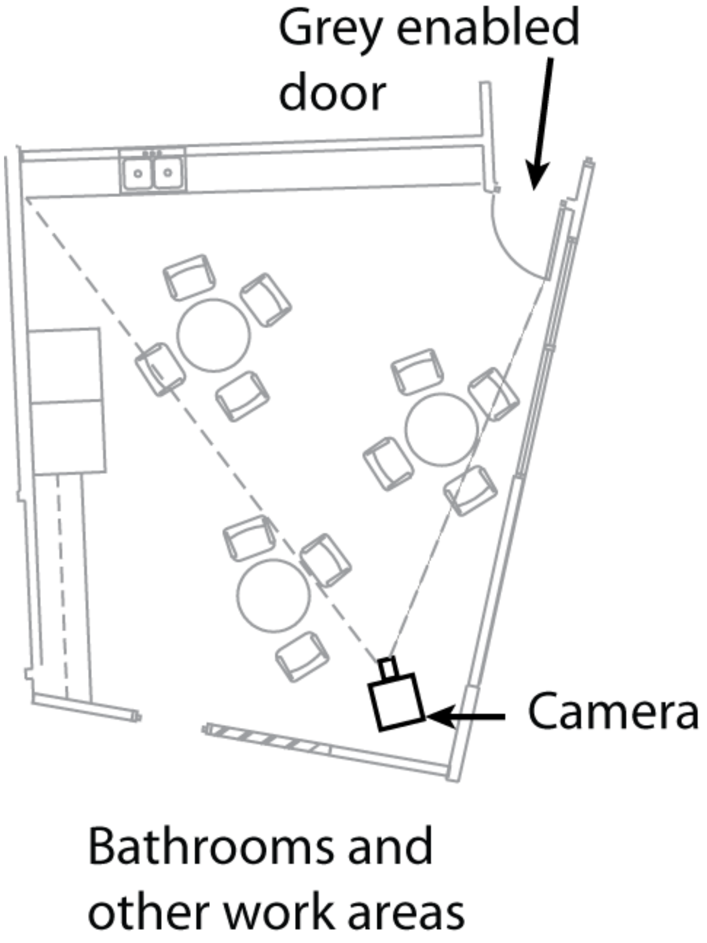
Data collection

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

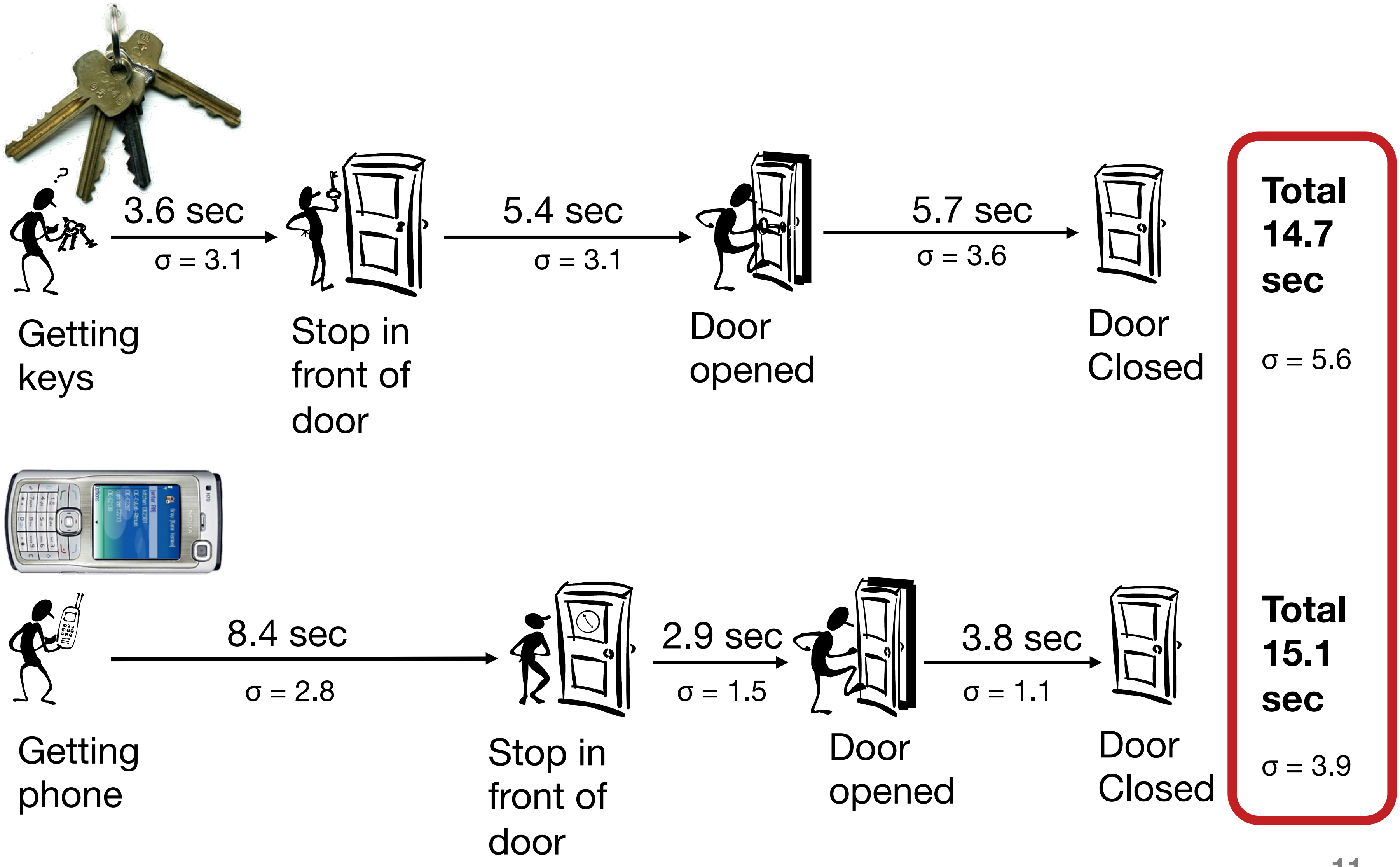


Users complained about speed

- 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, σ = 3.1 → Stop in front of door → 5.4 sec, σ = 3.1 → Door opened → 5.7 sec, σ = 3.6 → Door Closed

Total 14.7 sec

σ = 5.6

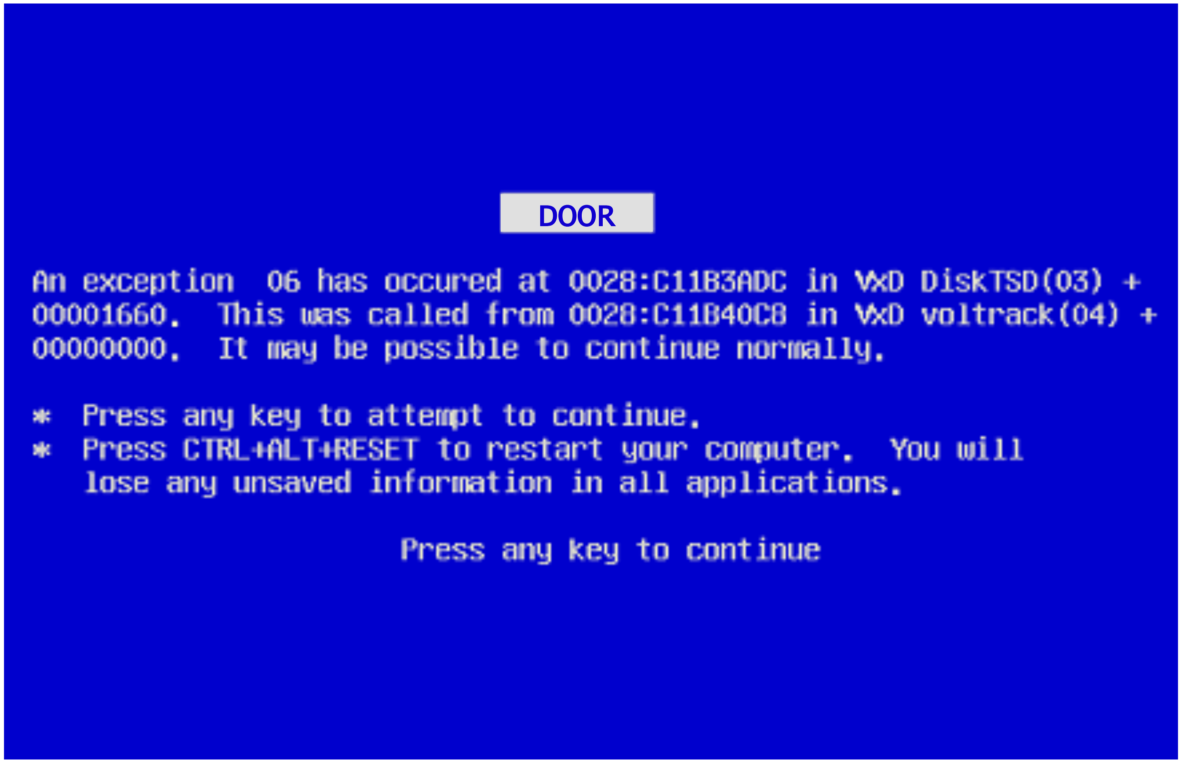
Getting phone → 8.4 sec, σ = 2.8 → Stop in front of door → 2.9 sec, σ = 1.5 → Door opened → 3.8 sec, σ = 1.1 → Door Closed

Total 15.1 sec

σ = 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



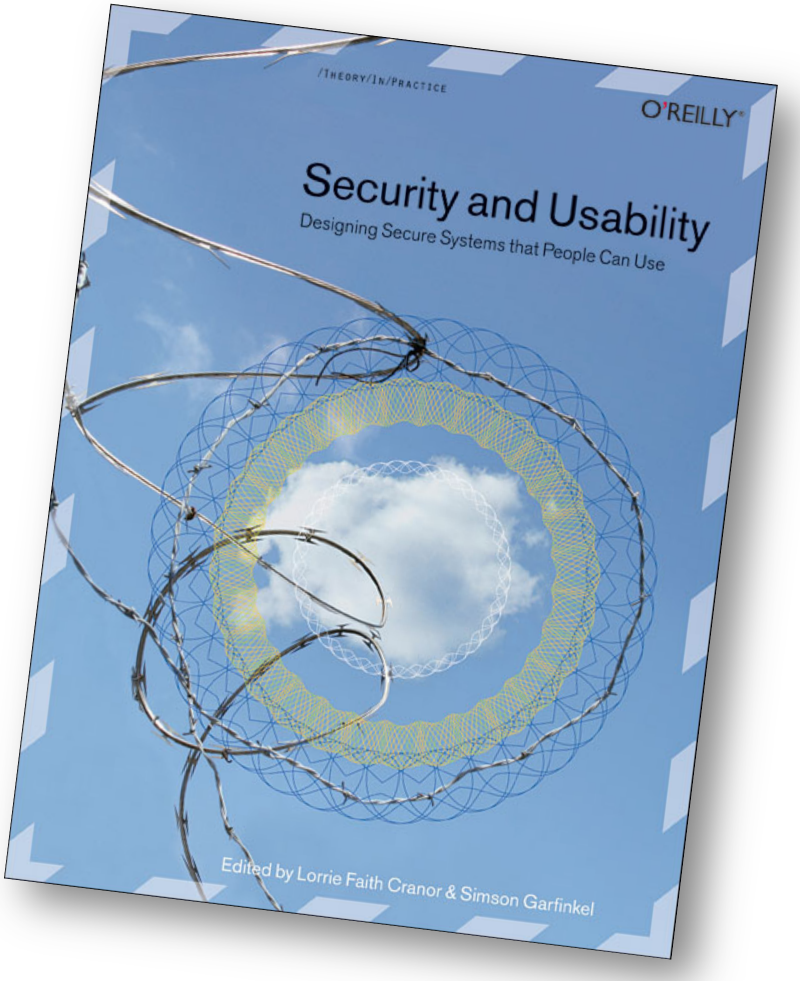
```
                          DOOR

An exception  06 has occured 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


/THEORY/IN/PRACTICE
O'REILLY®
Security and Usability
Designing Secure Systems that People Can Use
Edited by Lorrie Faith Cranor & Simson Garfinkel

What can make a system unusable?

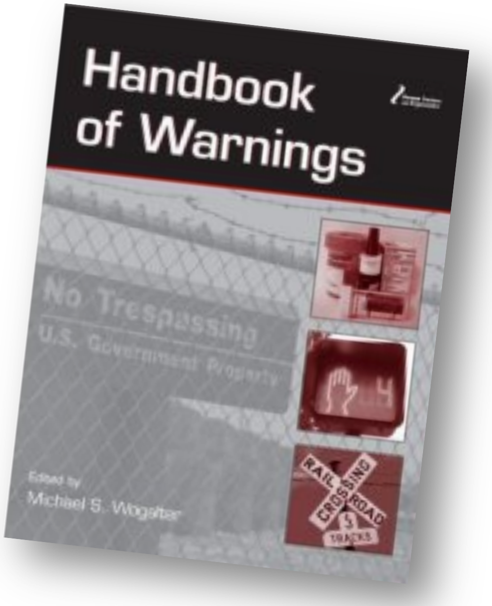
- Confusing / misleading / unhelpful user interface
- Requiring user to make decisions for which user is not qualified
- Assuming knowledge or abilities that user doesn’t have
- Assuming unreasonable amount of attention / effort

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

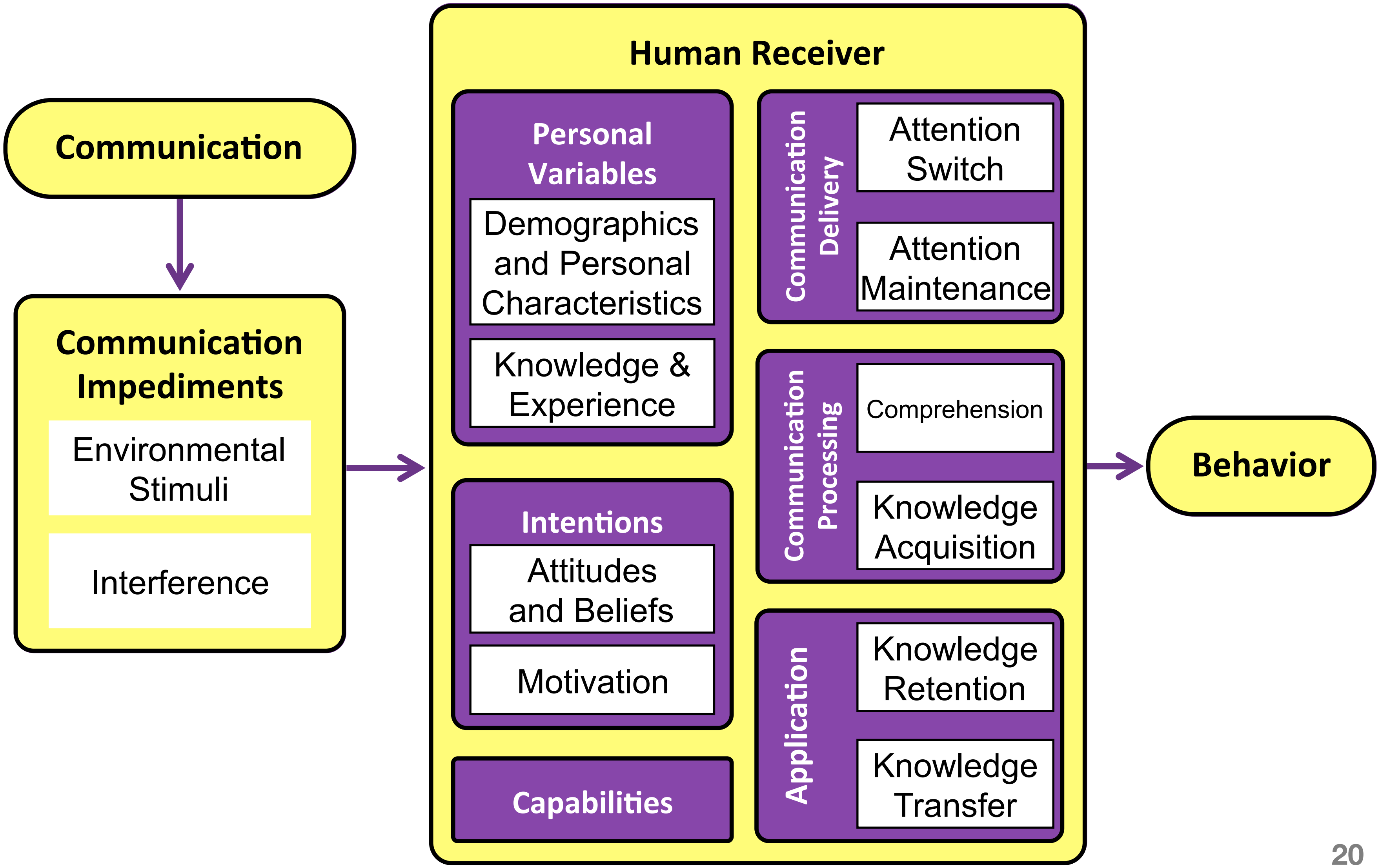
- Based on Communication-Human Information Processing Model (C-HIP) from Warnings Science



- Models human interaction with secure systems
- Can help identify human threats

L. Cranor. A Framework for Reasoning About the Human In the Loop. Usability, Psychology and Security 2008. http://www.usenix.org/events/upsec08/tech/full_papers/cranor/cranor.pdf

Human-in-the-loop framework



Communication

Communication Impediments

Environmental Stimuli

Interference

Human Receiver

Personal Variables

Demographics and Personal Characteristics

Knowledge & Experience

Intentions

Attitudes and Beliefs

Motivation

Capabilities

Communication Delivery

Attention Switch

Attention Maintenance

Communication Processing

Comprehension

Knowledge Acquisition

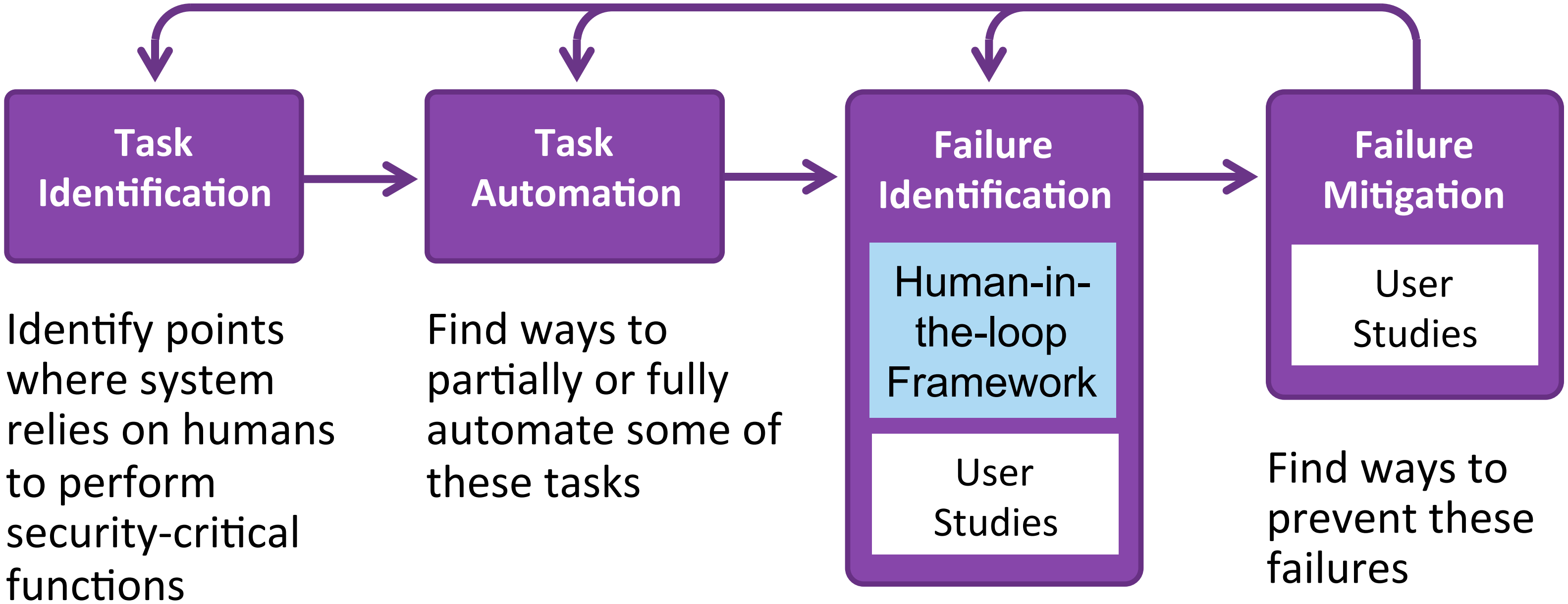
Application

Knowledge Retention

Knowledge Transfer

Behavior

Human threat identification and mitigation process



Task Identification

Identify points where system relies on humans to perform security-critical functions

Task Automation

Find ways to partially or fully automate some of these tasks

Failure Identification

Human-in-the-loop Framework

User Studies

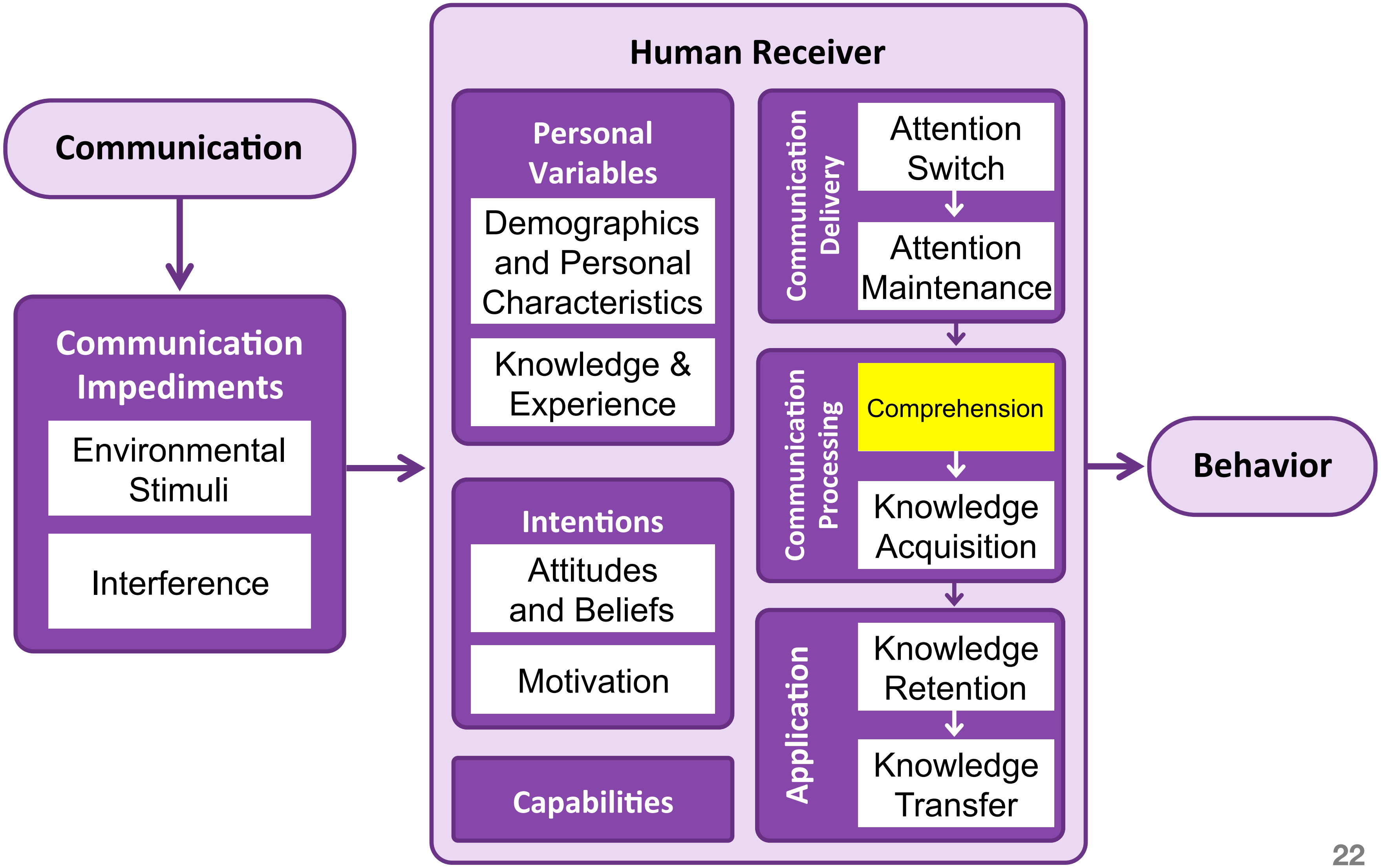
Identify potential failure modes for remaining tasks

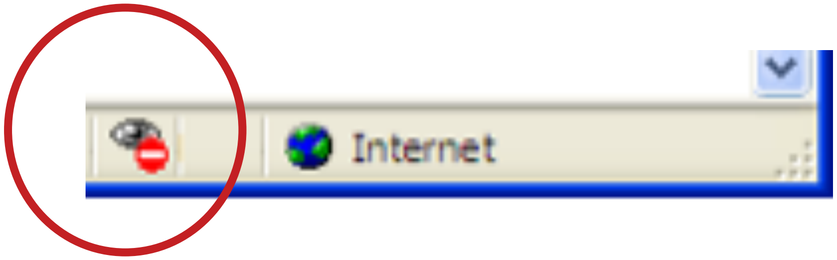
Failure Mitigation

User Studies

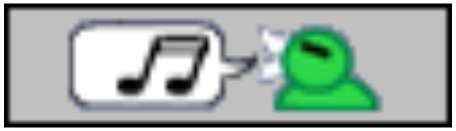
Find ways to prevent these failures

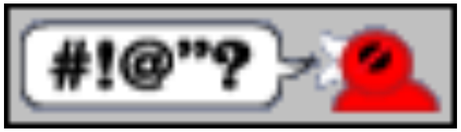
Human-in-the-loop framework





Internet Explorer cookie flag

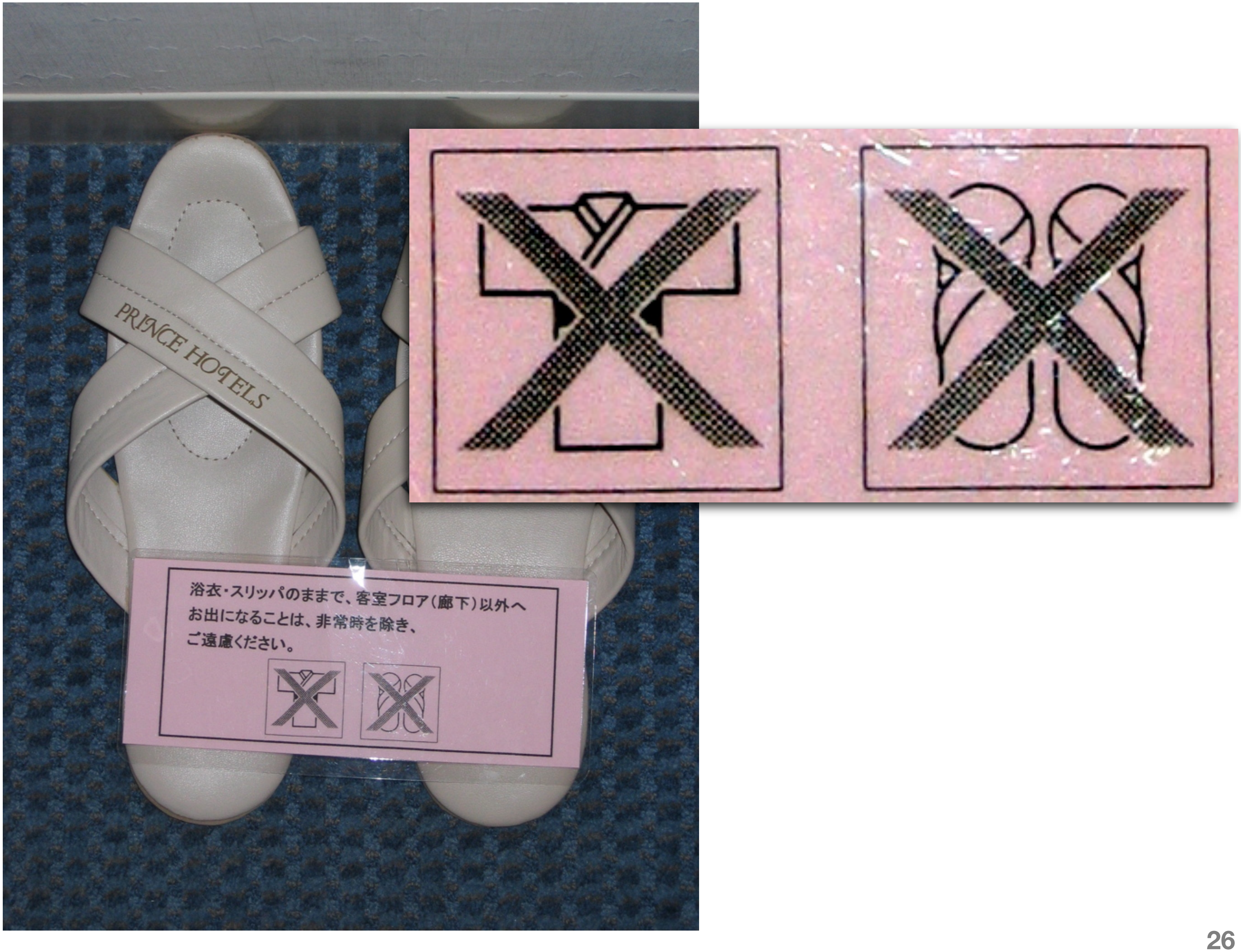




Privacy policy ***matches*** user's privacy preferences

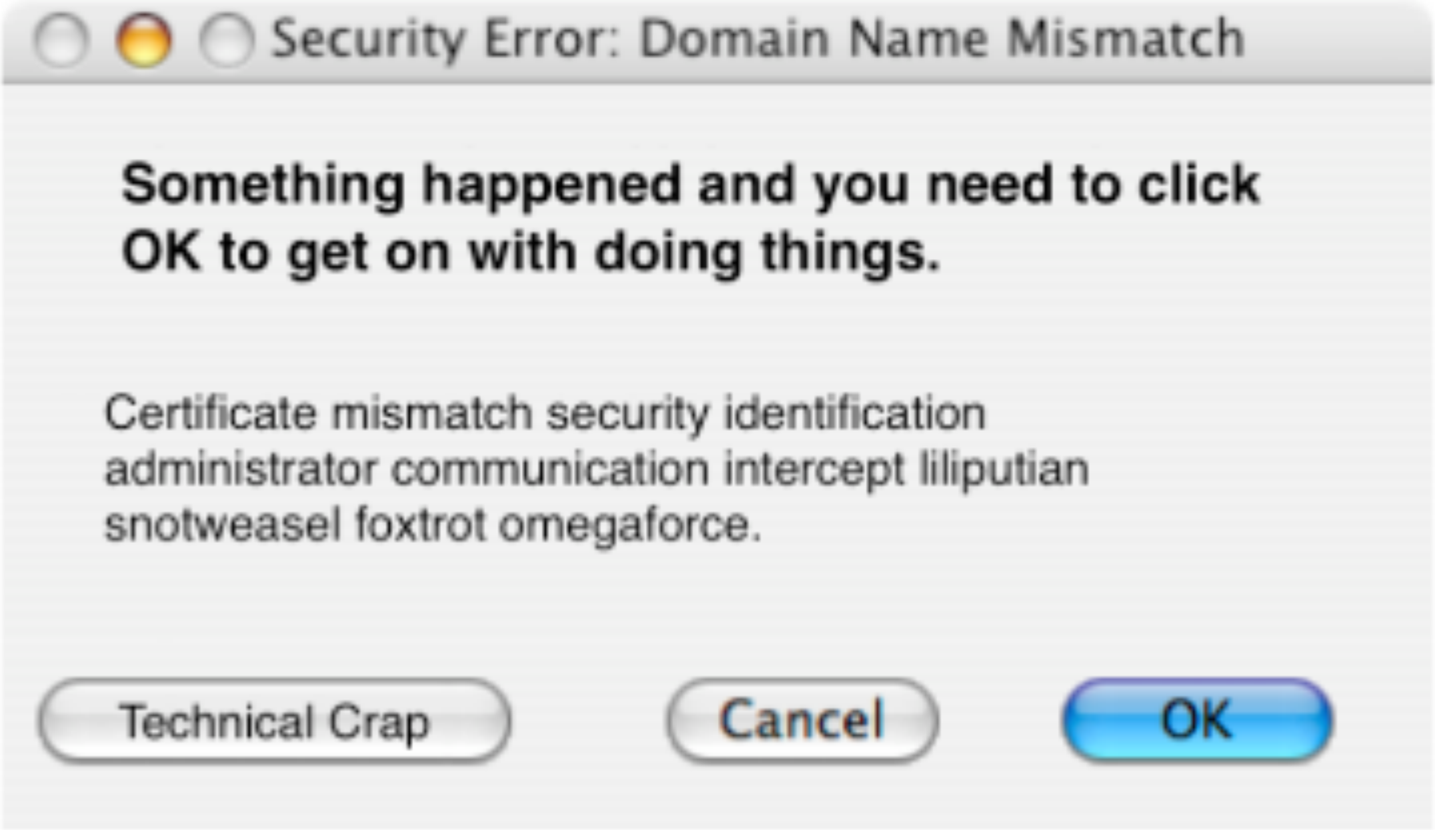
Privacy policy ***does not match*** user's privacy preferences

OPERATOR SPECIALTY COMPANY, INC.
