

# 04 - Introduction to Privacy

Lorrie Cranor

January 30, 2017

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

Carnegie  
Mellon  
University  
CyLab



Engineering &  
Public Policy



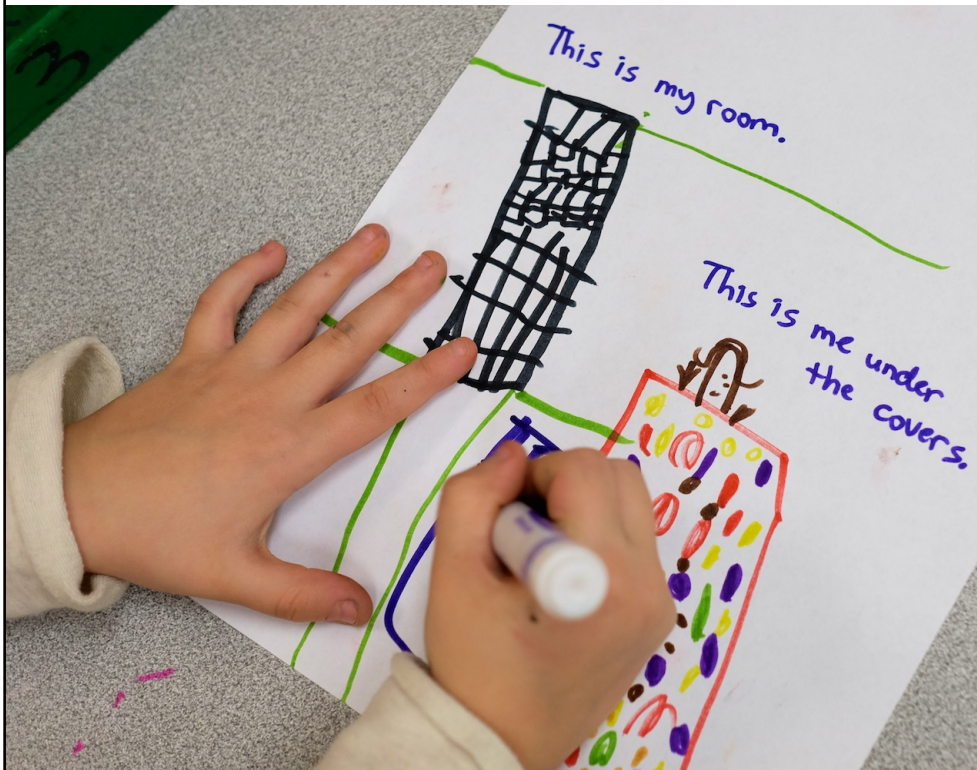
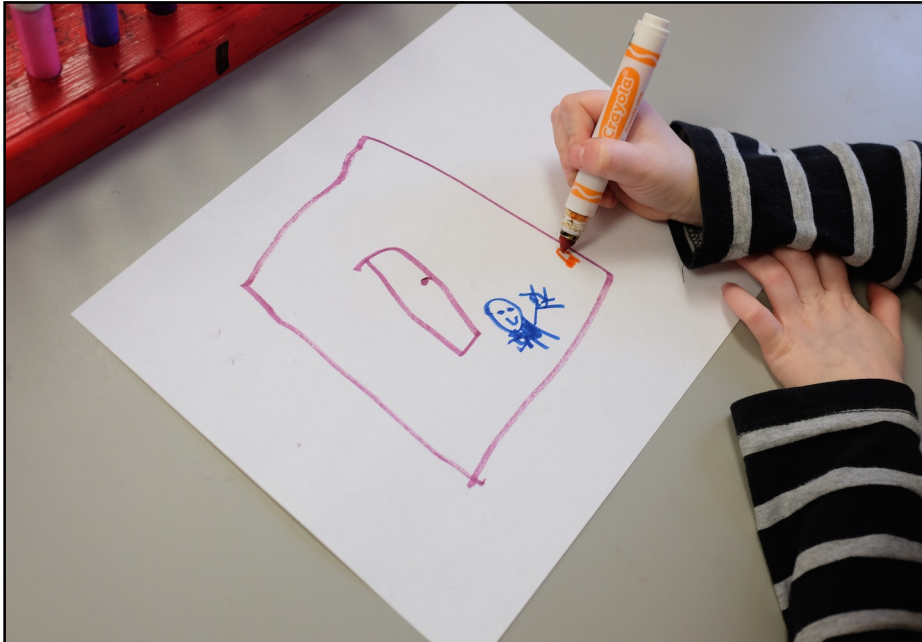
# Today's class