Moving Gate Can Cause
Serious Injury or Death
ARNING
AUTOS ONLY
NO PEDESTRIANS
NO MOTORCYCLES
NO BICYCLES
KEEP AWAY FROM GATE ARM
MOVING GATE ARM CAN CAUSE
SERIOUS INJURY OR VEHICLE DAMAGE
OSCO



浴衣・スリッパのままで、客室フロア（廊下）以外へ
お出になることは、非常時を除き、
ご遠慮ください。

Warnings



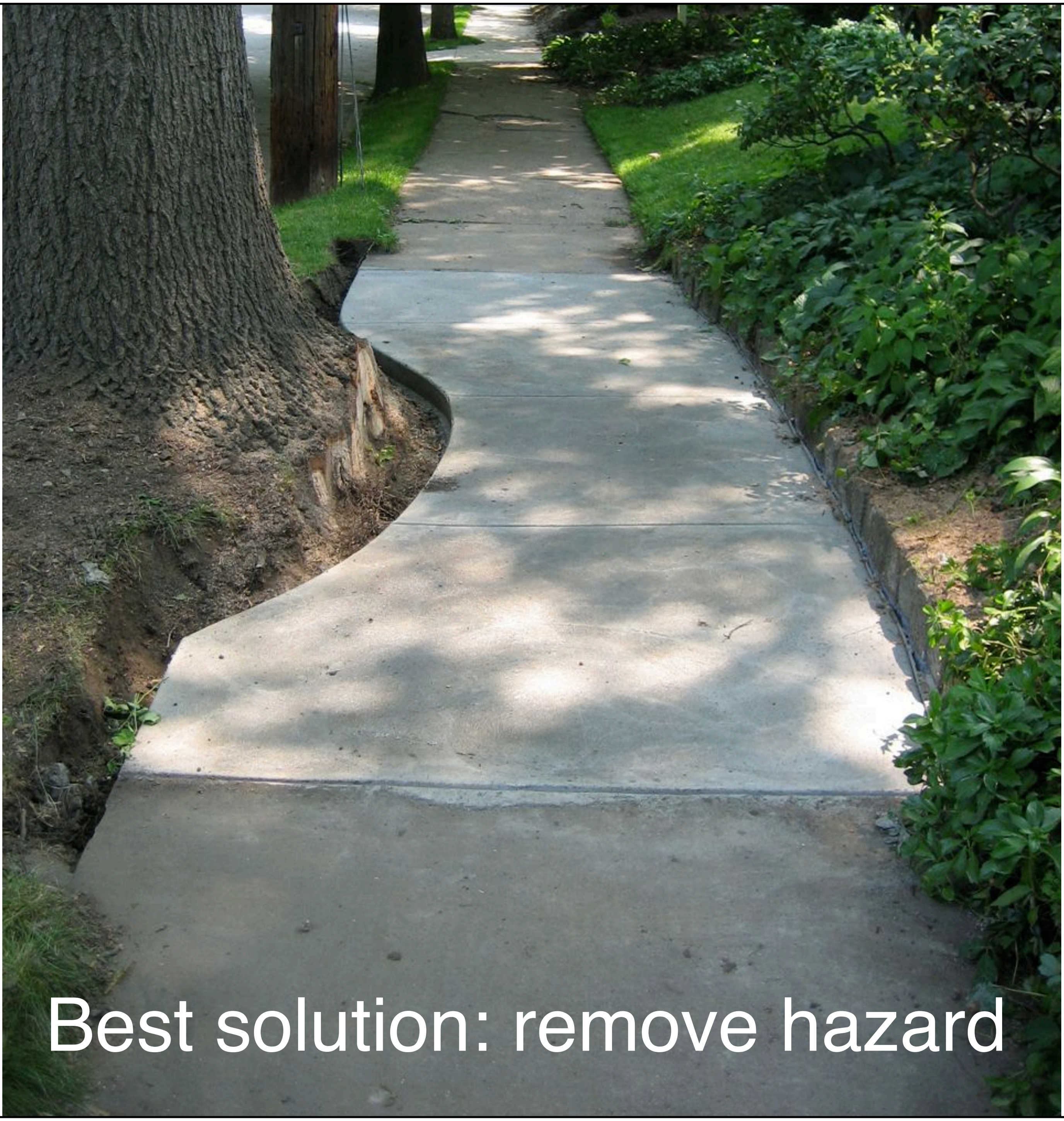
Security Error: Domain Name Mismatch

Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegaforce.

Image courtesy of Johnathan Nightingale

What to do about hazards?

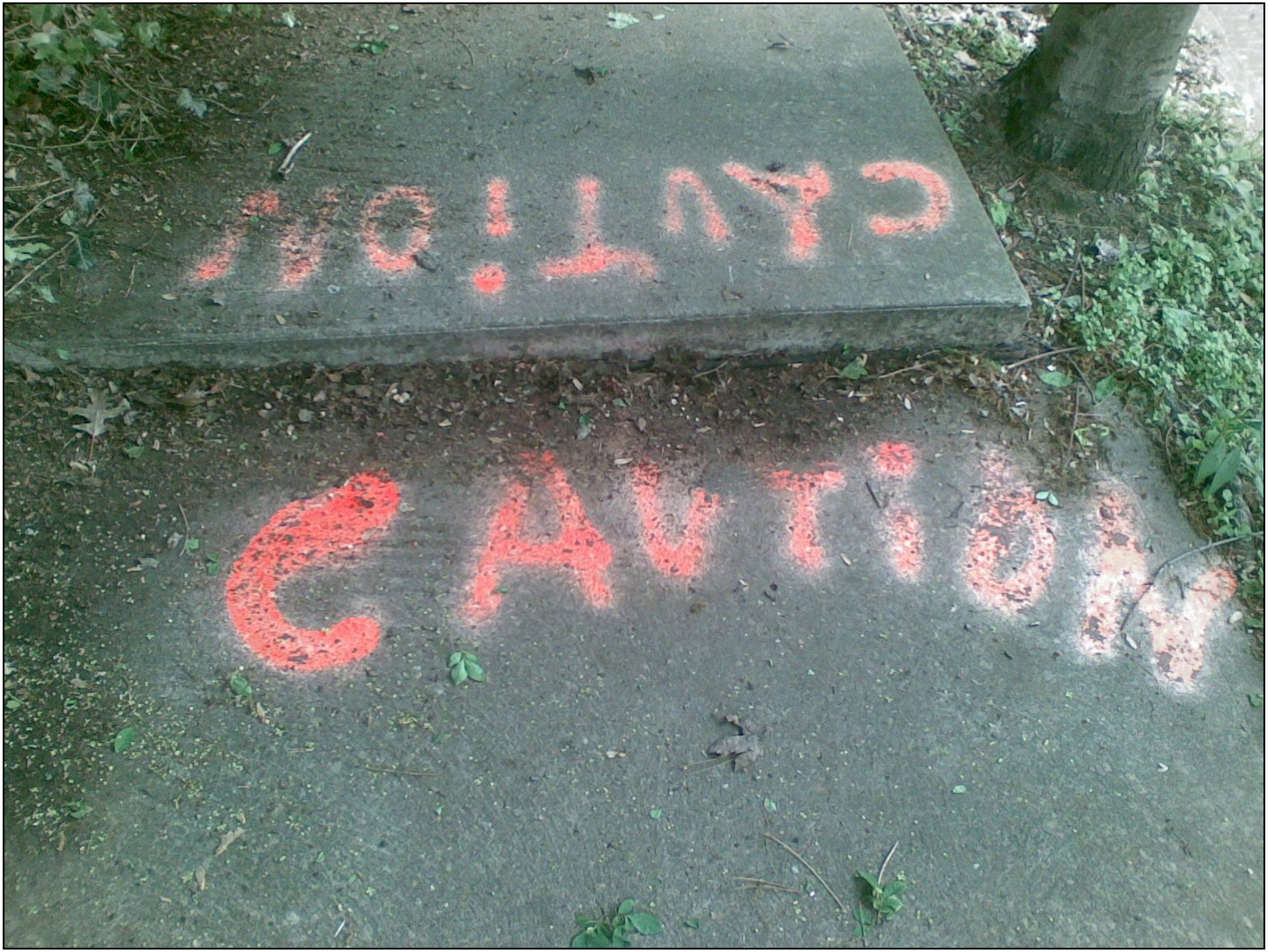


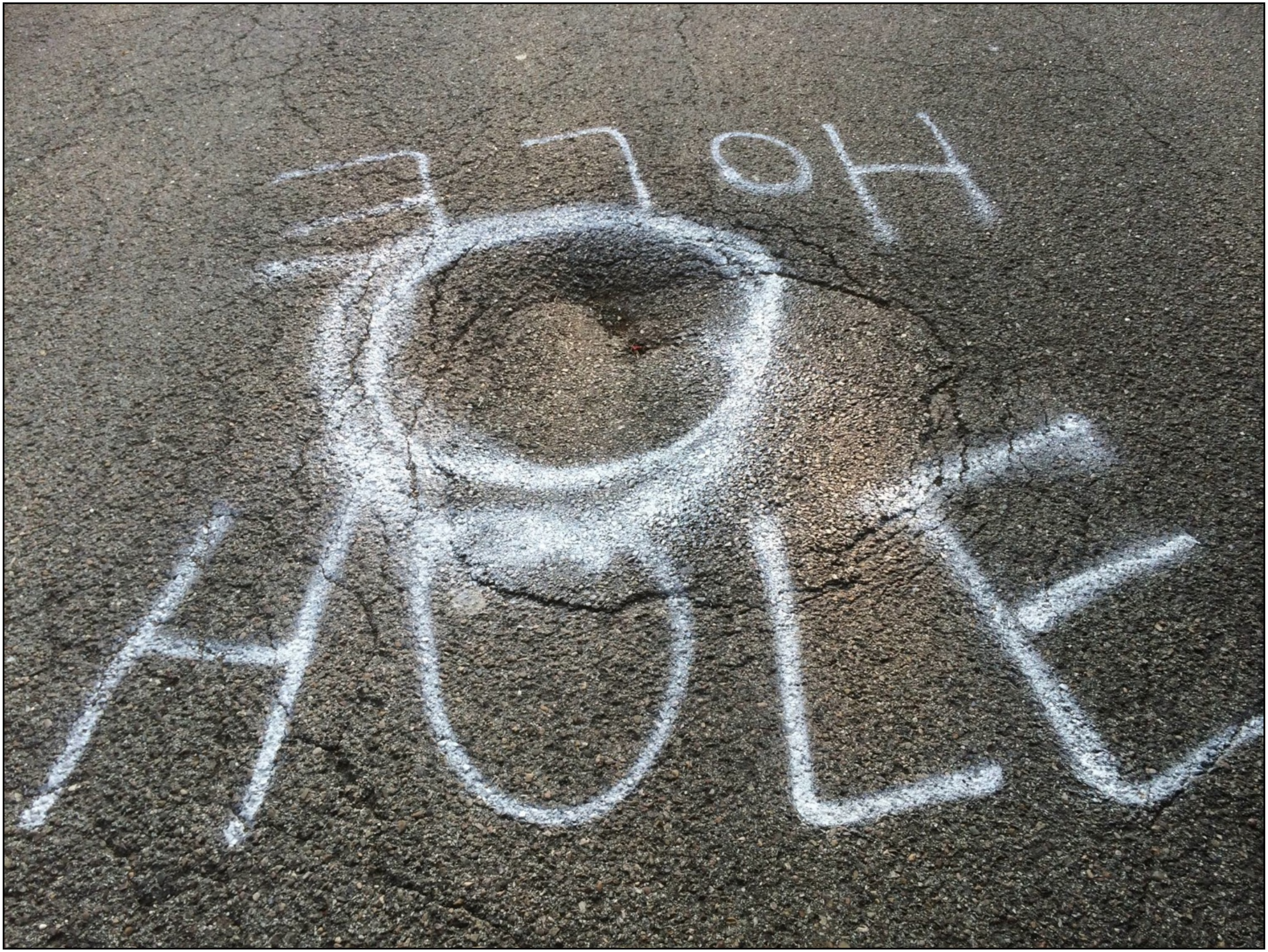
Best solution: remove hazard

Next best: guard against hazard

HOLE

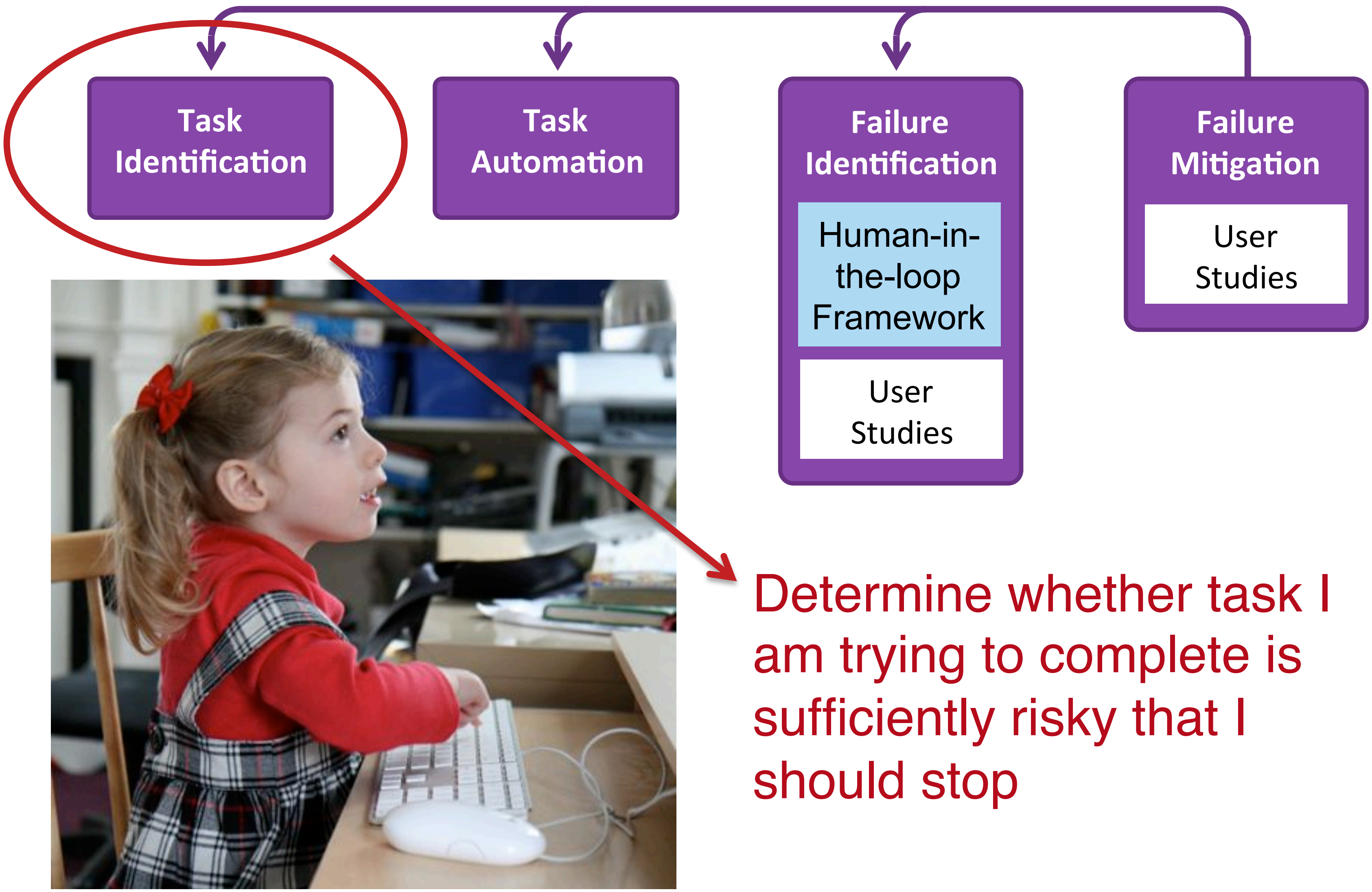
If all else fails: warn


CAUTION
CAUTION


HOLE
HOLE

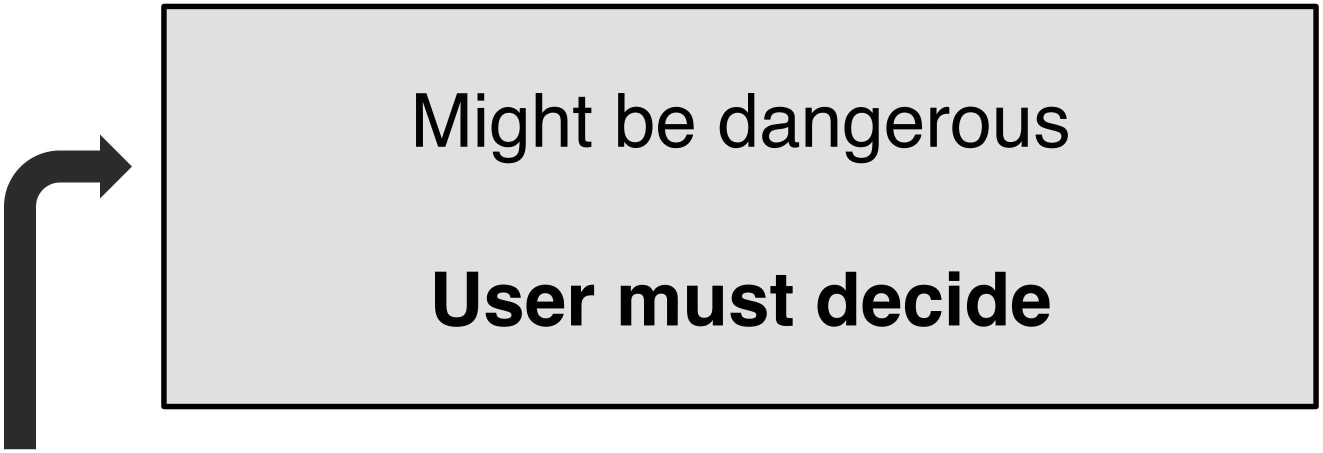
CAUTION ⚠ UNEVEN SURFACES

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

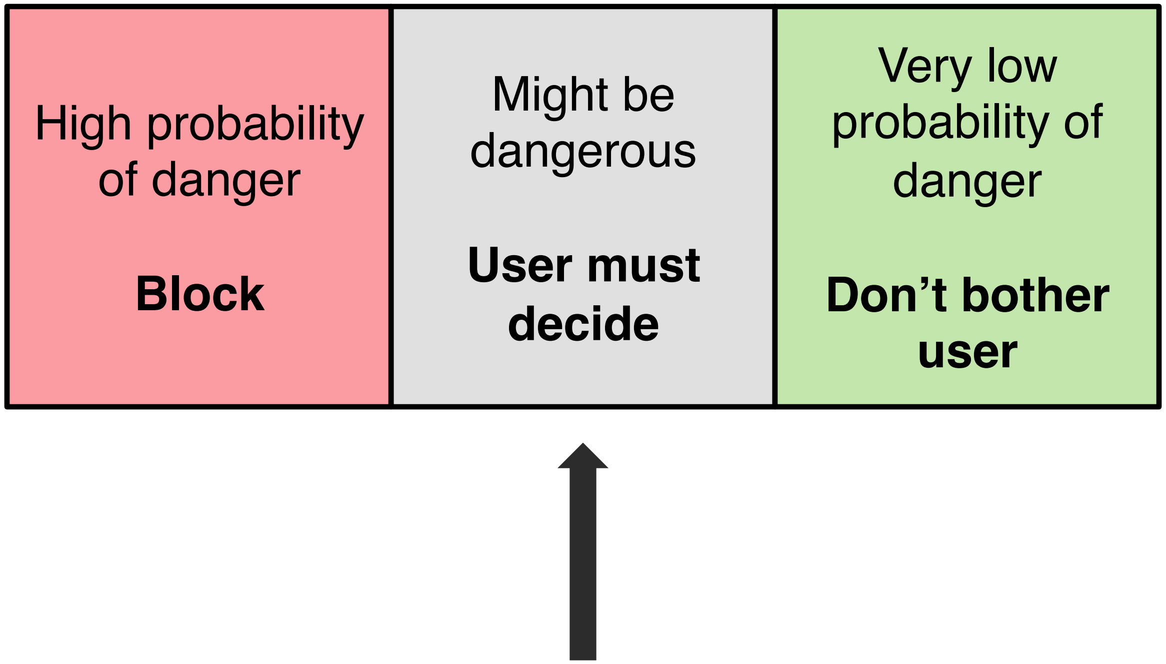


Might be dangerous

User must decide

Use automated
analysis to determine
probability of danger

Support user decision



High probability of danger

Block

Might be dangerous

User must decide

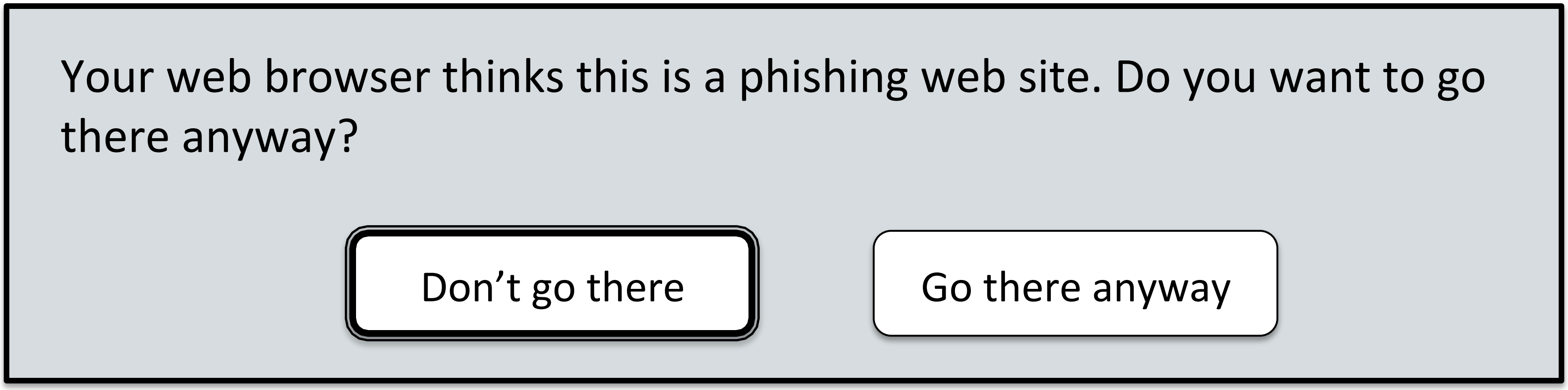
Very low probability of danger

Don’t bother user

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?

I don’t know what a phishing site is.

I really want to go to this site.

Of course I will go there anyway!

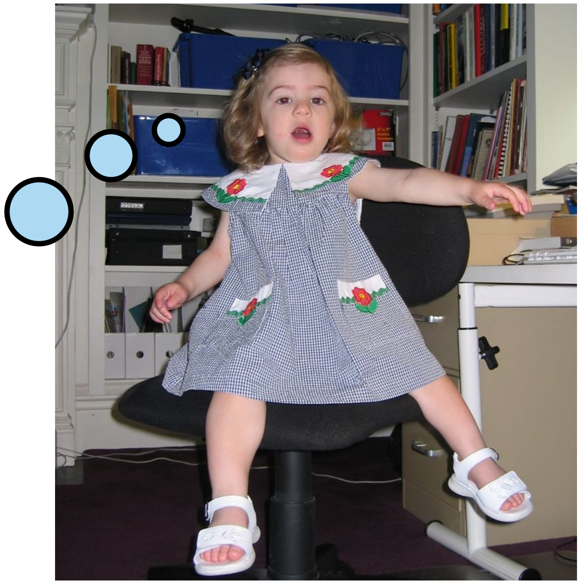
Better question

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!



Usable privacy and security studies 101

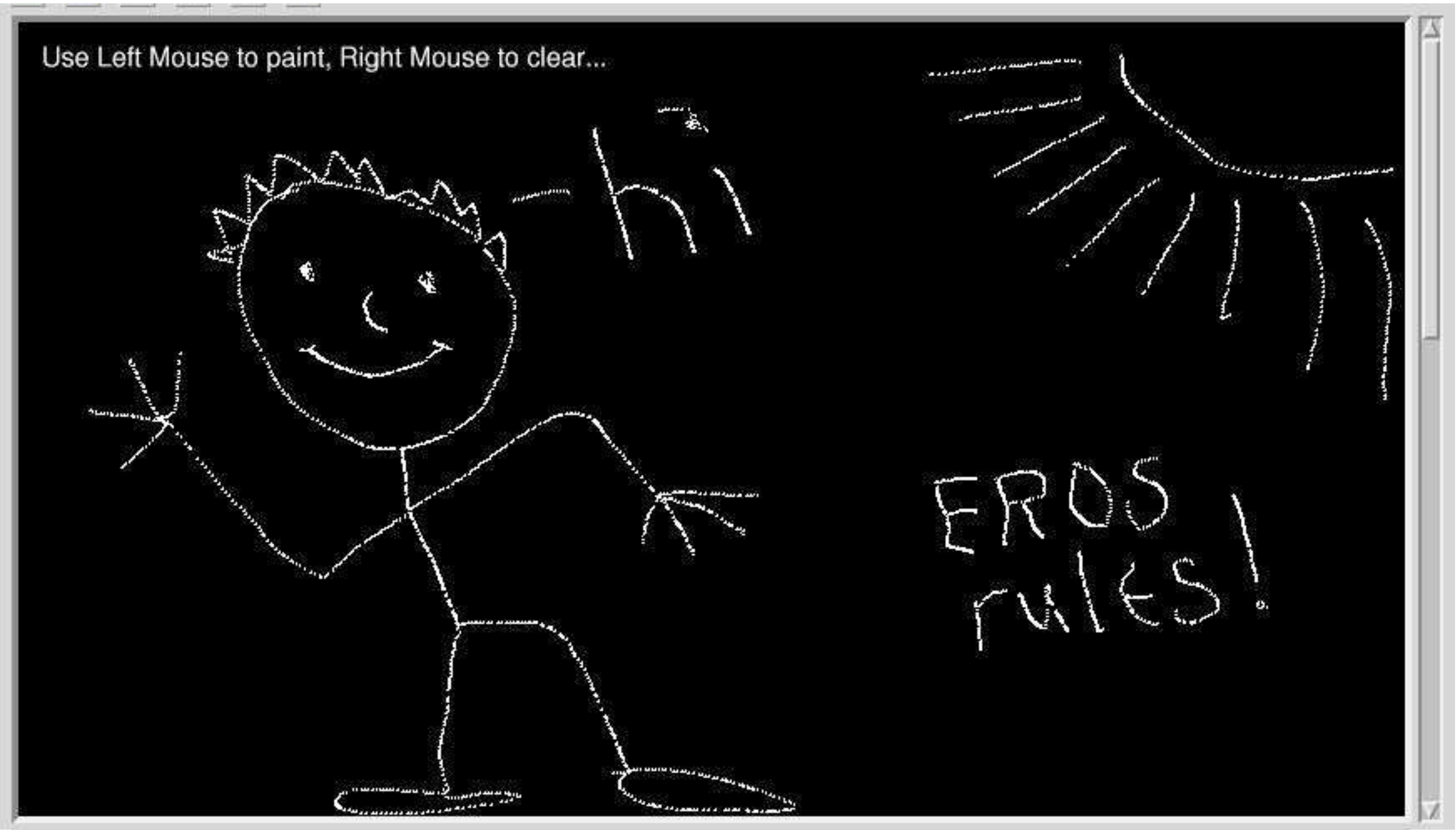
Why do usable privacy and security studies?

Purpose	Useful to…
Assess needs	Decide what to build
Evaluate	Determine whether system meets requirements and what needs to be improved
Understand tradeoffs	Decide which features/approaches/systems best fit particular needs
Find root causes	Determine where redesigns or new approaches are needed

Excuses for not doing usability studies

- If people weren’t so lazy/stupid/careless the system would work just fine
- I’m a cryptographer, not a usability expert
- I already know what people want
- No time, no money
- I find the system easy to use so it must be usable
- My kids can use the system so it definitely must be usable

Your kids are not typical users



Use Left Mouse to paint, Right Mouse to clear...

J. Shaprio, J. Vanderburgh, E. Northrup, D. Chizmadia. **Design of the EROS Trusted Window System.** USENIX Security 2004.

User study steps

- Identify research questions, metrics, and use cases
- Decide on type of study and design study protocol
- Develop detailed scripts, surveys, scenarios, incentives, instrumentation, prototypes, recruiting materials, etc.
- Obtain ethics approval
- Pilot and iterate on study design
- Collect data
- Analyze Results
- Repeat some or all of these steps as needed

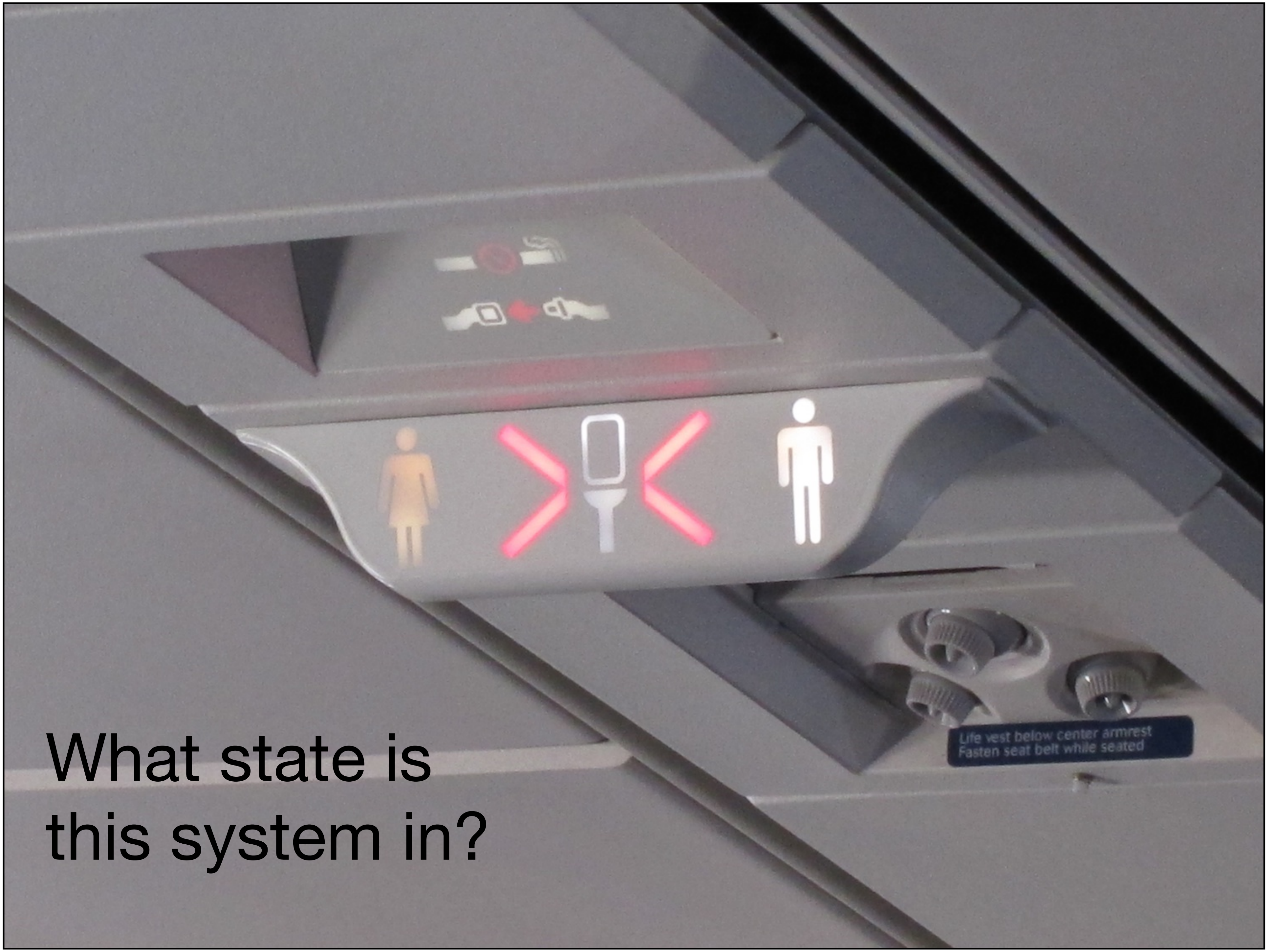
Usable security study challenges

- Keeping it real (ecological validity)
  - Create realistic sense of risk (but not real risk)
  - Provide realistic incentives
  - Don’t bias participants
- Measuring the right thing
  - Design the right protocol
  - Control the variables
  - Instrument
- Observing infrequent events and small differences
- Legal, ethical, and practical issues

Everyday usability

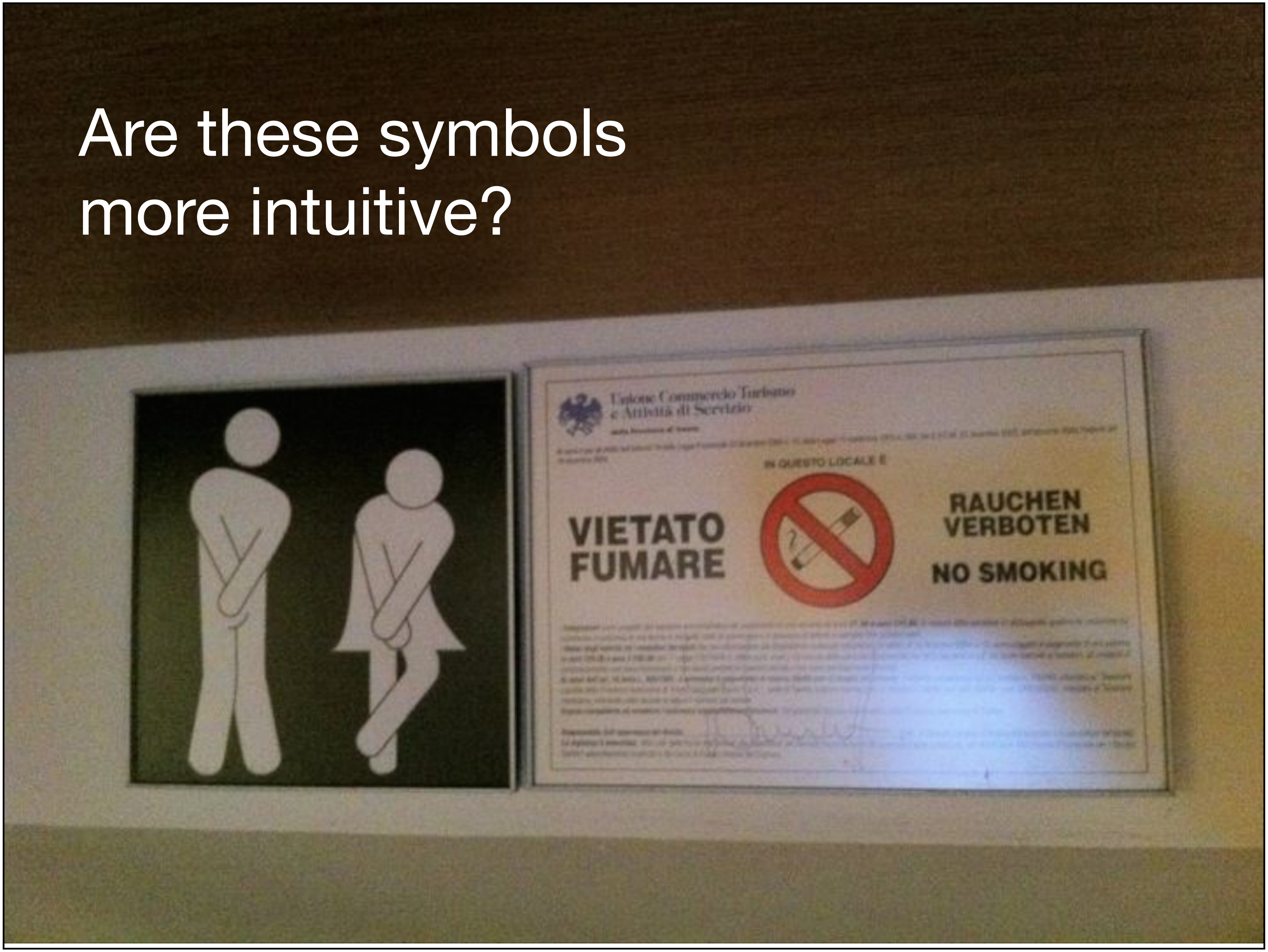
Lessons from the loo

Icons

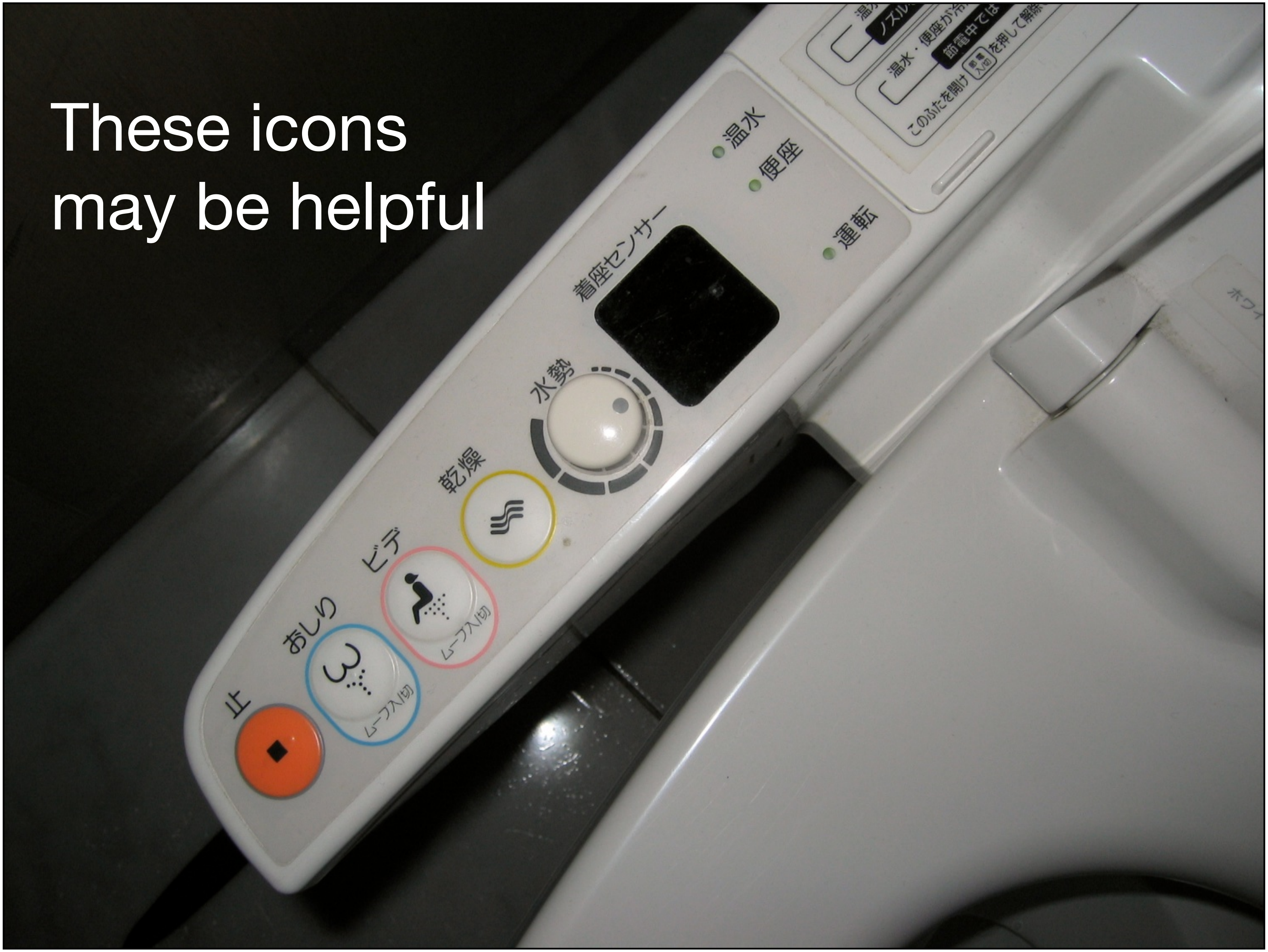


What state is this system in?

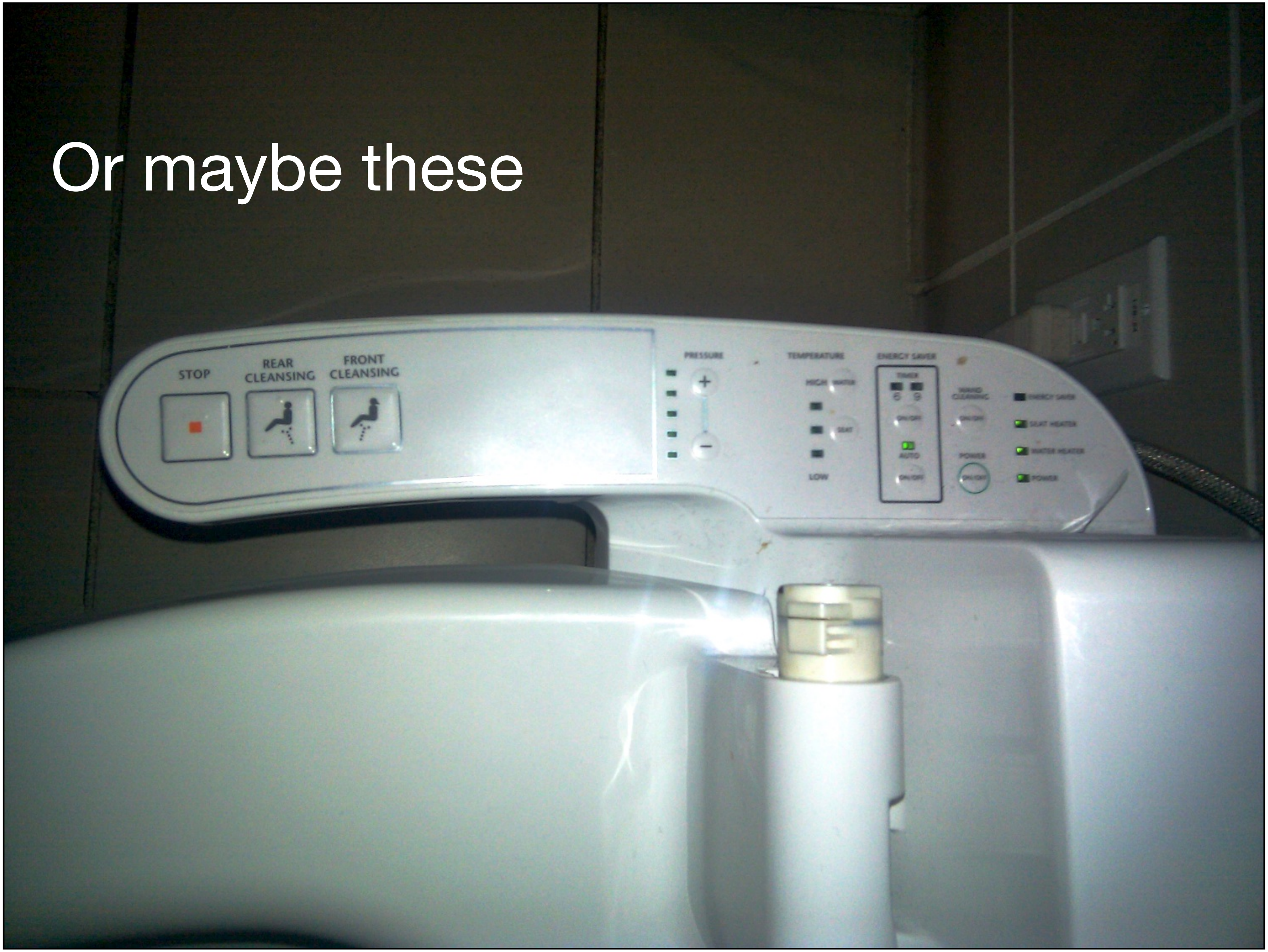
Are these symbols more intuitive?