- What does privacy mean to you?
- Privacy goals
- Why is privacy hard to measure?
- How privacy is protected
- Privacy notice and choice (intro)
- Homework presentations



# What does privacy mean to you?

[http://cups.cs.cmu.edu/  
privacyillustrated/](http://cups.cs.cmu.edu/privacyillustrated/)











## Mechanical Turk is a marketplace for work.

We give businesses and developers access to an on-demand, scalable workforce.  
Workers select from thousands of tasks and work whenever it's convenient.

**376,614 HITs** available. [View them now.](#)

## Make Money by working on HITs

HITs - *Human Intelligence Tasks* - are individual tasks that you work on. [Find HITs now.](#)

### As a Mechanical Turk Worker you:

- Can work from home
- Choose your own work hours
- Get paid for doing good work



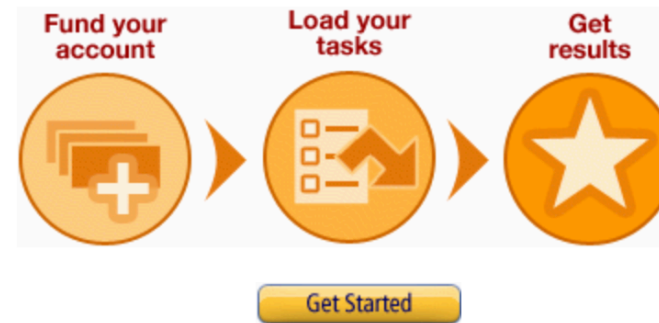
or [learn more about being a Worker](#)

## Get Results from Mechanical Turk Workers

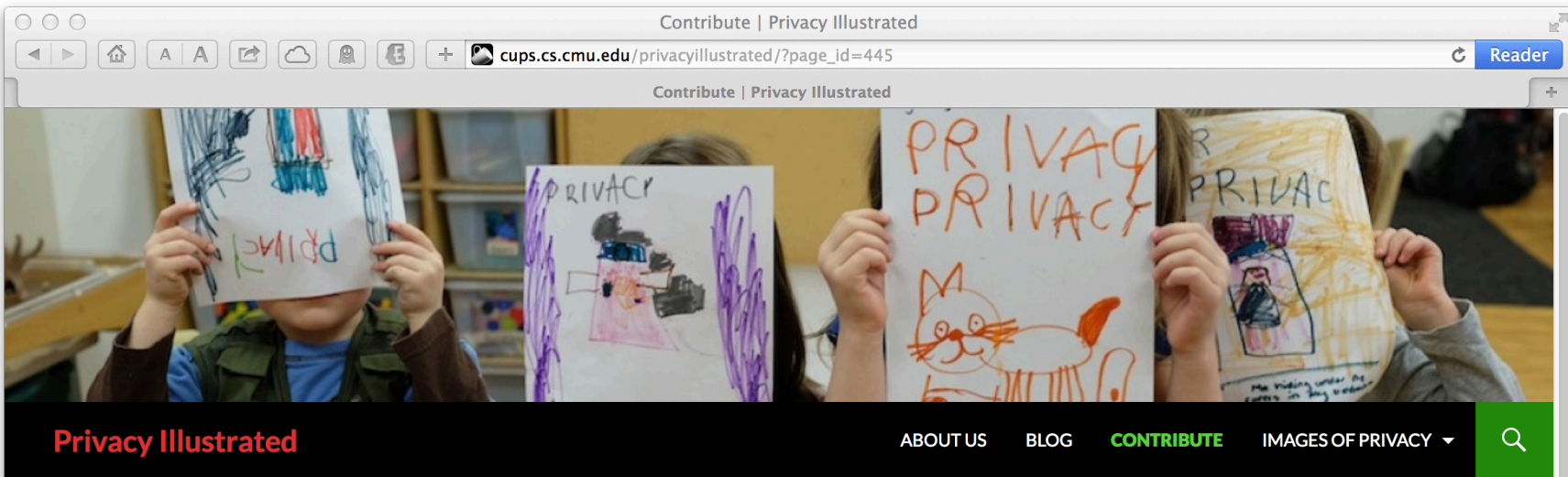
Ask workers to complete HITs - *Human Intelligence Tasks* - and get results using Mechanical Turk. [Get Started.](#)

### As a Mechanical Turk Requester you:

- Have access to a global, on-demand, 24 x 7 workforce
- Get thousands of HITs completed in minutes
- Pay only when you're satisfied with the results







## CONTRIBUTE

What does privacy mean to you?