These icons
may be helpful

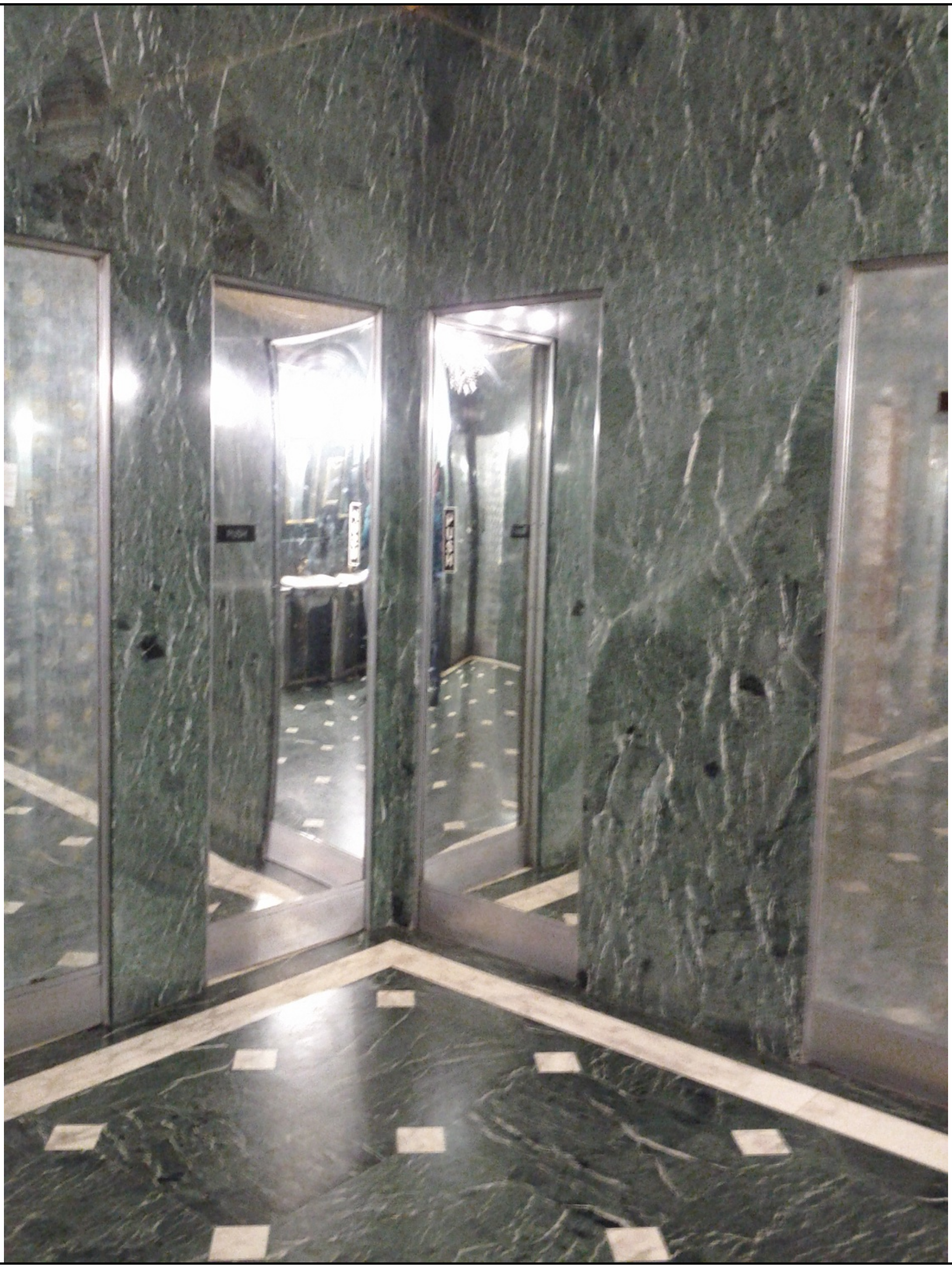


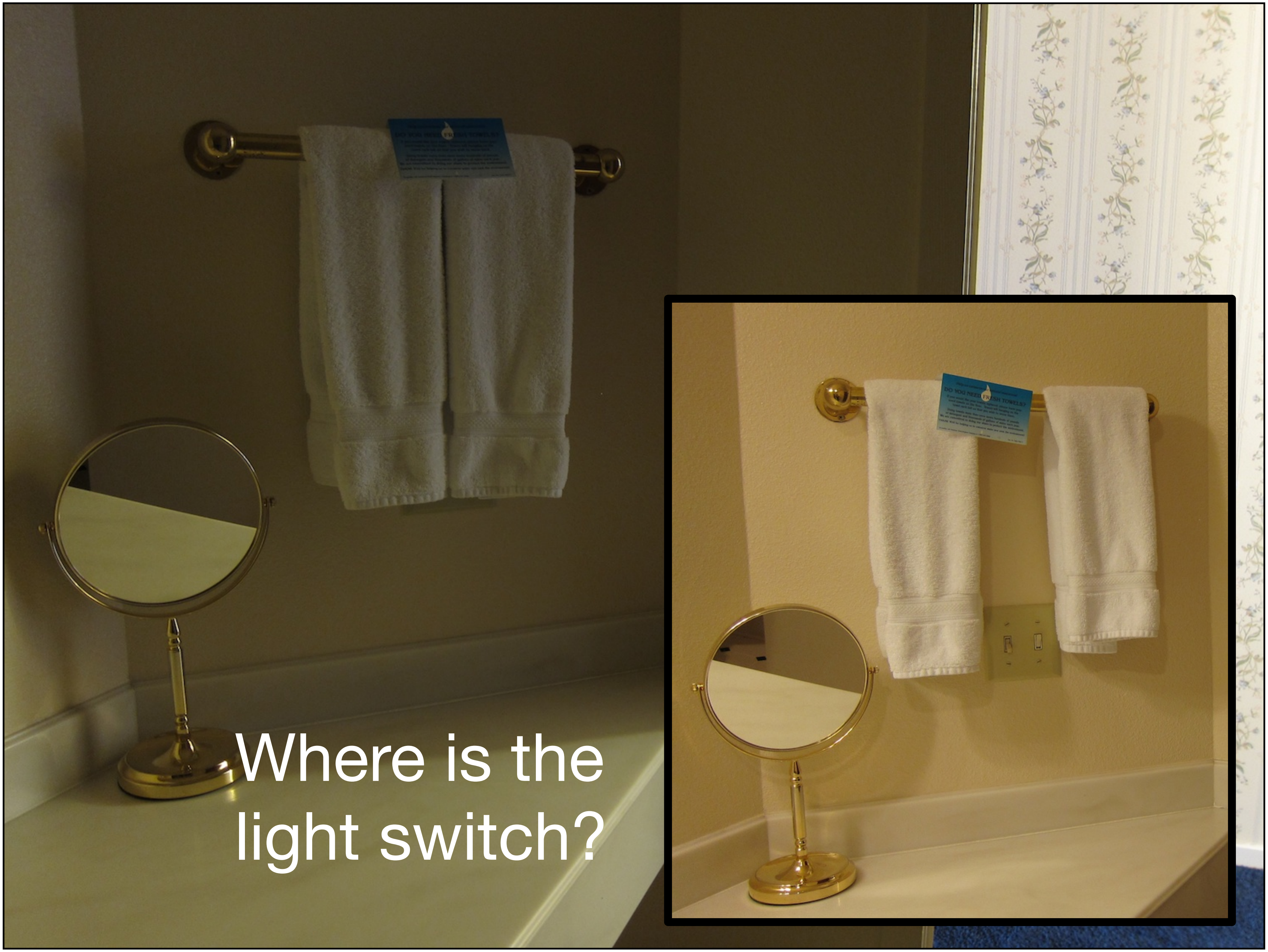
Or maybe these



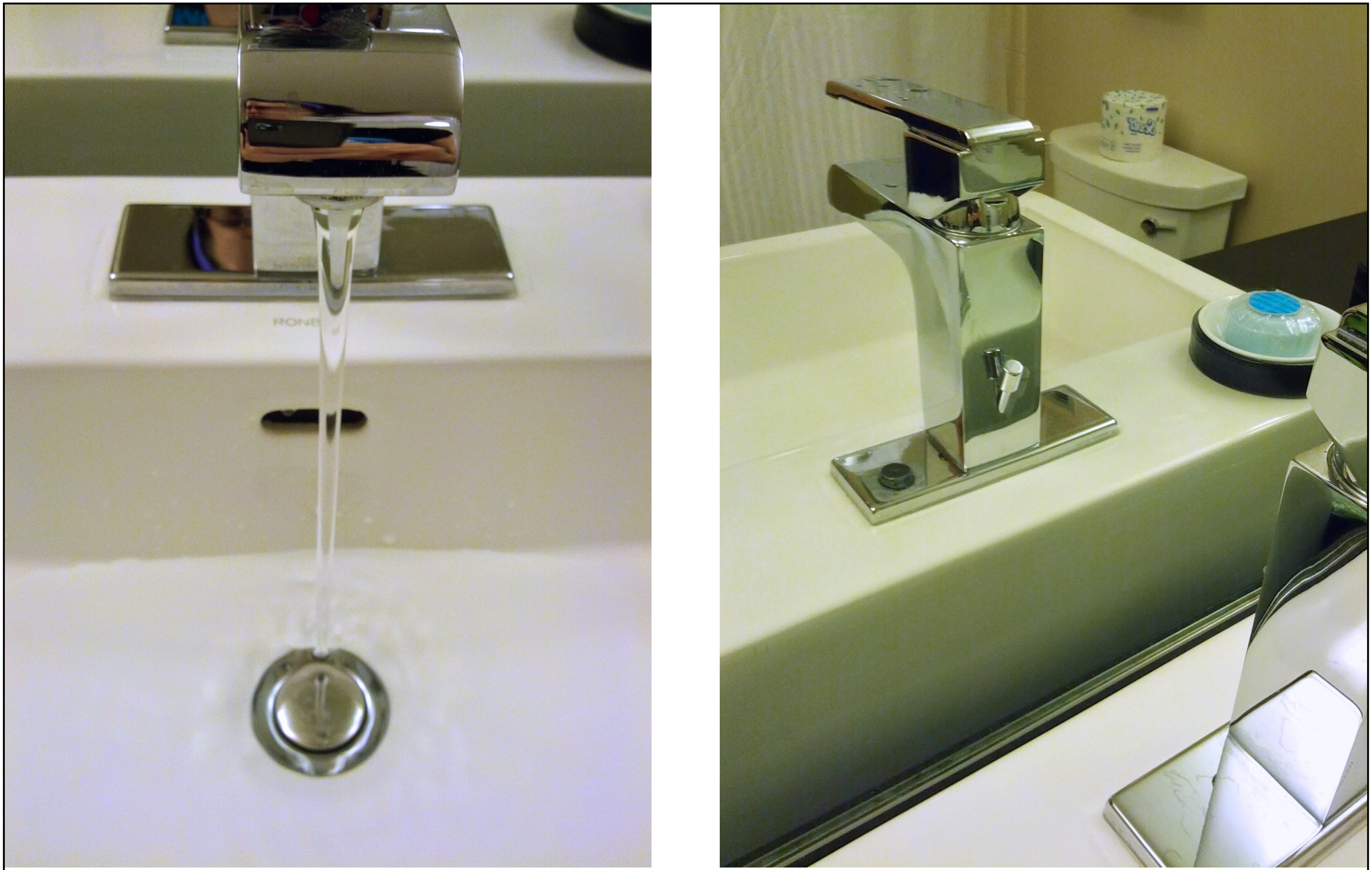
Hidden features

Where are the doors?

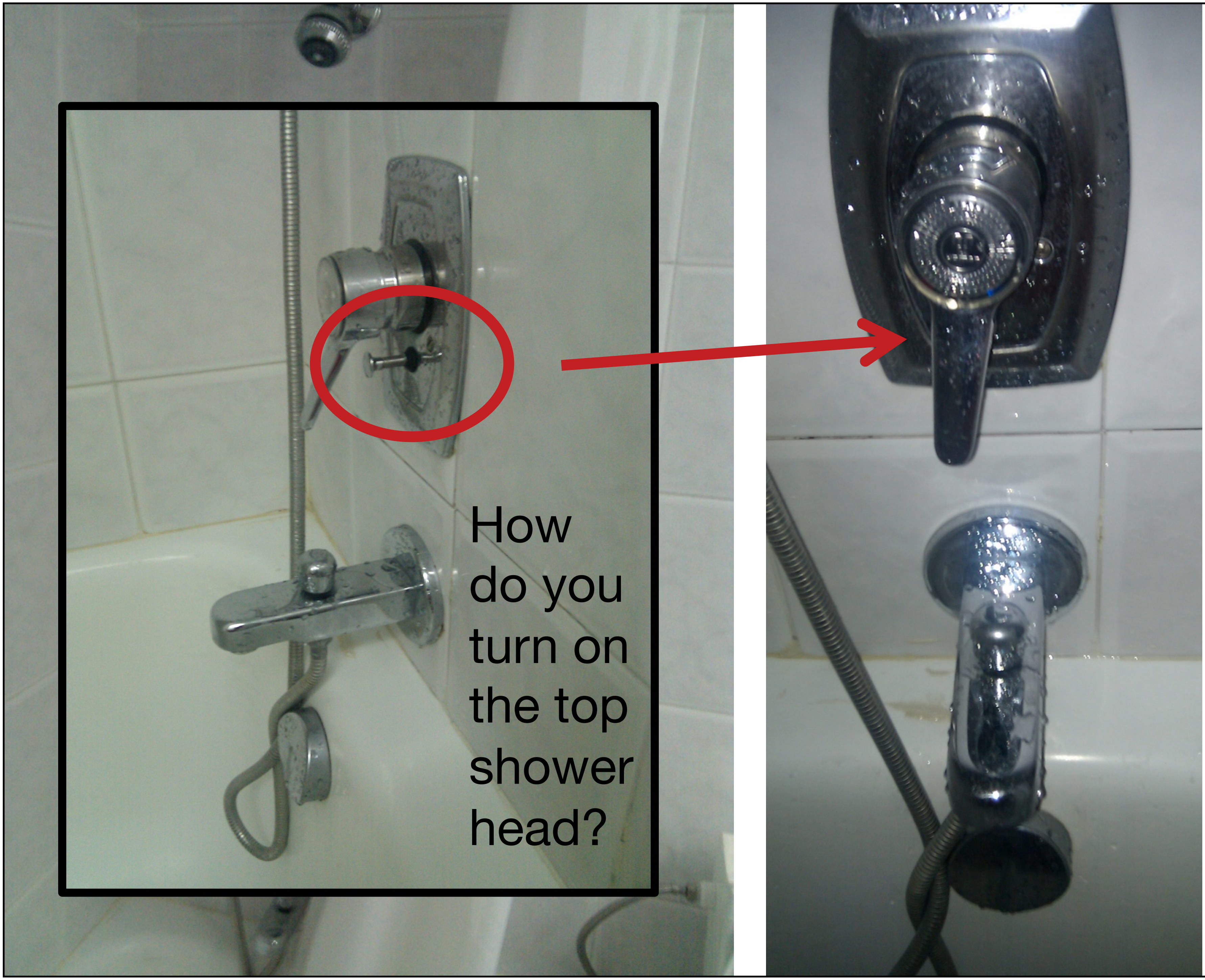




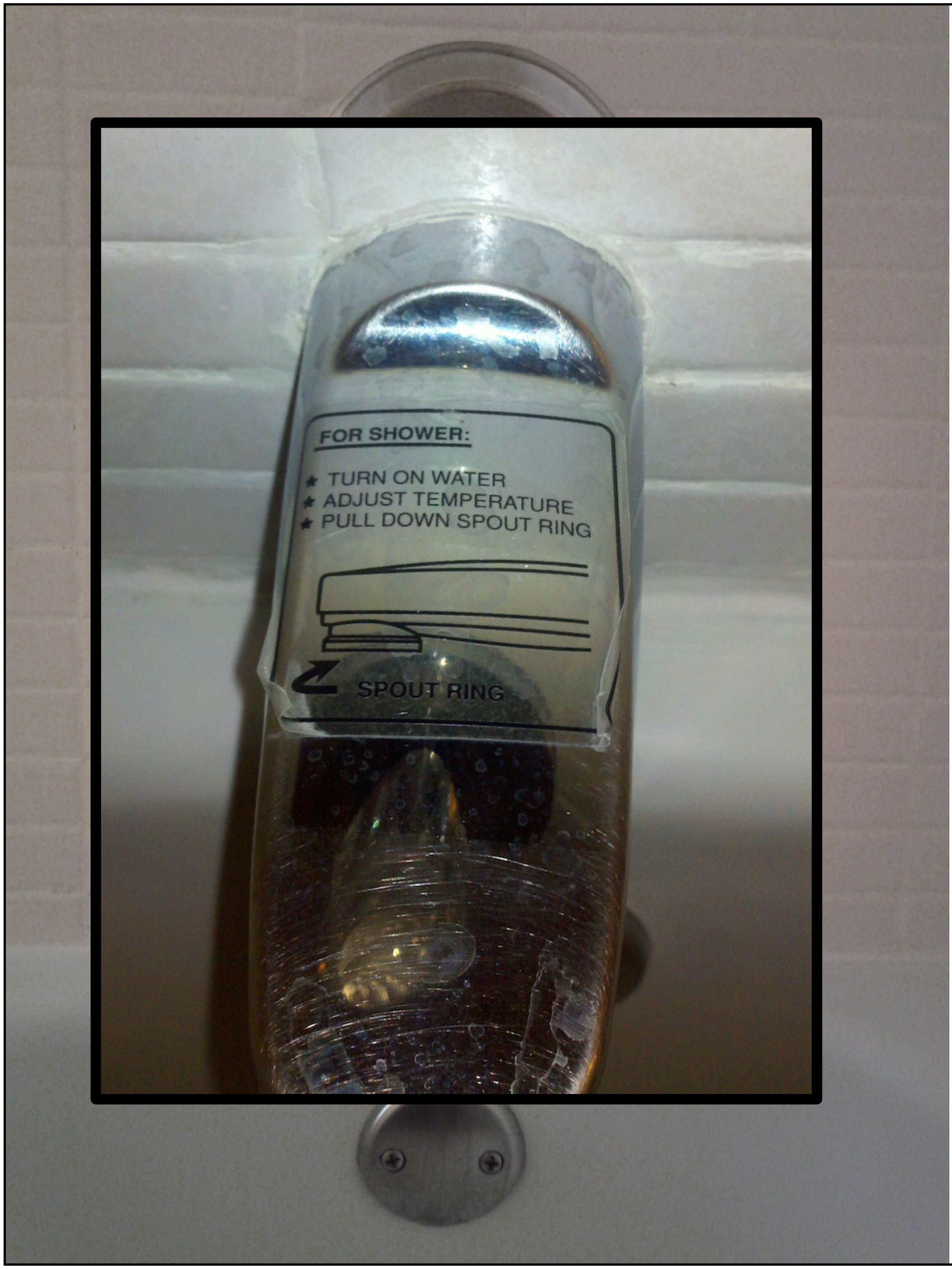
Where is the light switch?



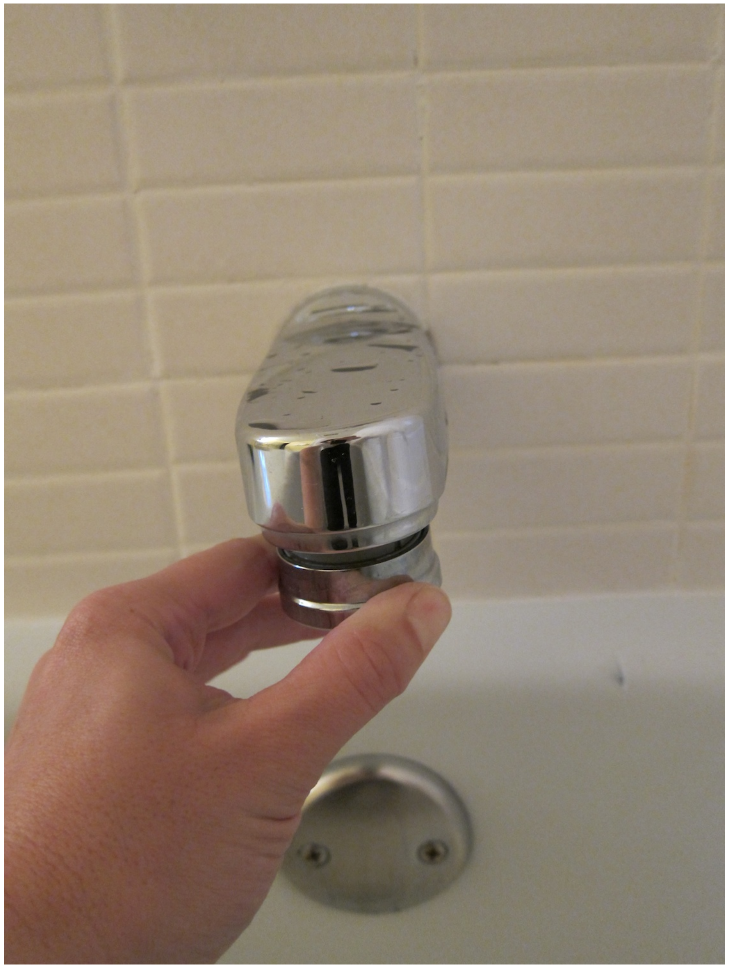
How do you unplug the sink?

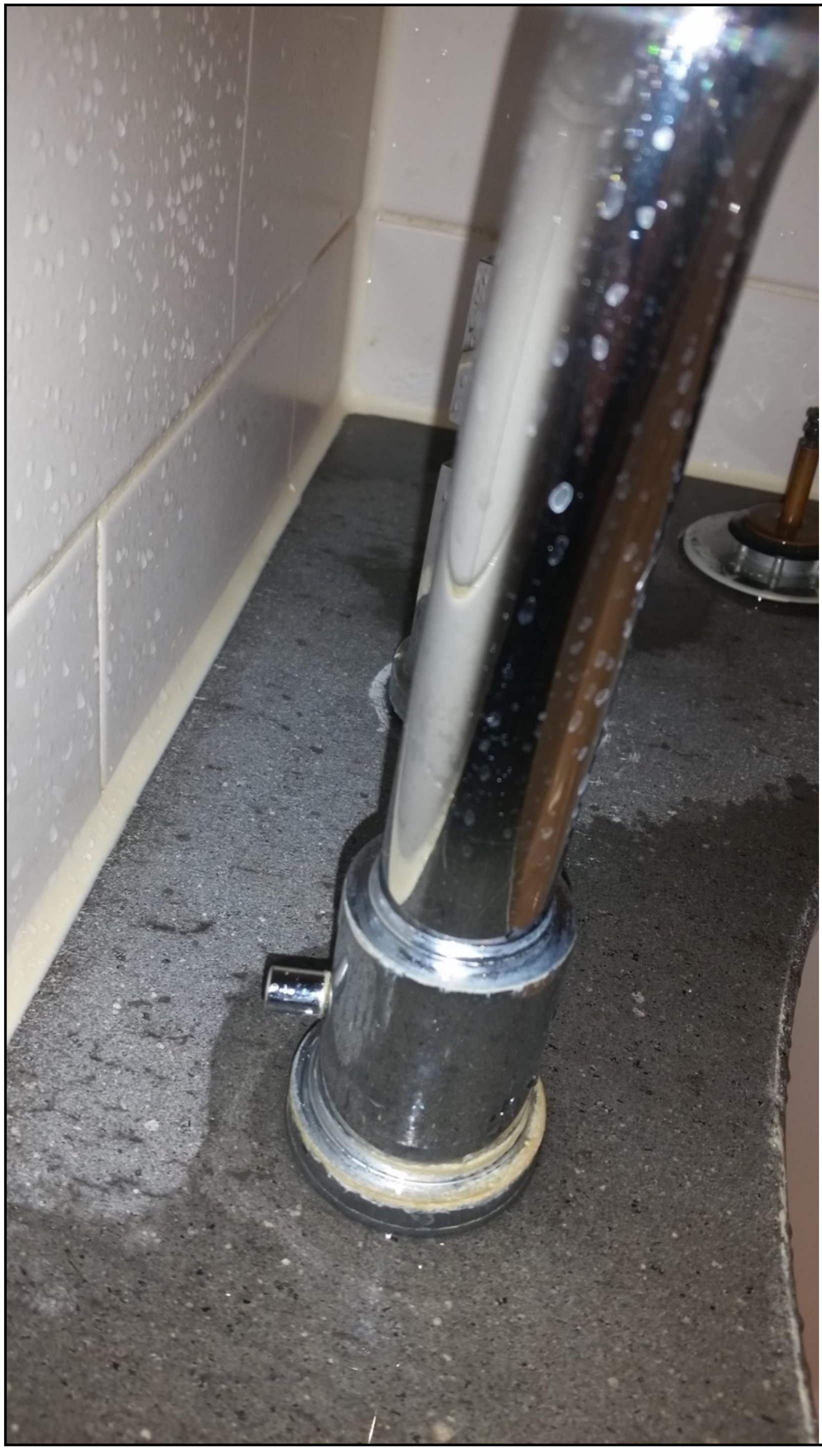


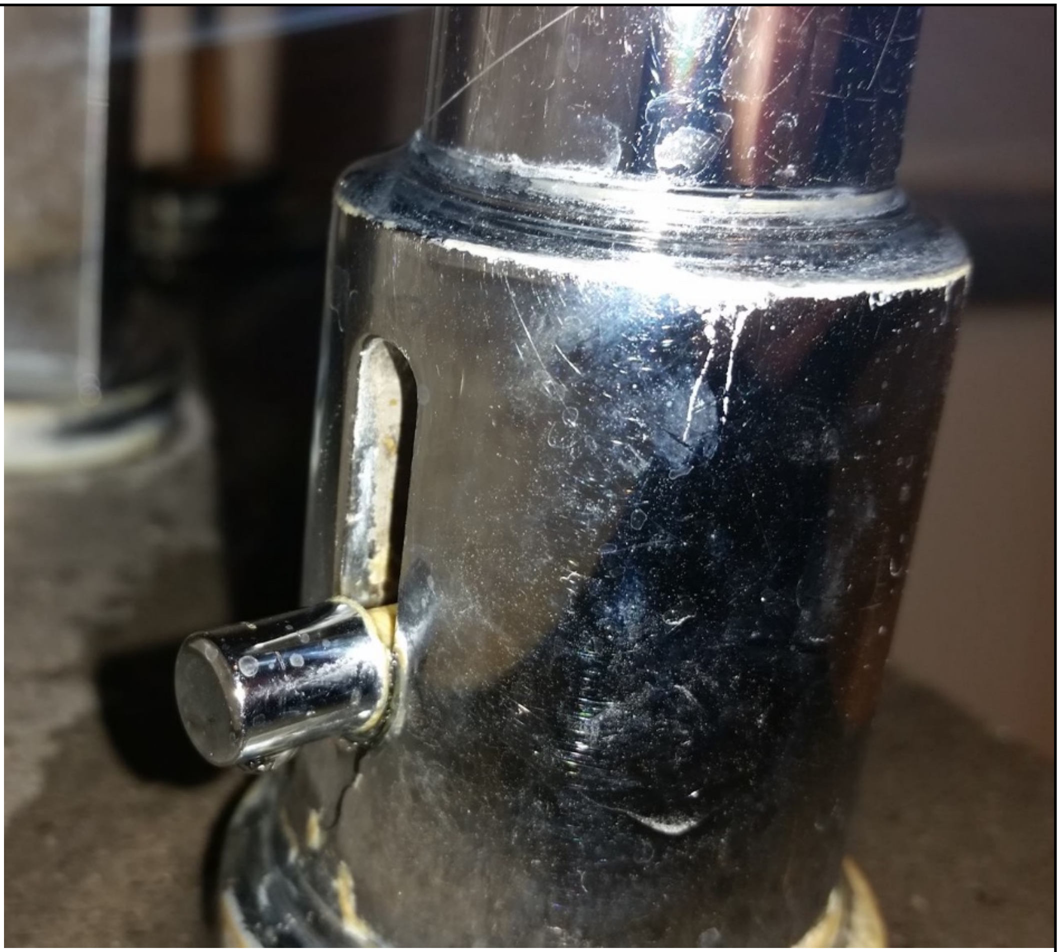
How do you turn on the top shower head?



How do you turn on this shower?



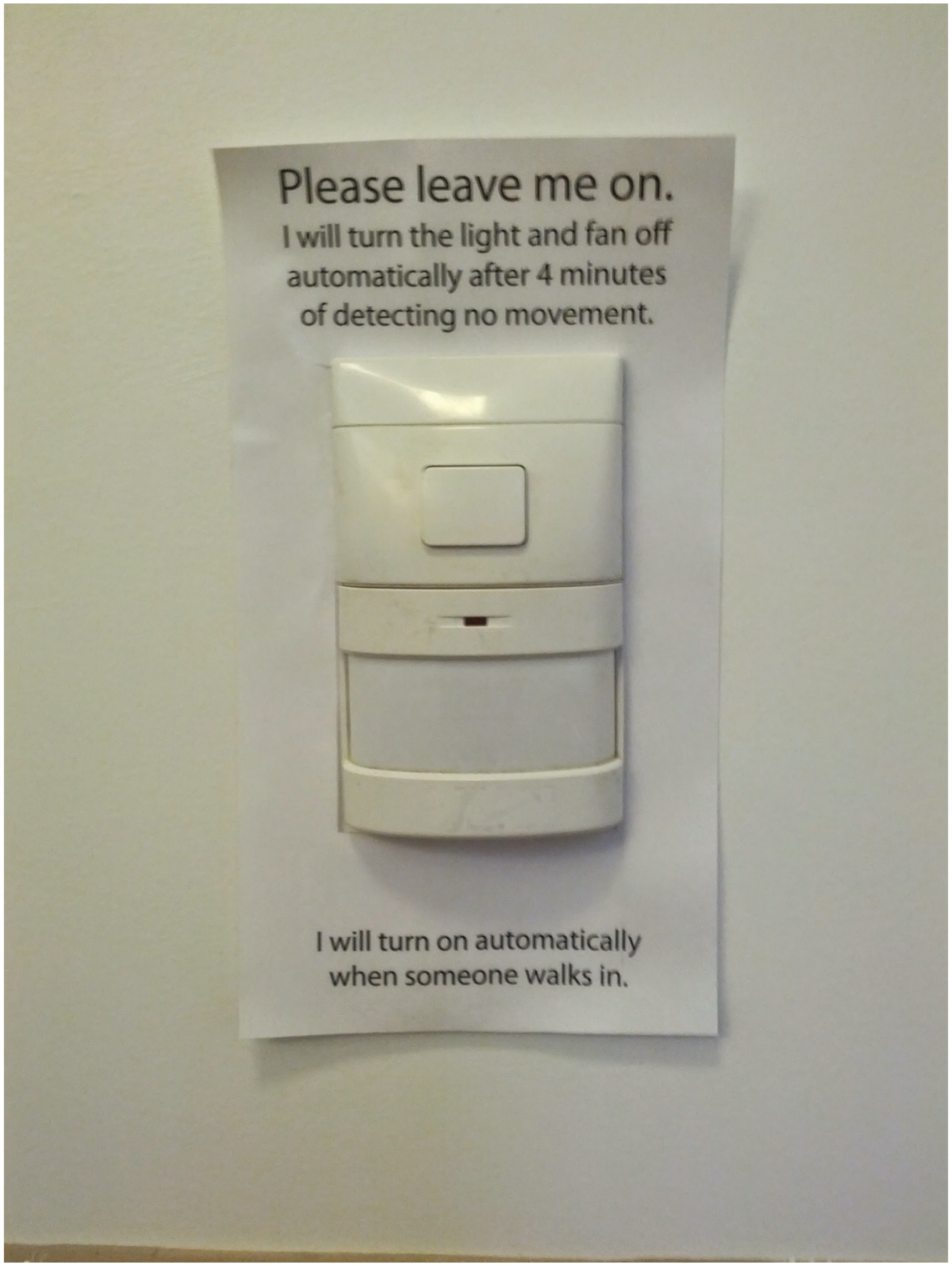




How do you turn on this shower?

More or less confusing features

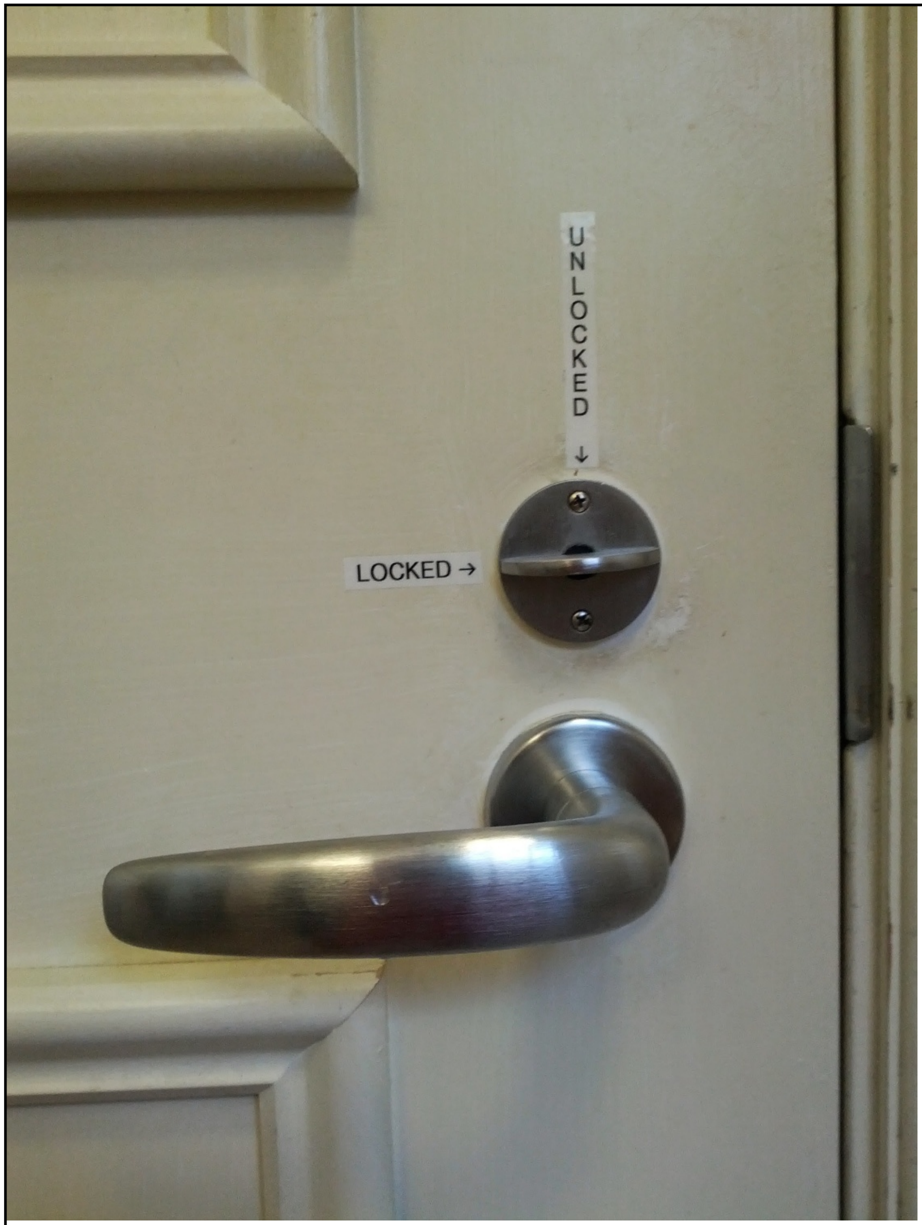
People were confused until they posted instructions



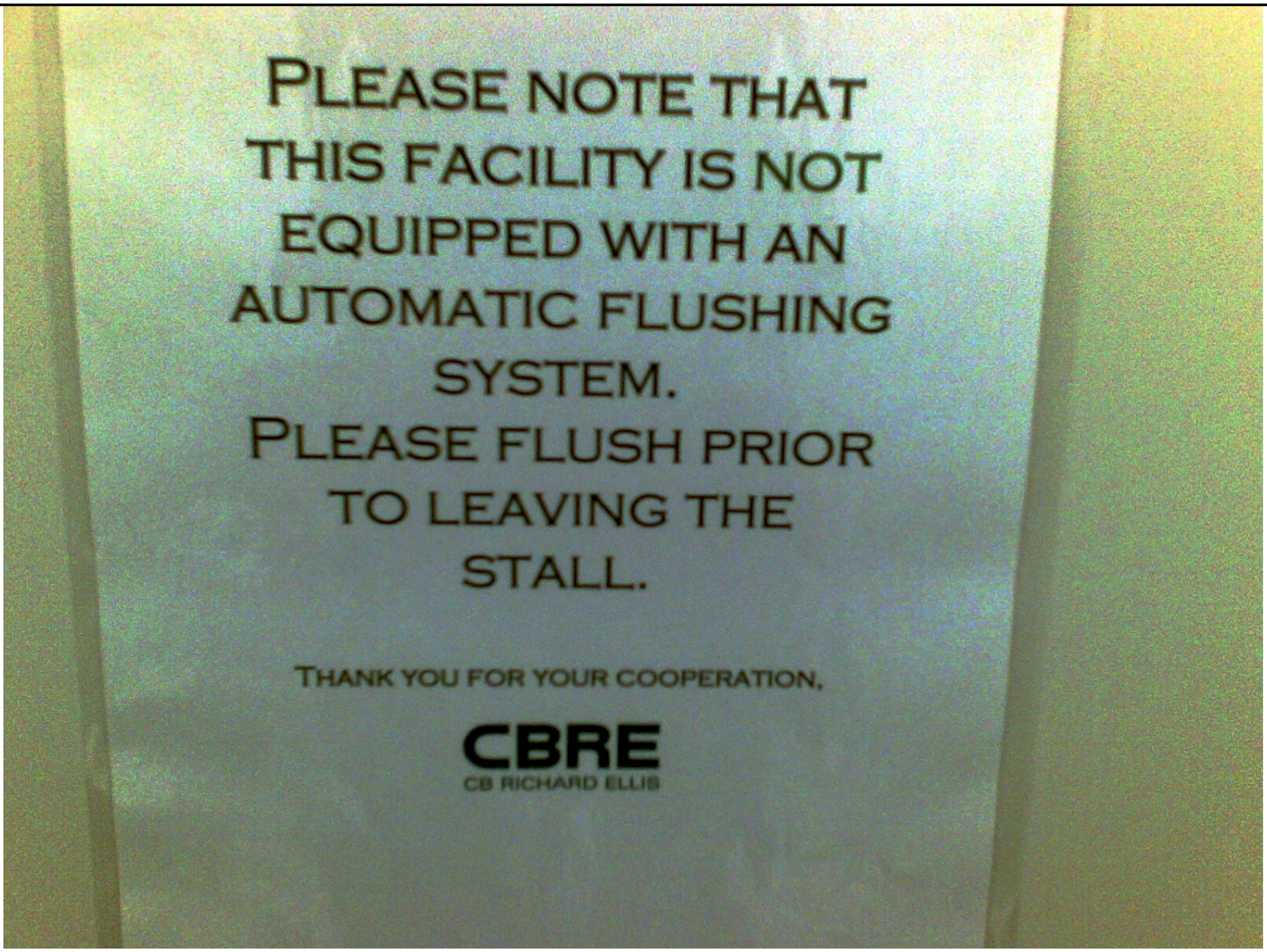
Please leave me on.

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.



This is at Harvard



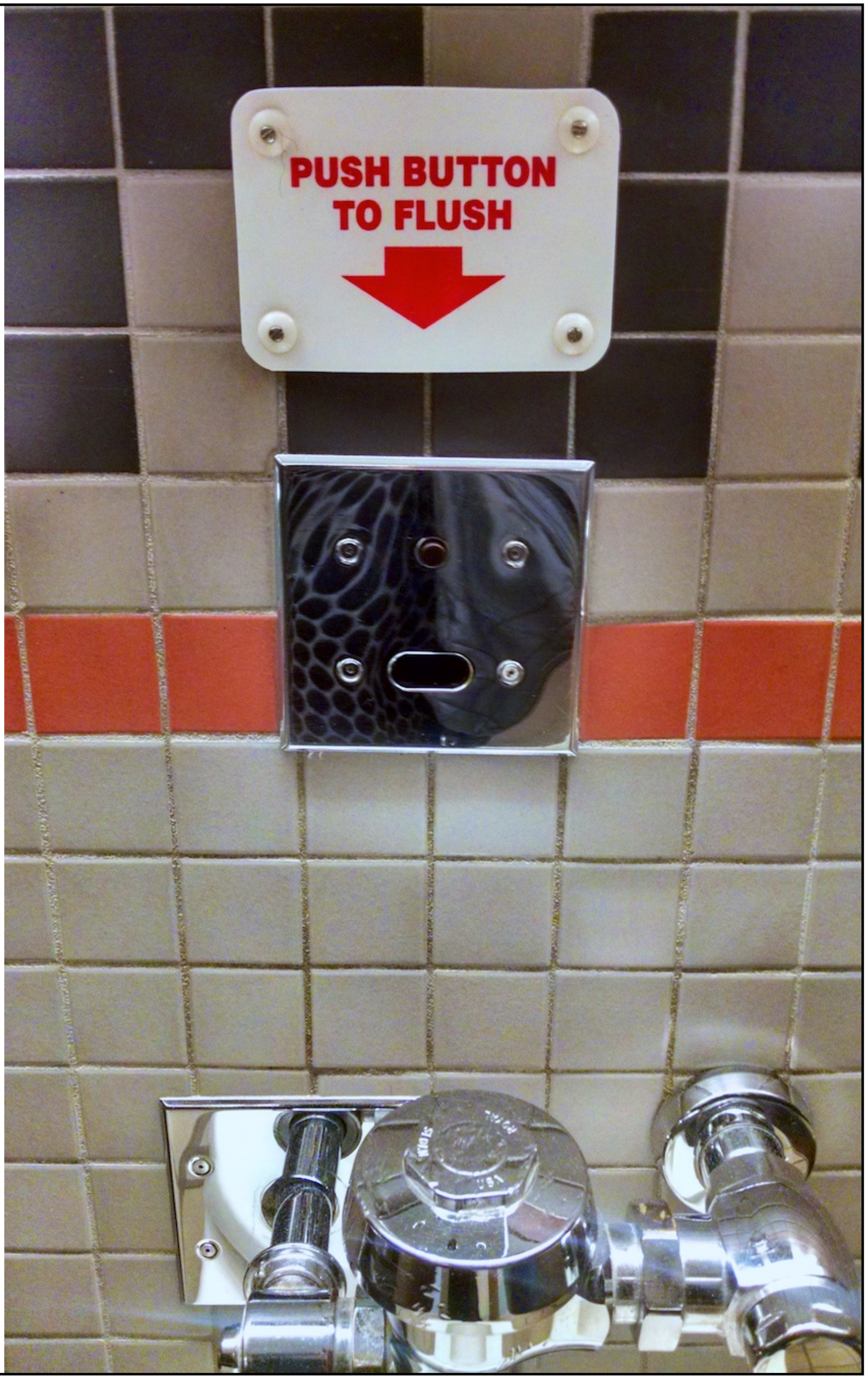
PLEASE NOTE THAT
THIS FACILITY IS NOT
EQUIPPED WITH AN
AUTOMATIC FLUSHING
SYSTEM.
PLEASE FLUSH PRIOR
TO LEAVING THE
STALL.

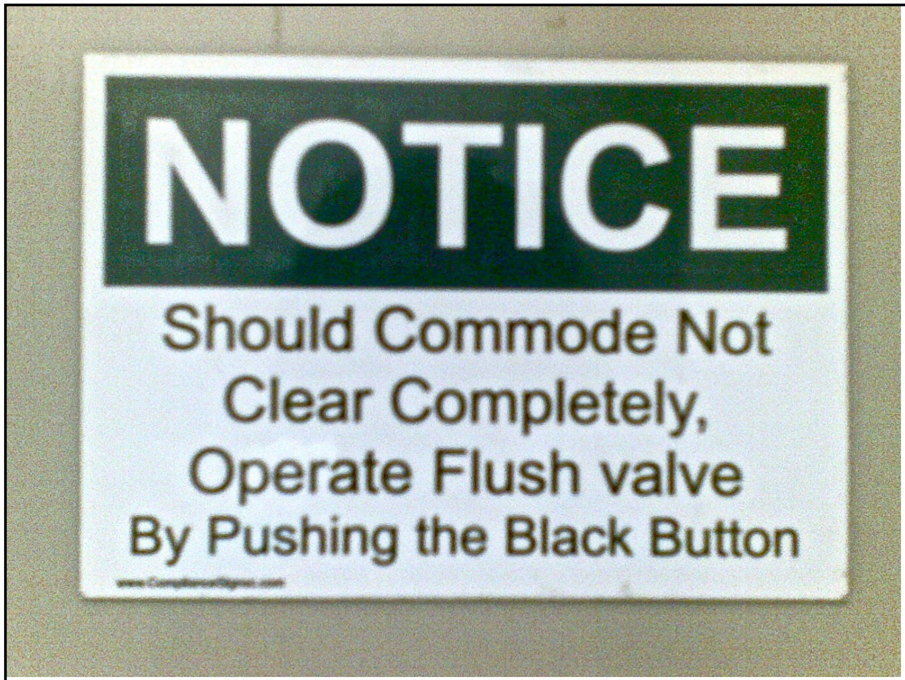
THANK YOU FOR YOUR COOPERATION,

CBRE
CB RICHARD ELLIS

People may become habituated to expect the system to work automatically

This one is supposed to work automatically

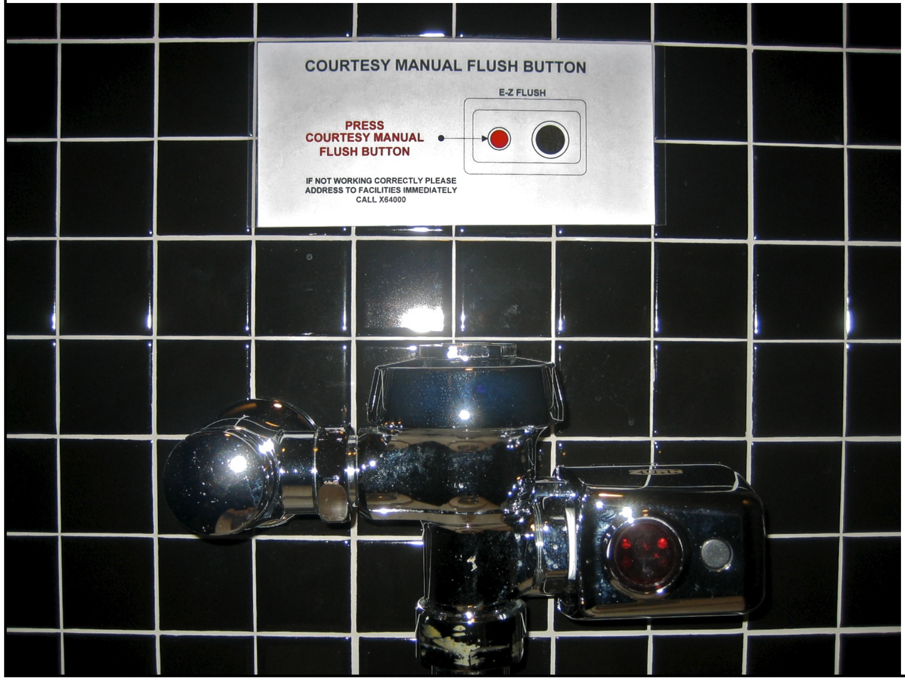




NOTICE

Should Commode Not Clear Completely, Operate Flush valve By Pushing the Black Button

www.ComplianceSigns.com

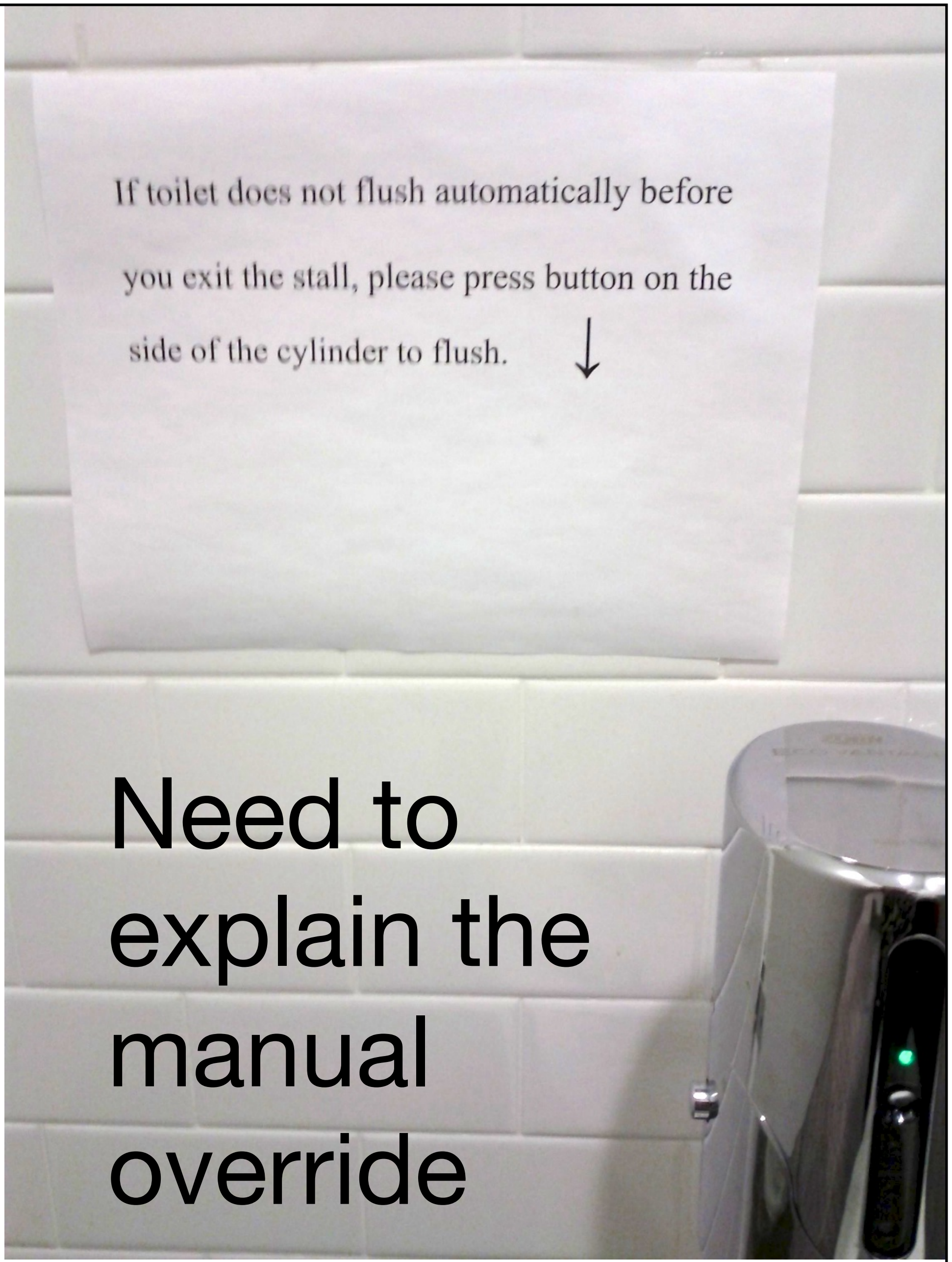


COURTESY MANUAL FLUSH BUTTON

E-Z FLUSH

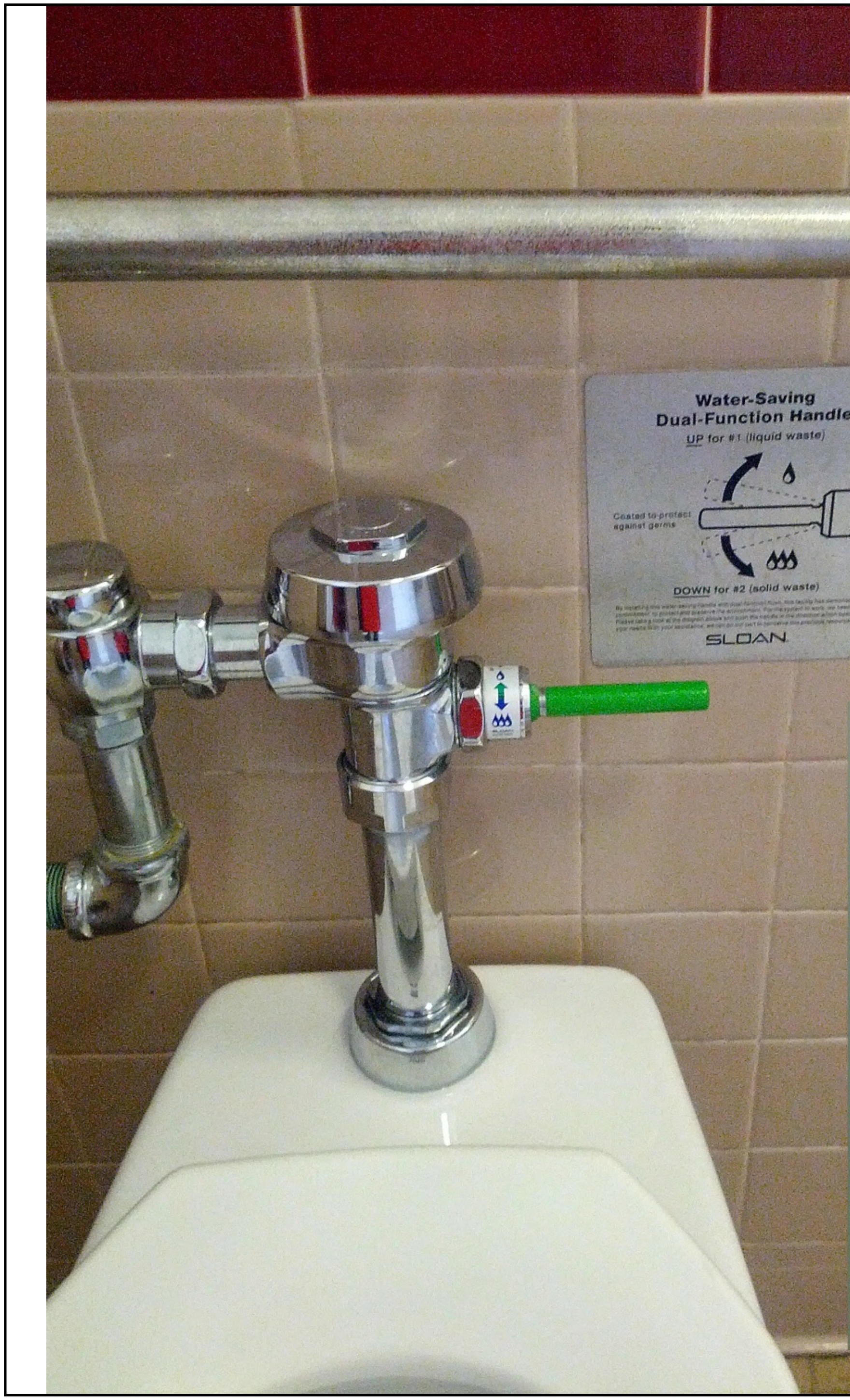
PRESS COURTESY MANUAL FLUSH BUTTON

IF NOT WORKING CORRECTLY PLEASE ADDRESS TO FACILITIES IMMEDIATELY CALL X64000

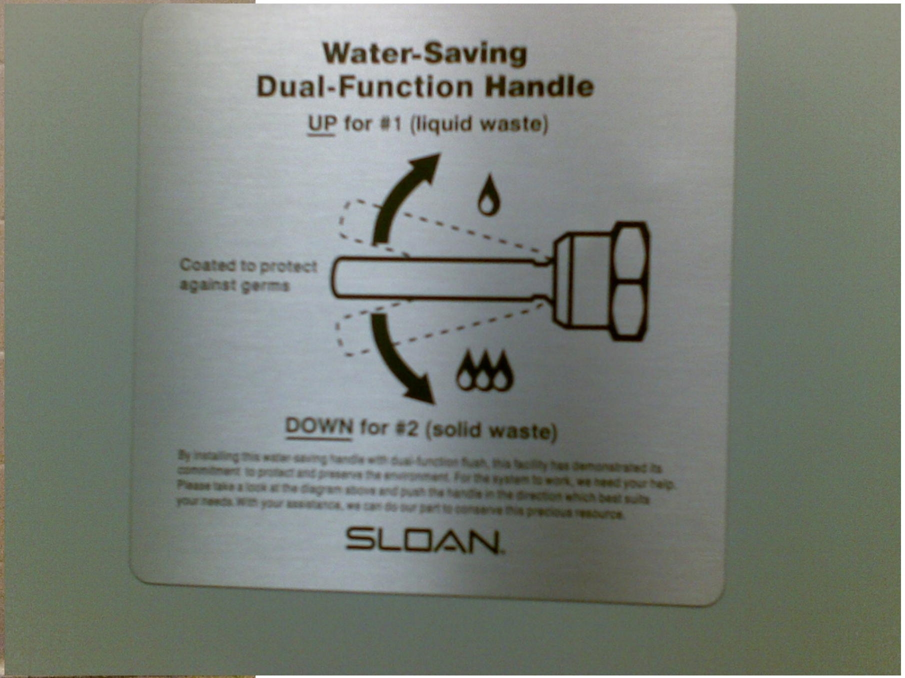


If toilet does not flush automatically before you exit the stall, please press button on the side of the cylinder to flush. ↓

Need to explain the manual override



Should toilets require this much explanation?