Contribute to the dialogue by submitting your own picture.

Please draw a picture of what privacy means to you and then upload it below. You can either draw the picture on paper and then take a picture of it to upload or scan it for upload. Alternatively, you can draw it using a tablet or other electronic medium and then upload it.



### RECENT POSTS

[The making of Privacy Illustrated: Kids with their drawings](#)  
January 14, 2015

[Privacy Illustrated in the Pittsburgh Post-Gazette](#)  
January 12, 2015

[Join us for CMU Privacy Day on January 28](#)  
January 12, 2015

[Privacy Illustrated appears in new Deep Lab book](#)  
December 23, 2014

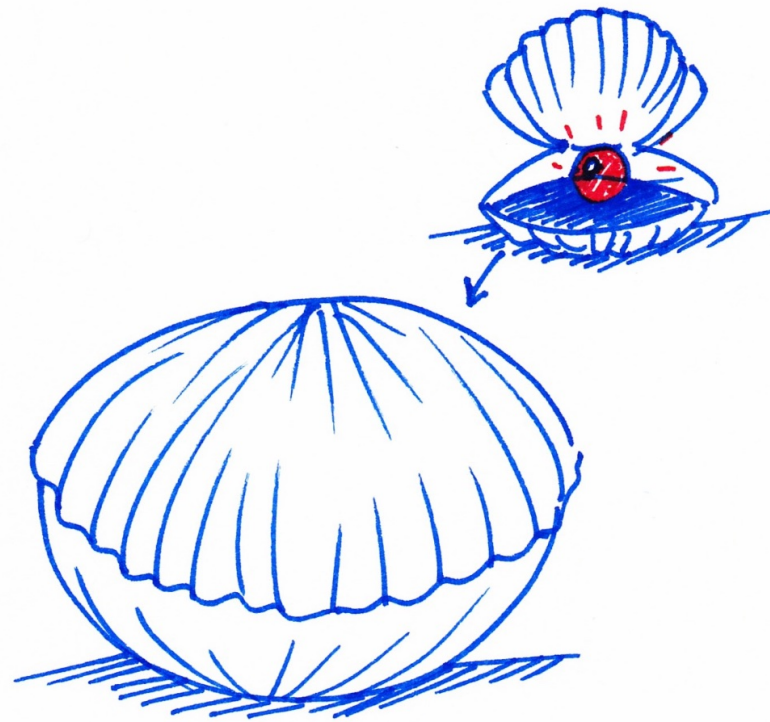
[Privacy Illustrated Book Chapter](#)  
December 13, 2014





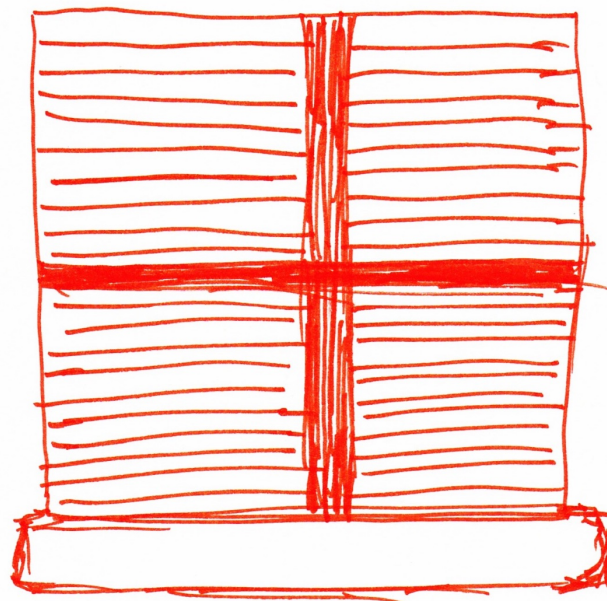
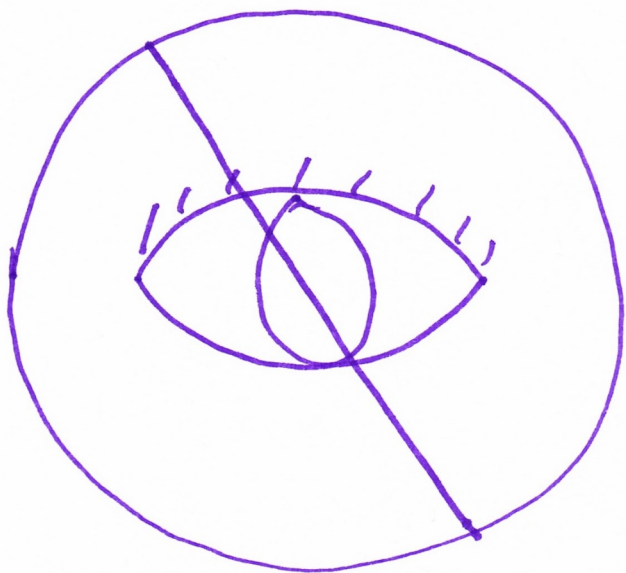
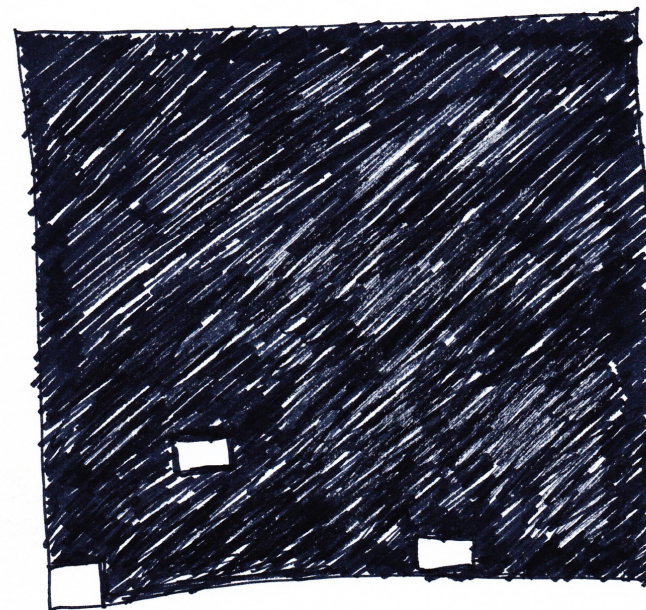
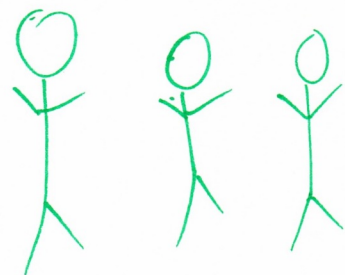
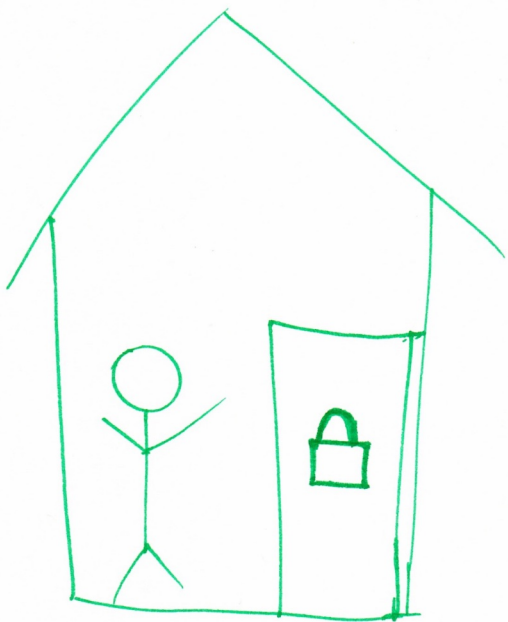