Water-Saving
Dual-Function Handle

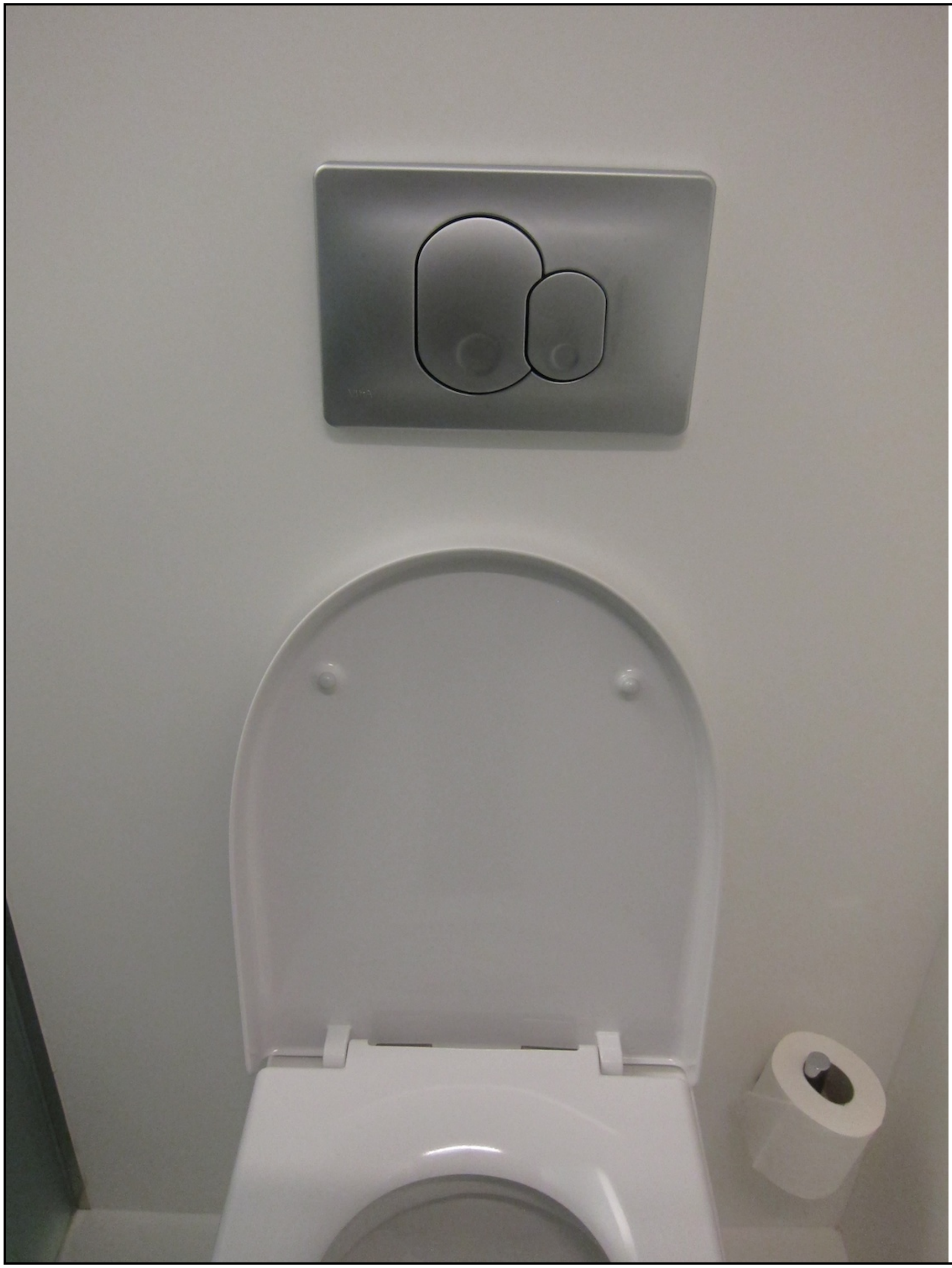
UP for #1 (liquid waste)

Coated to protect against germs

DOWN for #2 (solid waste)

By installing this water-saving handle with dual-function flush, this facility has demonstrated its commitment to protect and preserve the environment. For the system to work, we need your help. Please take a look at the diagram above and push the handle in the direction which best suits your needs. With your assistance, we can do our part to conserve this precious resource.

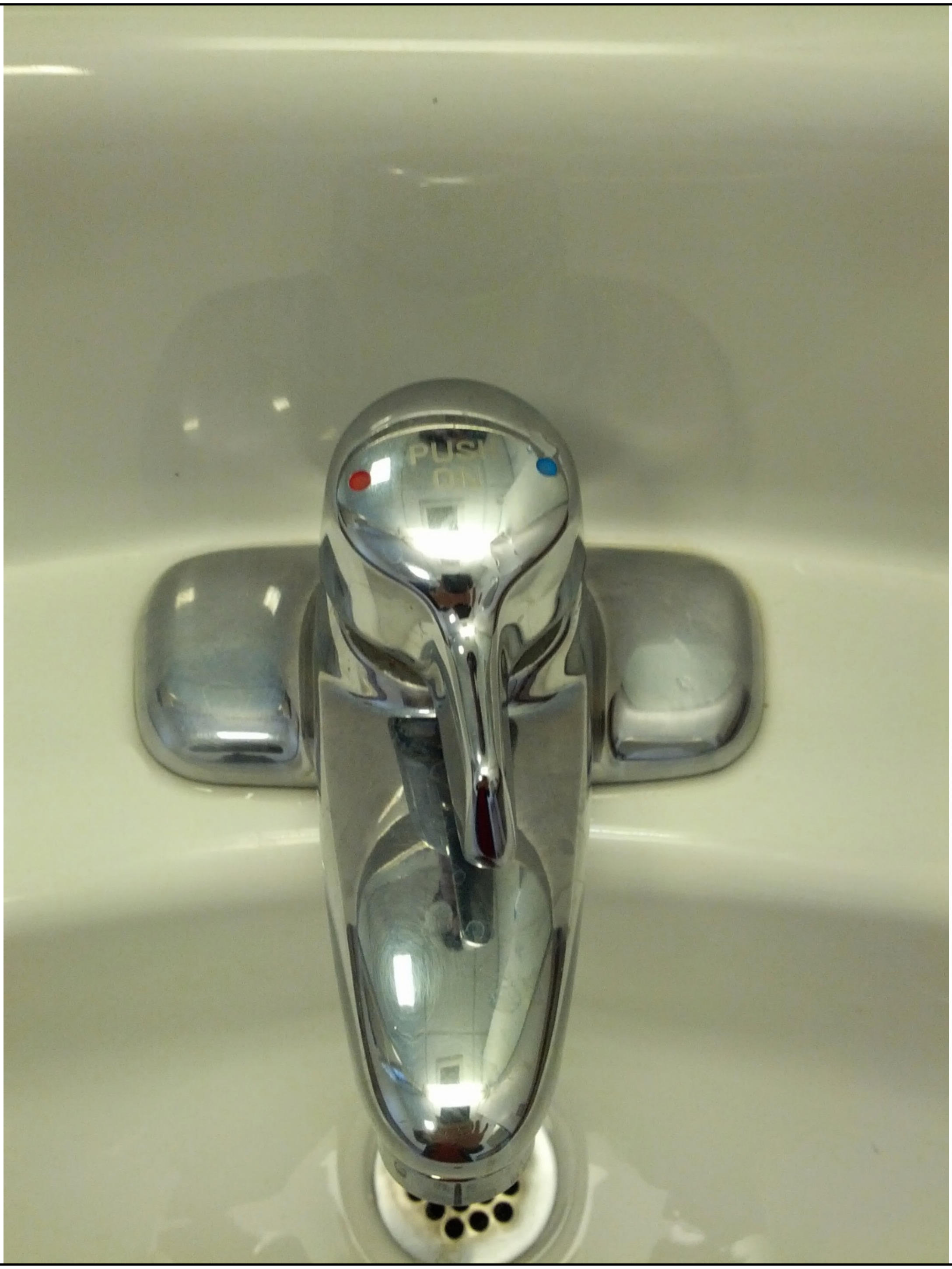
SLOAN



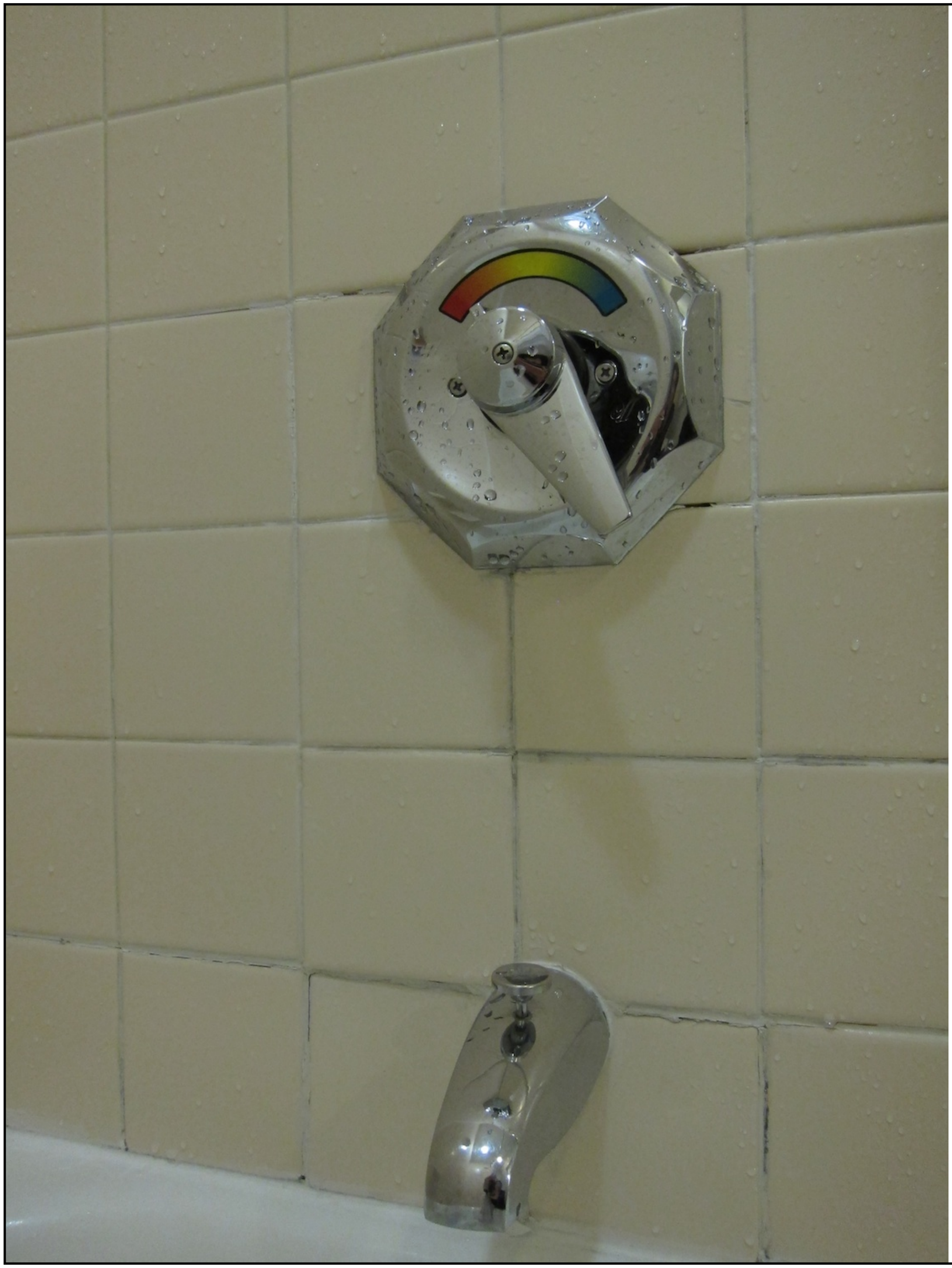
A more intuitive approach?

A more intuitive approach?

(but that tile…)

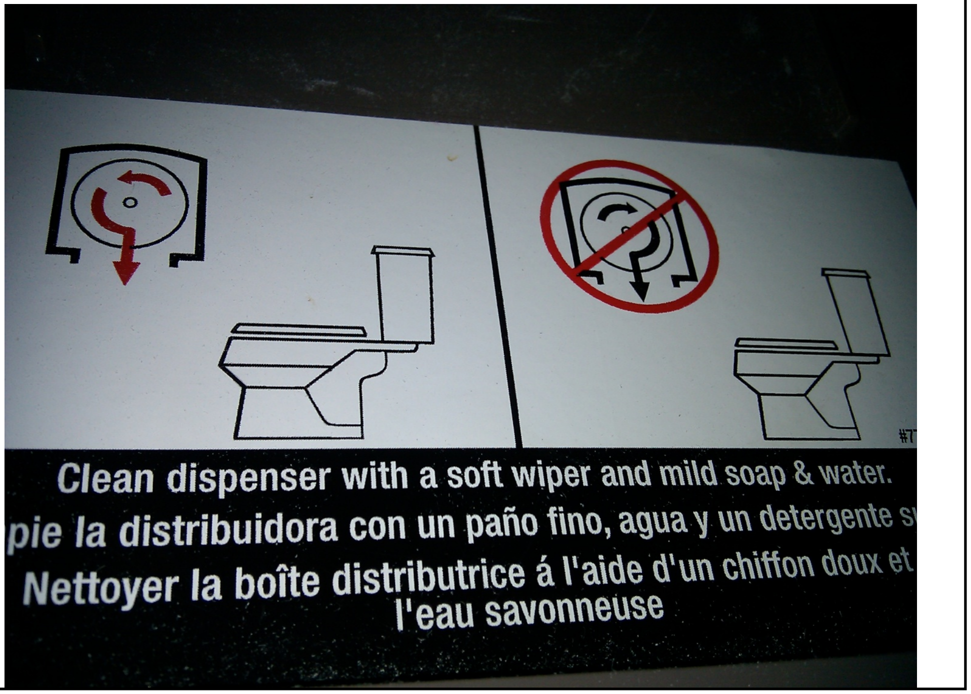


Normally you pull handles



Which way do you turn it to make it hot?

Some things are easier to change than others

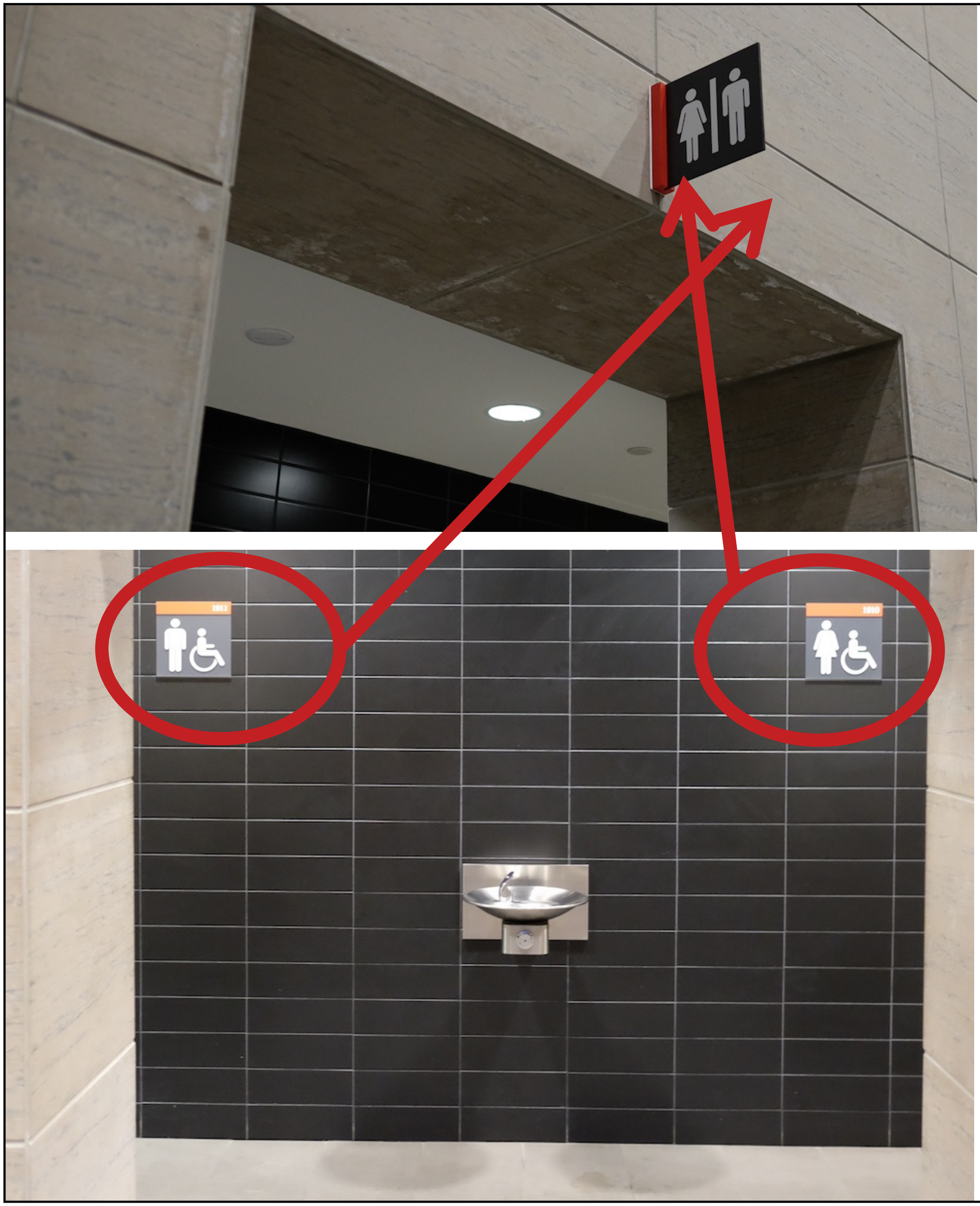


Clean dispenser with a soft wiper and mild soap & water.