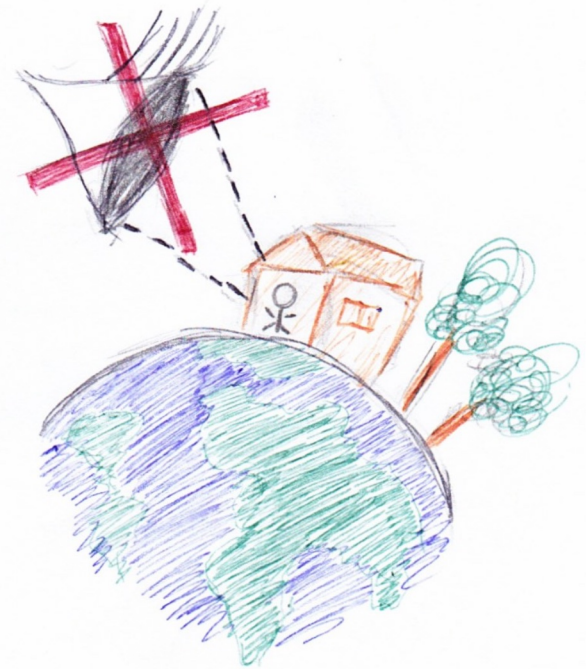
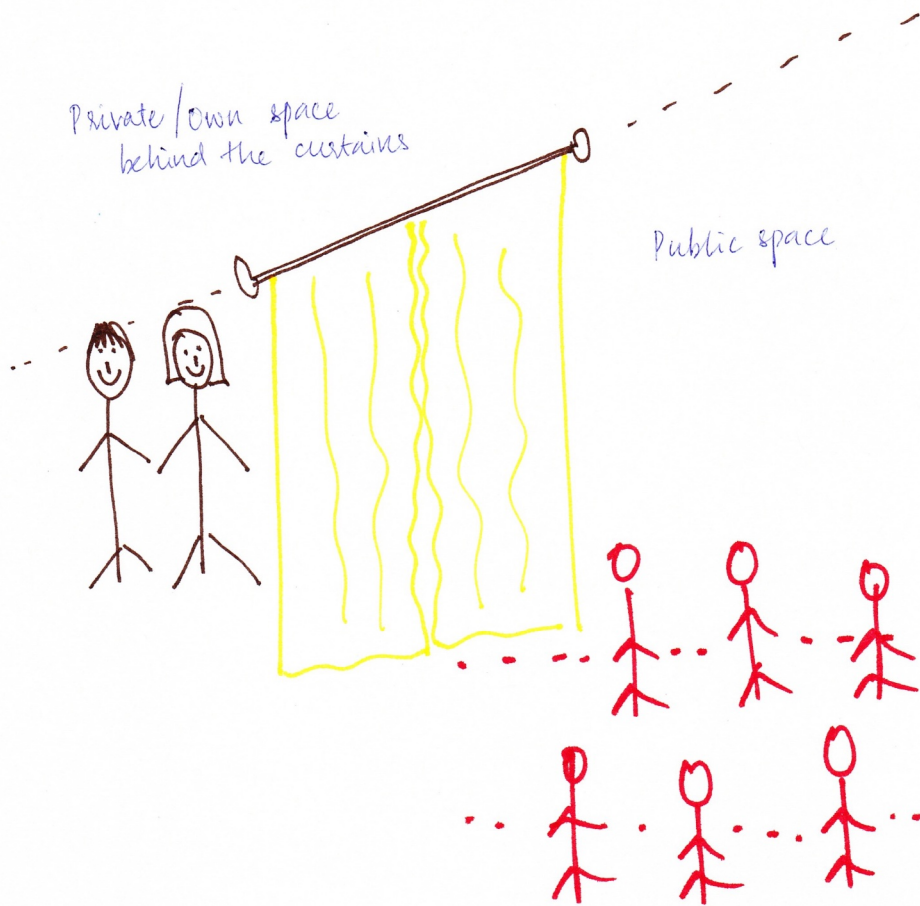