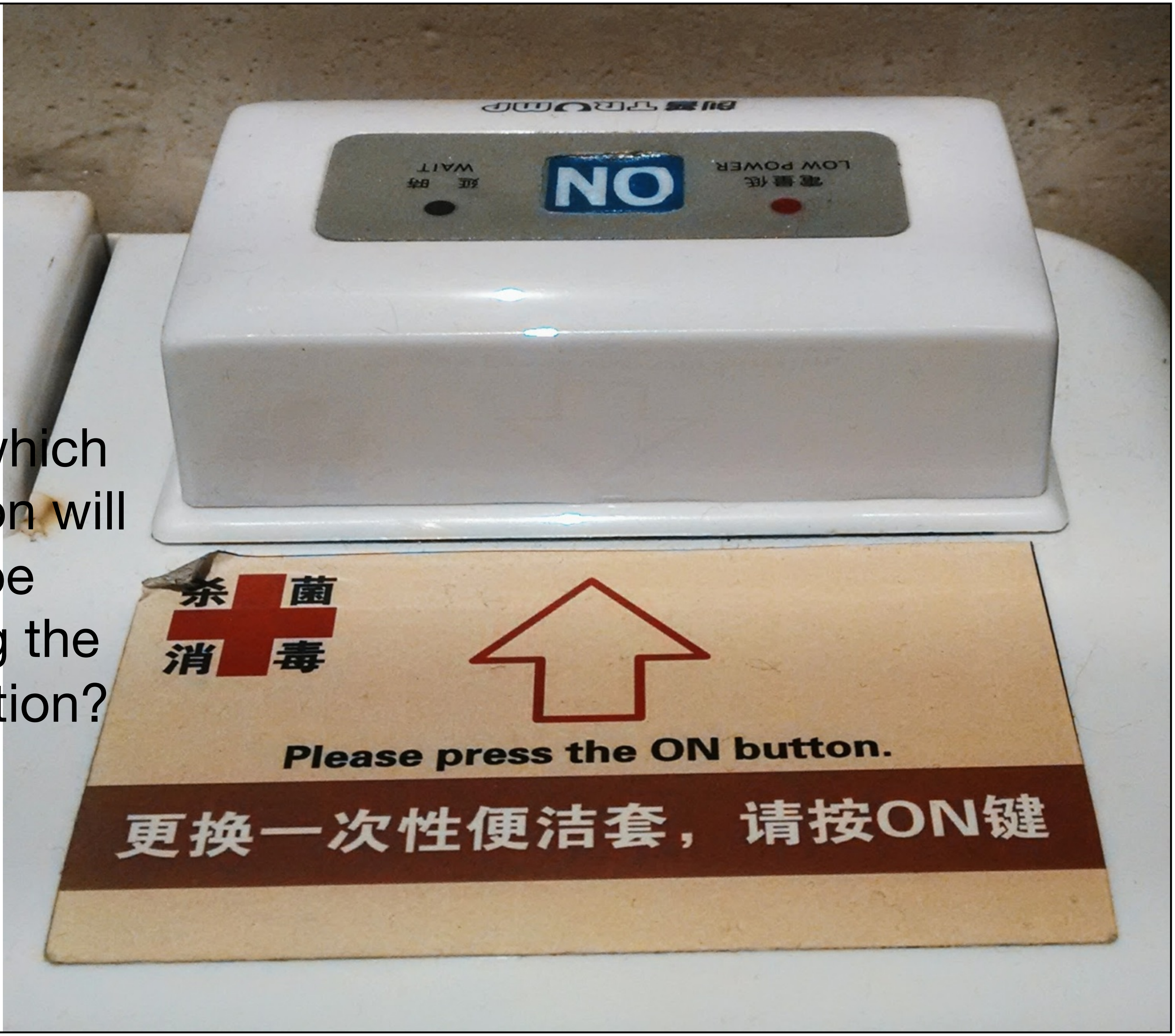
pie la distribuidora con un paño fino, agua y un detergente s

Nettoyer la boîte distributrice á l'aide d'un chiffon doux et
l'eau savonneuse

Perspective matters

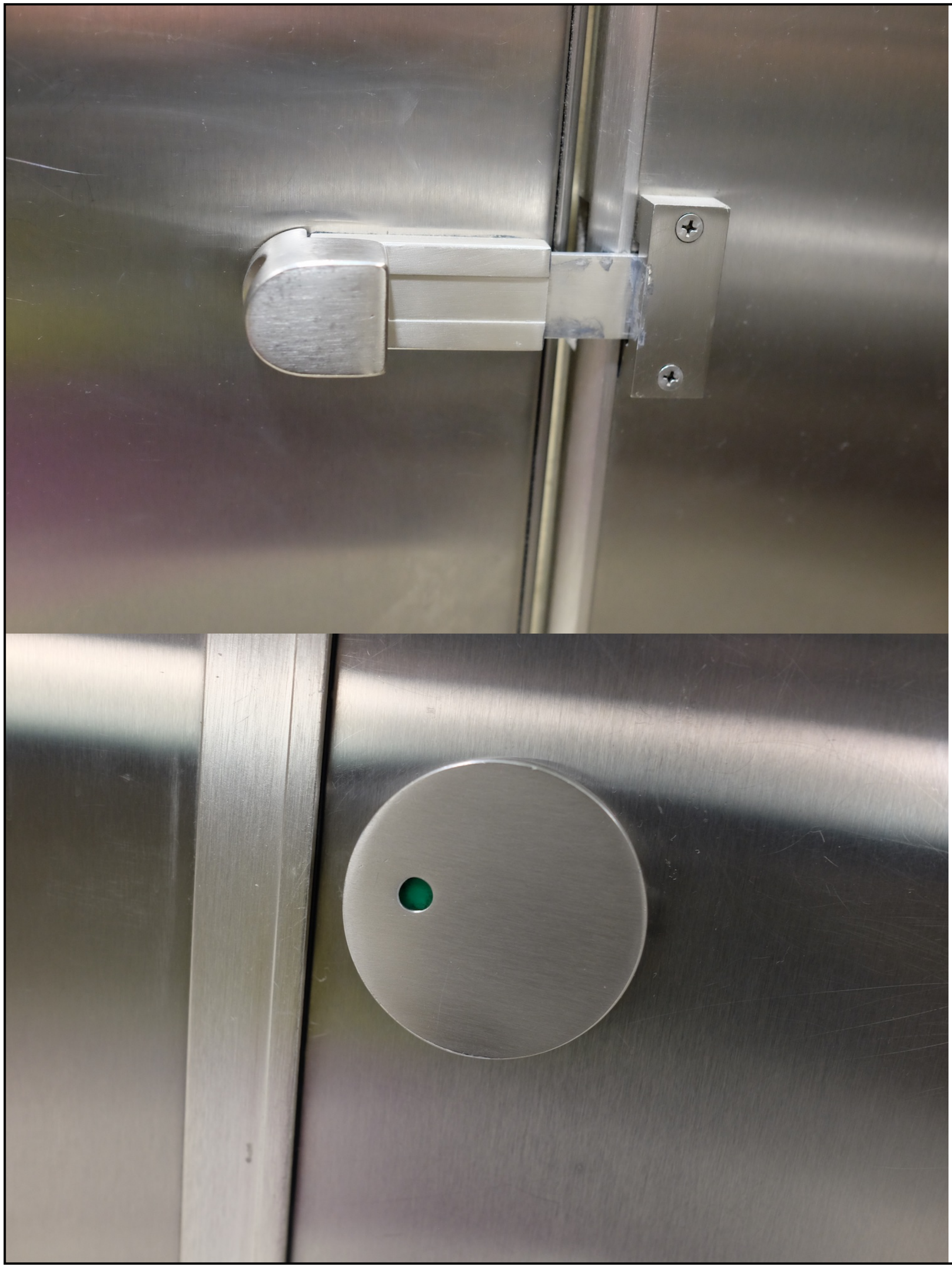


Is the ladies' room on the left or the right?



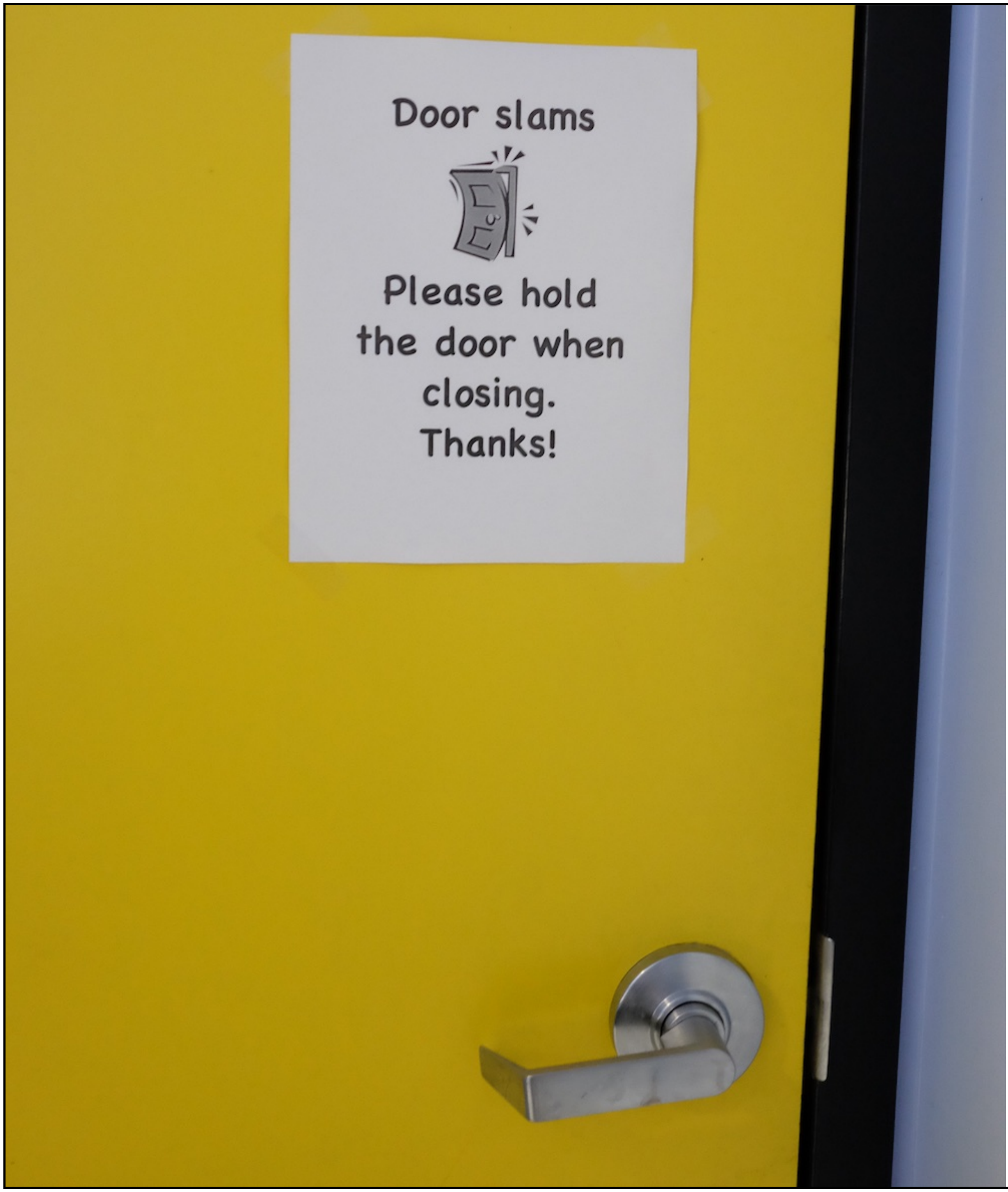
From which direction will users be viewing the instruction?

Design communicates function

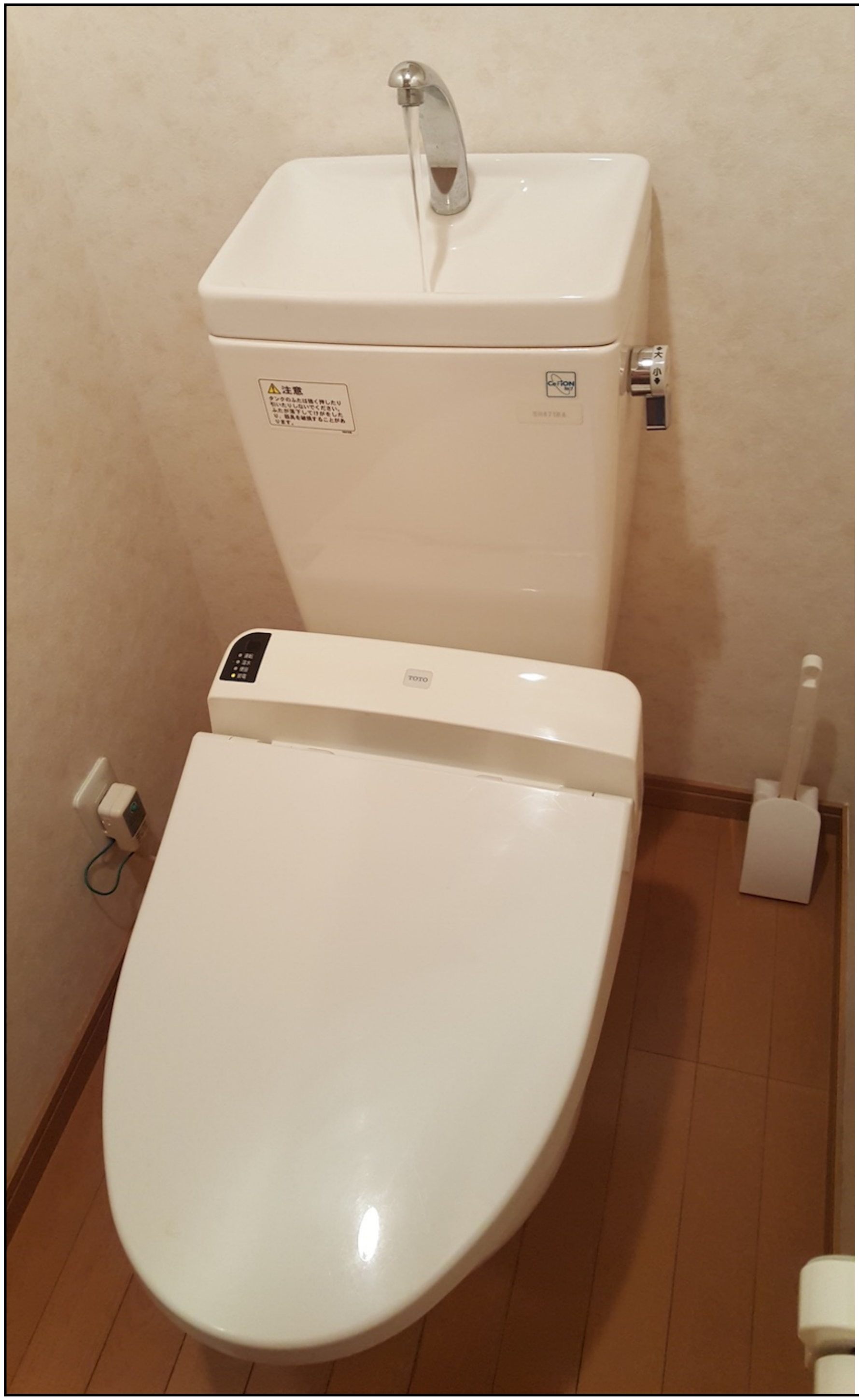


Locking and unlocking door automatically changes color of lock indicator

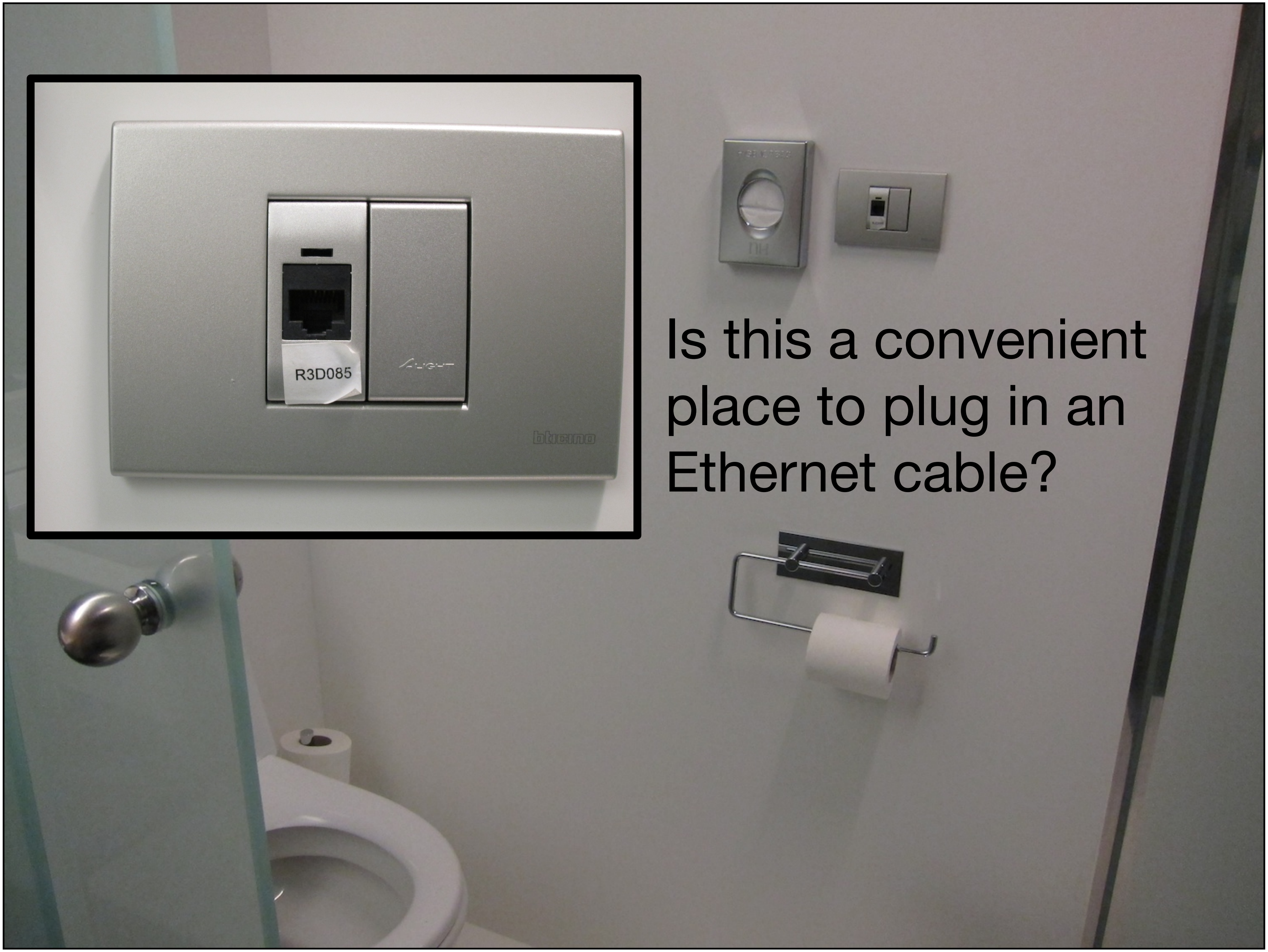
Inconvenient designs



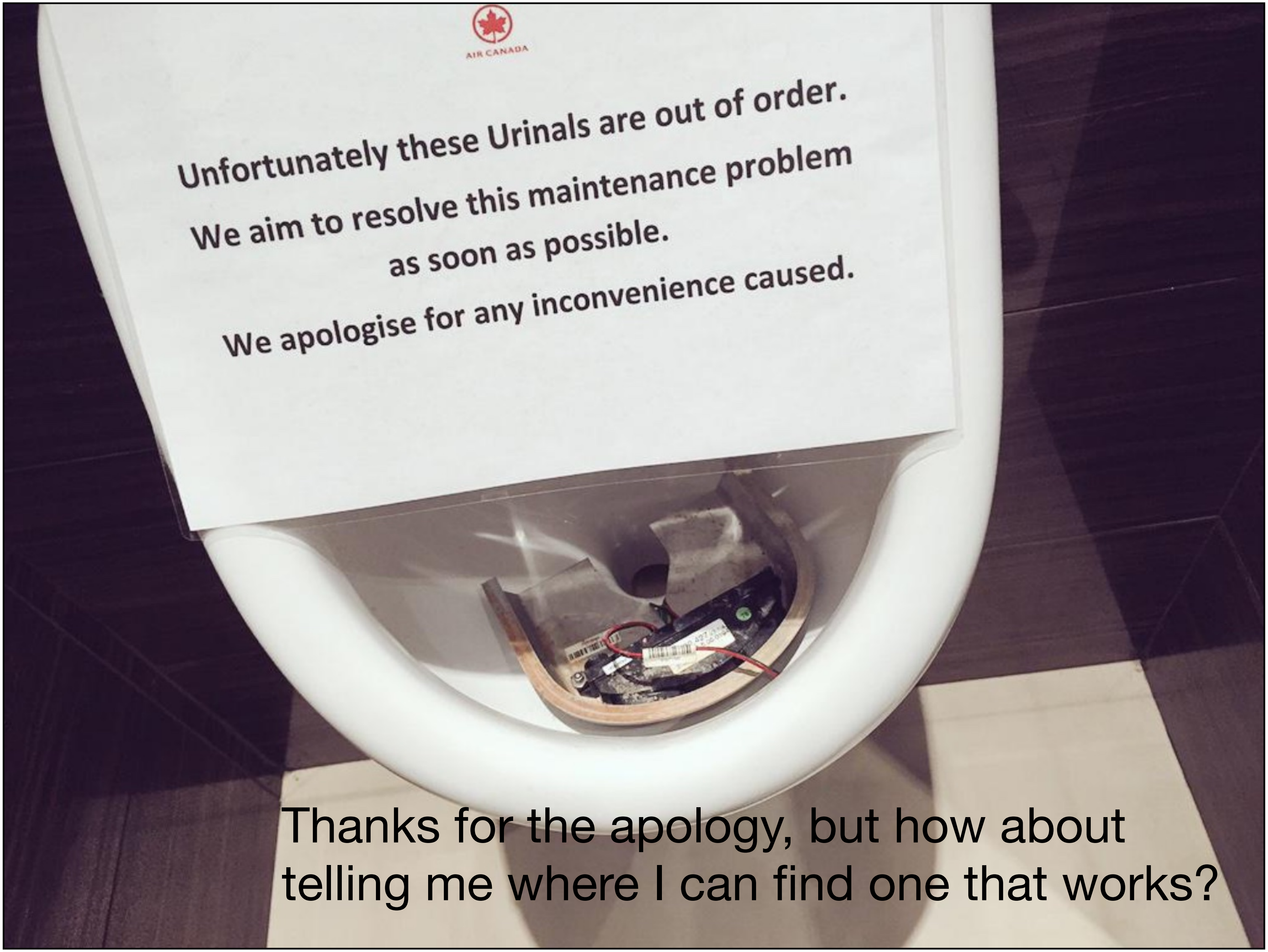
A better solution would be to add a spring so the door won’t slam



It saves space, but kind of an awkward way to wash your hands



Is this a convenient place to plug in an Ethernet cable?



Unfortunately these Urinals are out of order.

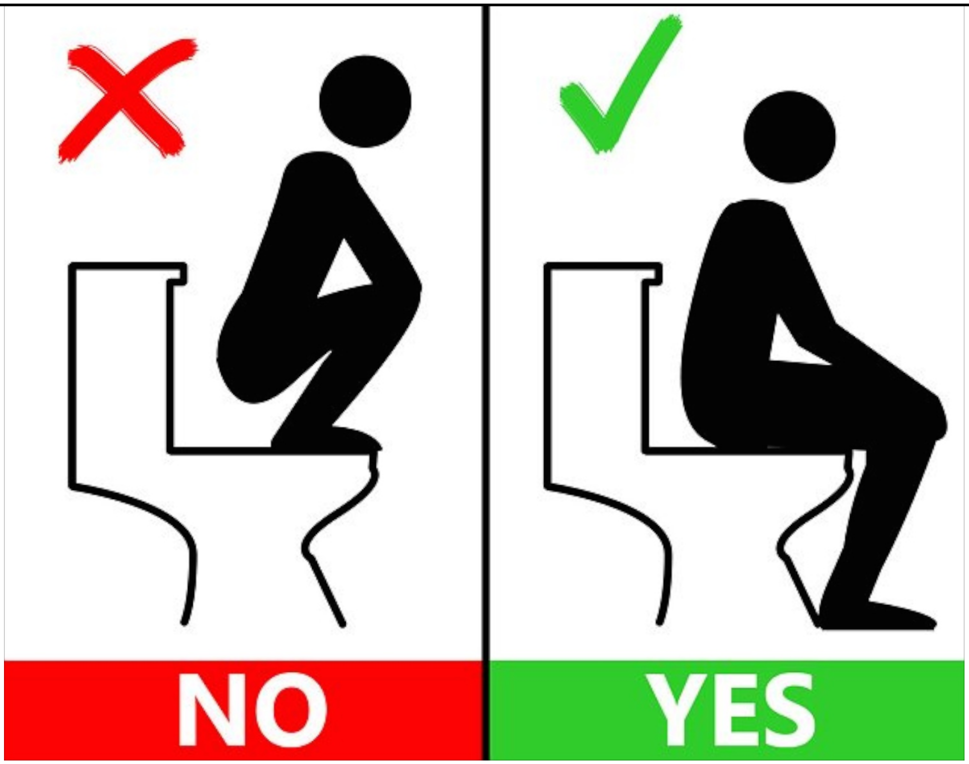
We aim to resolve this maintenance problem
as soon as possible.

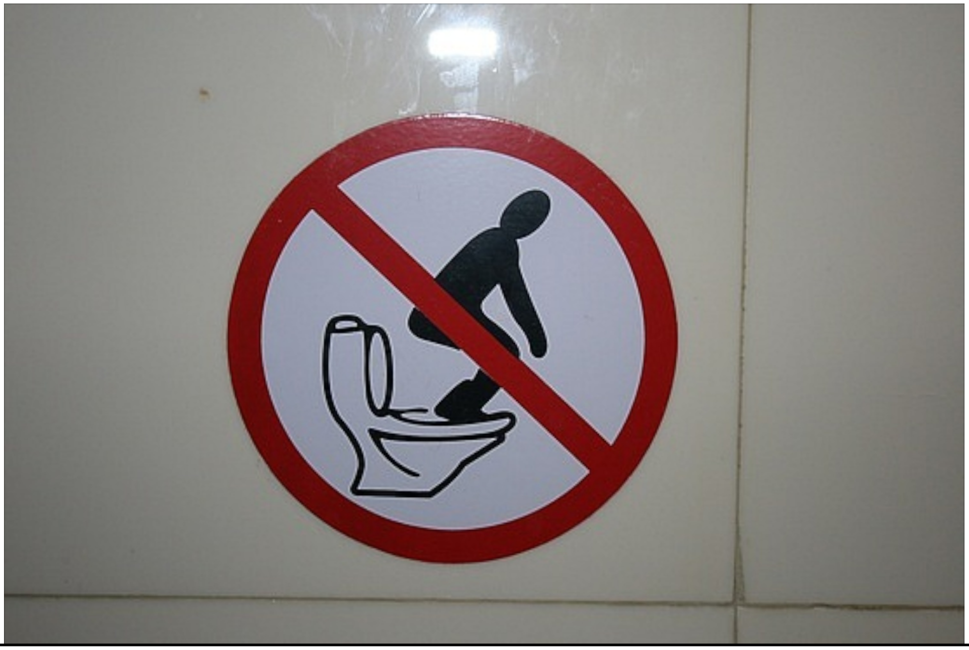
We apologise for any inconvenience caused.

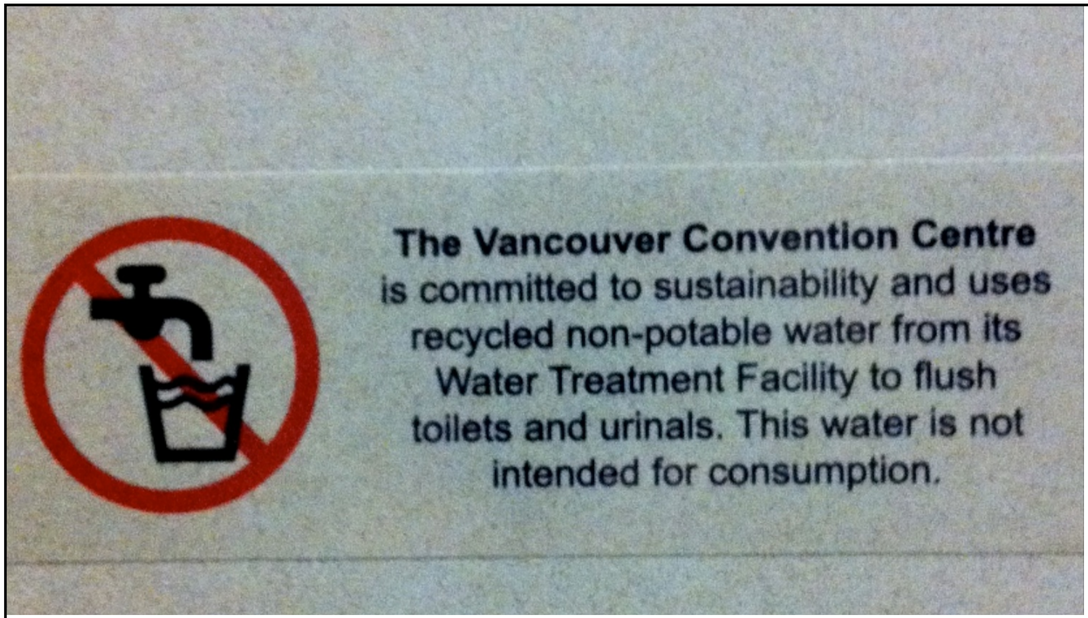
Thanks for the apology, but how about telling me where I can find one that works?

Other issues

Designing for cultural differences

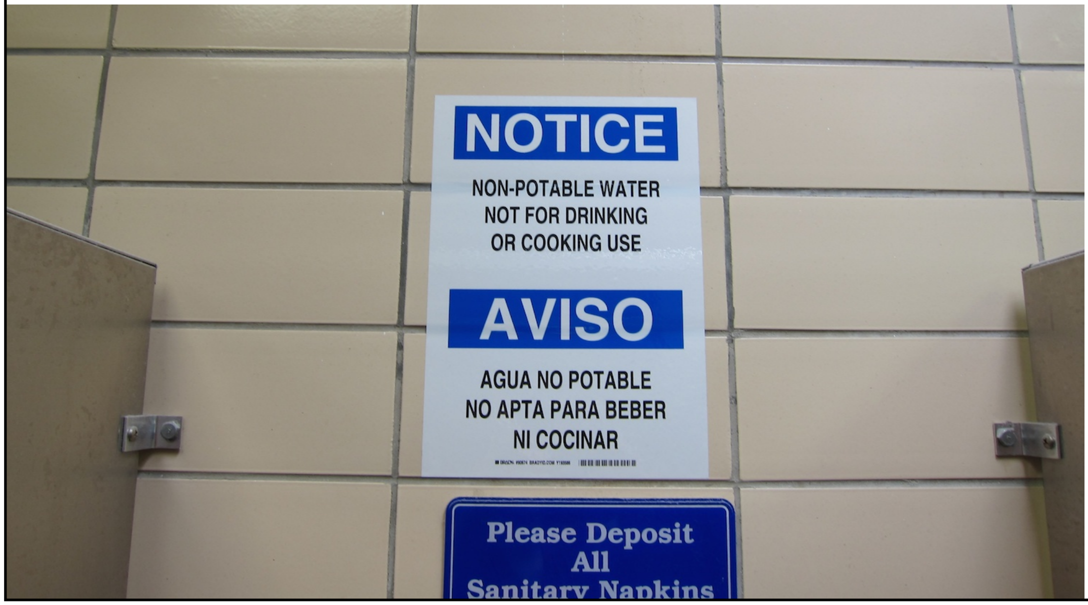






The Vancouver Convention Centre is committed to sustainability and uses recycled non-potable water from its Water Treatment Facility to flush toilets and urinals. This water is not intended for consumption.

Don’t drink the potty water!



NOTICE

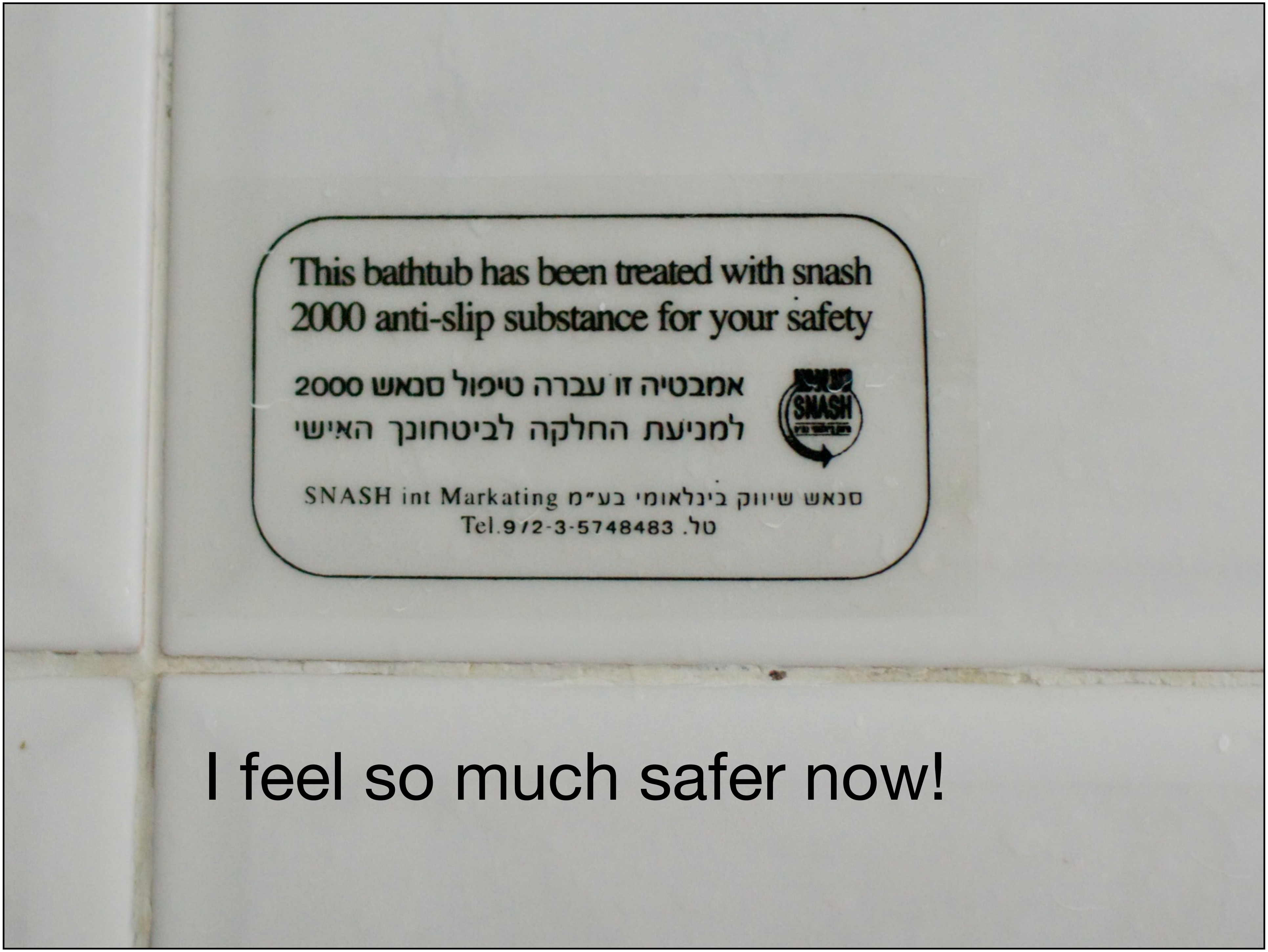
NON-POTABLE WATER
NOT FOR DRINKING
OR COOKING USE

AVISO

AGUA NO POTABLE
NO APTA PARA BEBER
NI COCINAR

Please Deposit
All
Sanitary Napkins

CAUTION: NON-POTABLE WATER, DO NOT DRINK
PRECAUCIÓN: AGUA NO POTABLE, NO BEBER

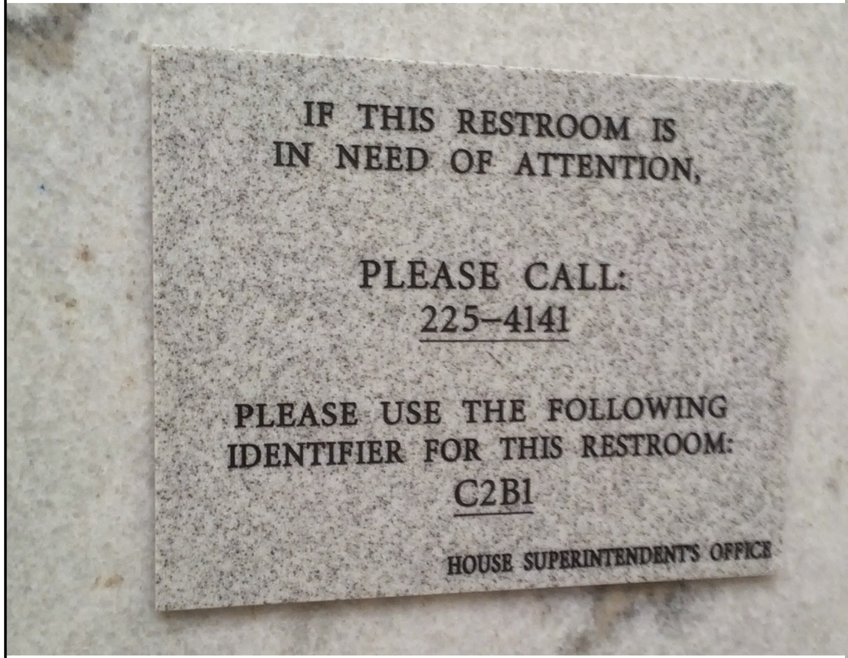


This bathtub has been treated with snash
2000 anti-slip substance for your safety

אמבטיה זו עברה טיפול סנאש 2000
למניעת החלקה לביטחונך האישי

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

I feel so much safer now!



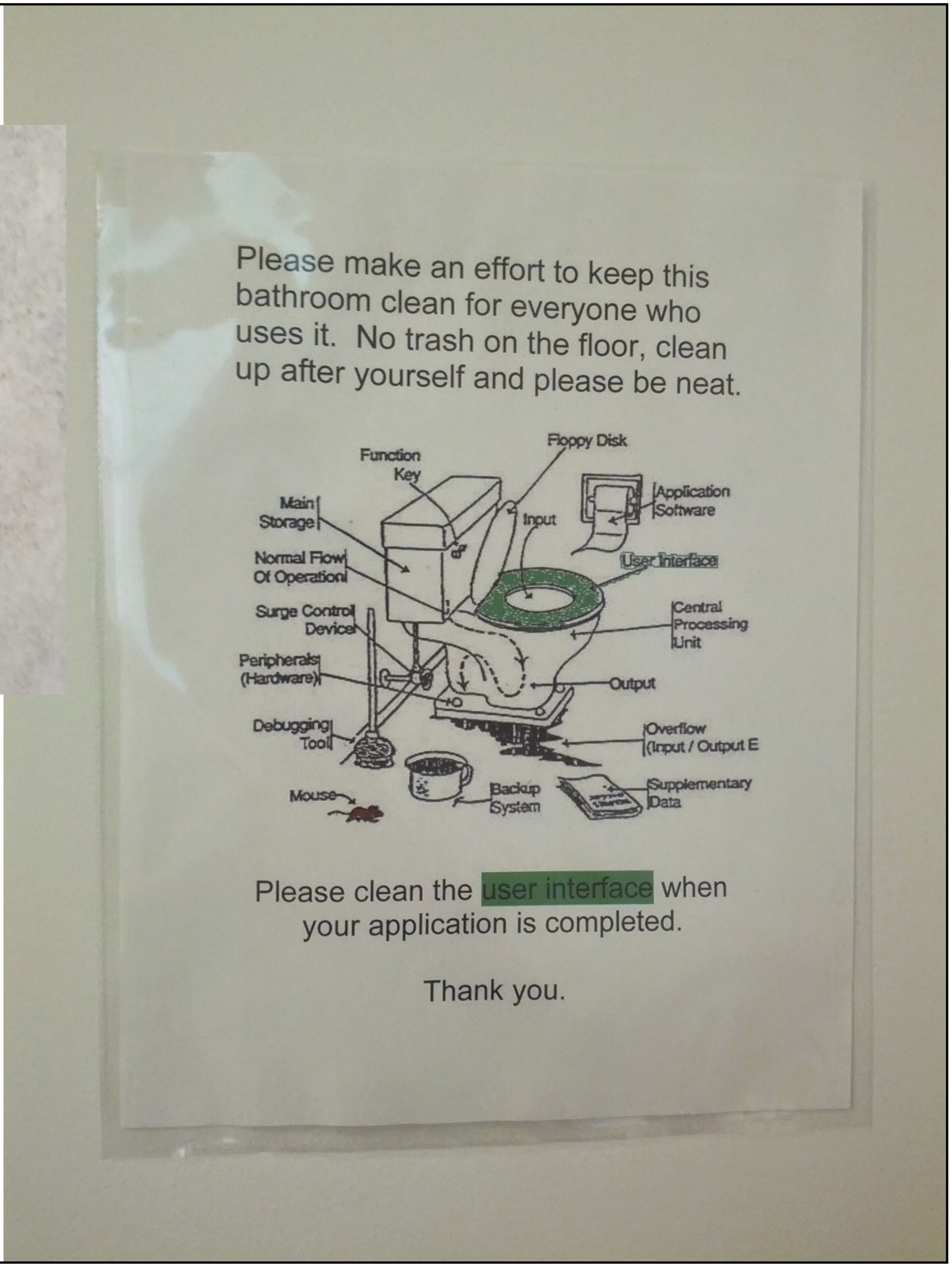
IF THIS RESTROOM IS
IN NEED OF ATTENTION,

PLEASE CALL:
225–4141

PLEASE USE THE FOLLOWING
IDENTIFIER FOR THIS RESTROOM:
C2B1

HOUSE SUPERINTENDENT'S OFFICE

Maintenance instructions can be helpful

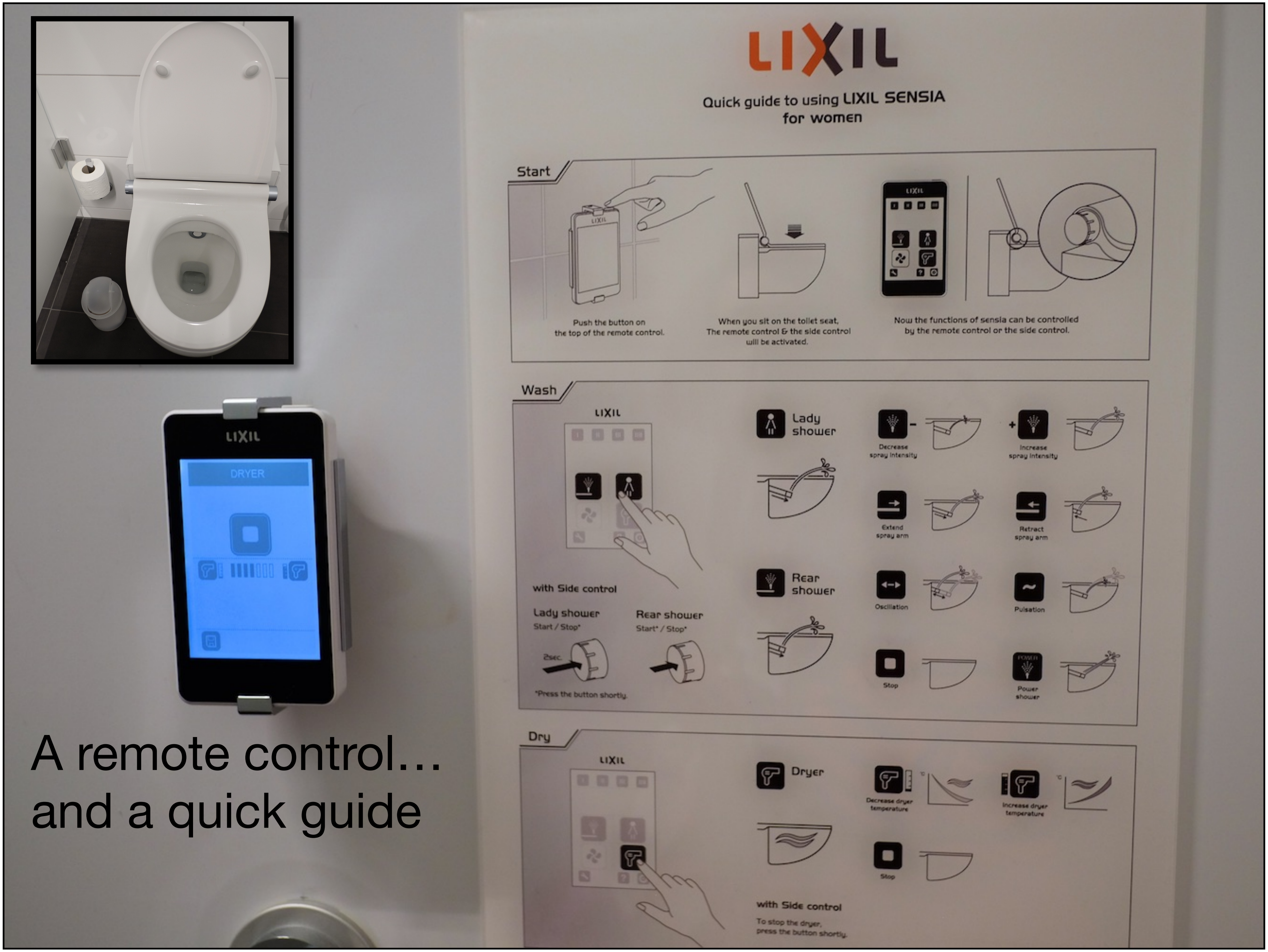


Please make an effort to keep this bathroom clean for everyone who uses it. No trash on the floor, clean up after yourself and please be neat.

Function Key
Floppy Disk
Main Storage
Input
Application Software
User Interface
Normal Flow Of Operation
Surge Control Device
Central Processing Unit
Peripherals (Hardware)
Output
Debugging Tool
Overflow (Input / Output E
Mouse
Backup System
Supplementary Data

Please clean the user interface when your application is completed.

Thank you.



LIXIL

Quick guide to using LIXIL SENSIA
for women

Start

Push the button on
the top of the remote control.

When you sit on the toilet seat,
The remote control & the side control
will be activated.

Now the functions of sensia can be controlled
by the remote control or the side control.

Wash

Lady shower

Rear shower

Decrease spray intensity

Increase spray intensity

Extend spray arm

Retract spray arm

Oscillation

Pulsation

Stop

Power shower

with Side control

Lady shower
Start / Stop*

Rear shower
Start* / Stop*

*Press the button shortly.

Dry

Dryer

Decrease dryer temperature

Increase dryer temperature

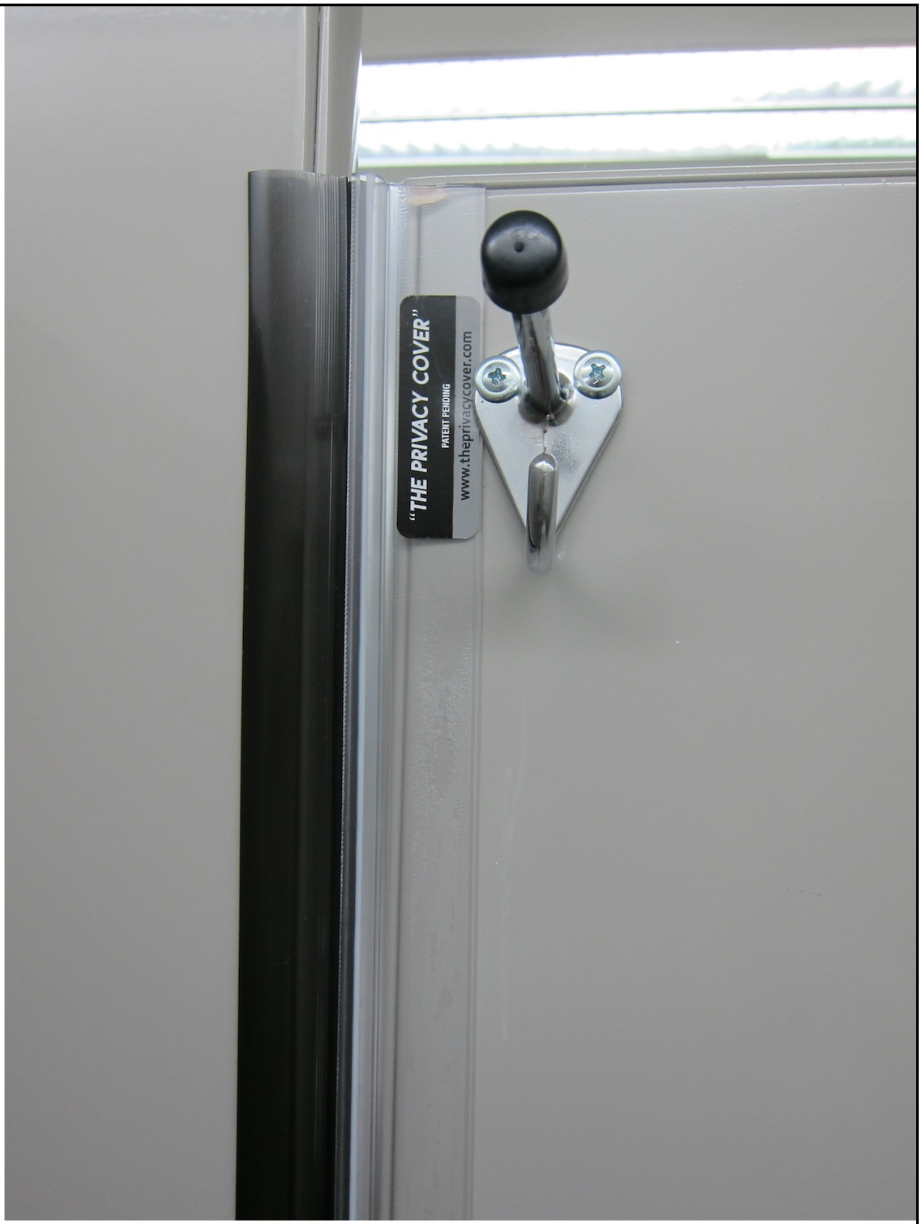
Stop

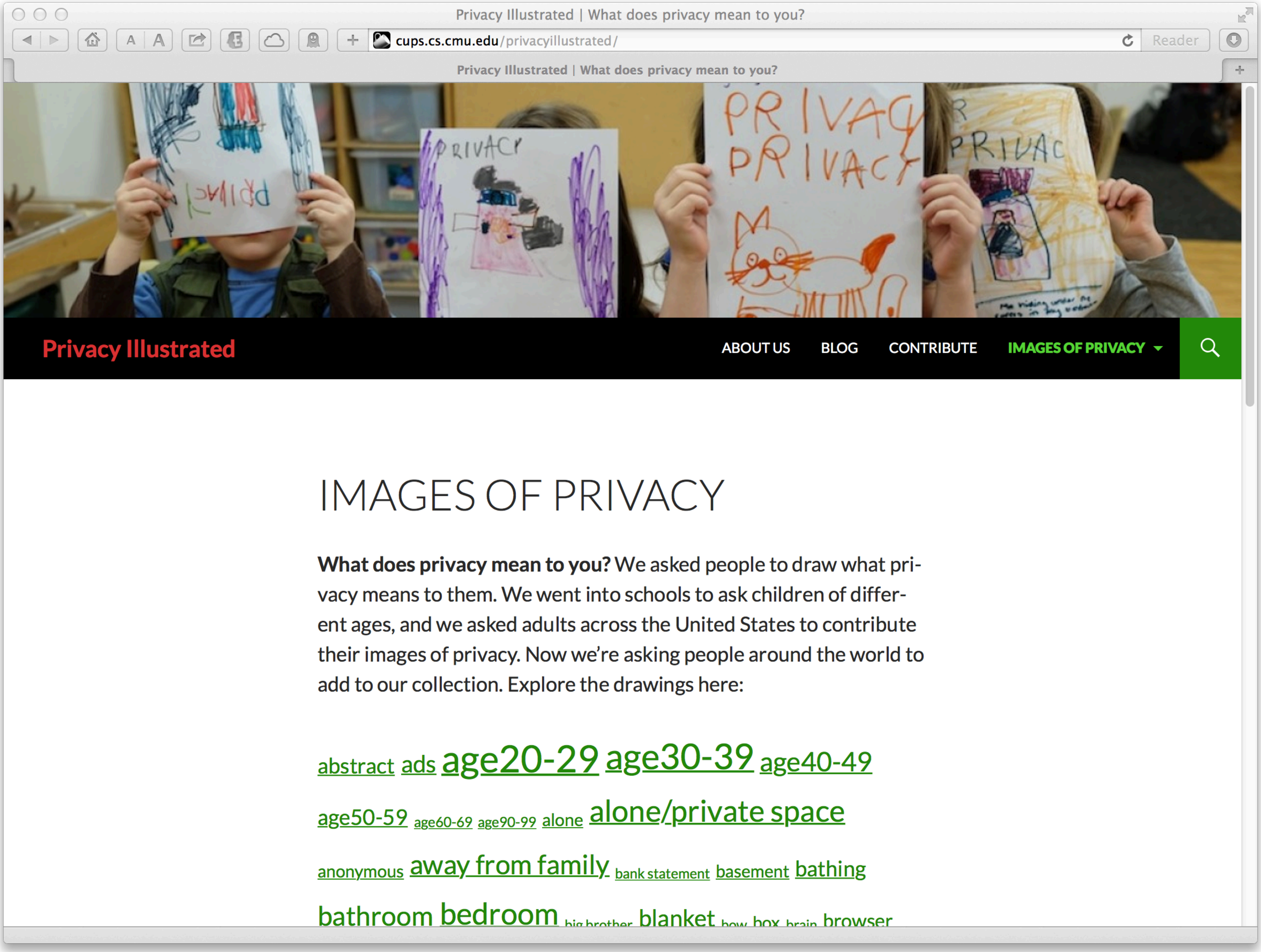
with Side control

To stop the dryer,
press the button shortly.

A remote control…
and a quick guide

A patch for a privacy problem





Privacy Illustrated | What does privacy mean to you?
cups.cs.cmu.edu/privacyillustrated/
Reader
Privacy Illustrated | What does privacy mean to you?
PRIVACY
PRIVACY
PRIVACY
PRIVACY
PRIVAC

Privacy Illustrated

ABOUT US BLOG CONTRIBUTE IMAGES OF PRIVACY

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