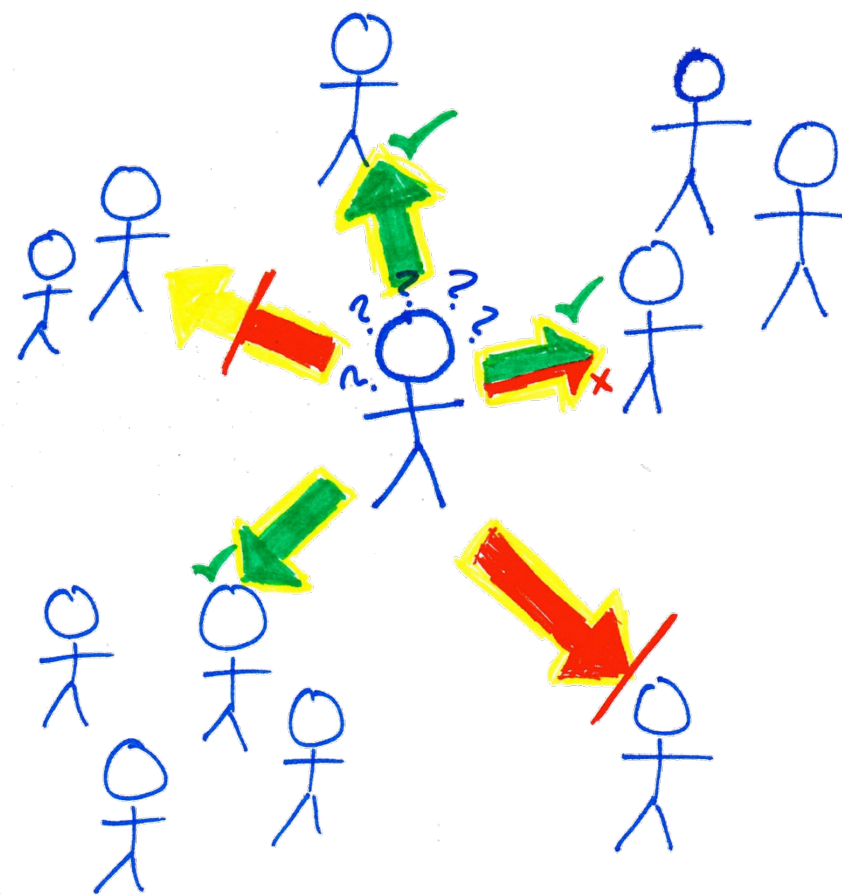
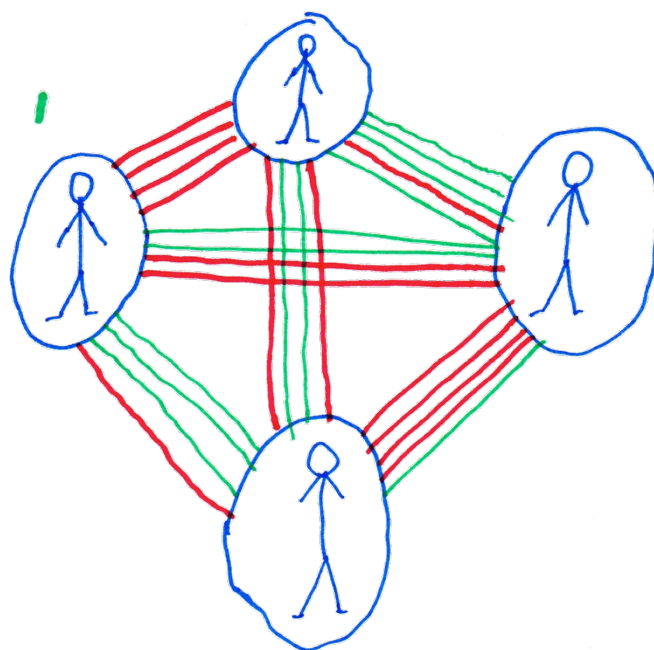
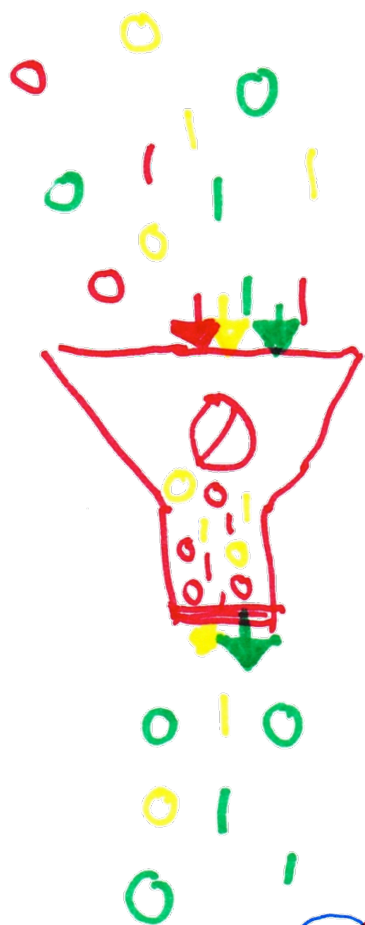
PEARL OYSTERS HAVE SOMETHING VALUABLE  
TO PROTECT - **THE PEARL**.  
THEY CAN DO SO BY SIMPLY 'CLOSING THE LID'.  
IF ONLY SAFEGUARDING THE DATA IN MY  
LAPTOP WERE THAT SIMPLE!

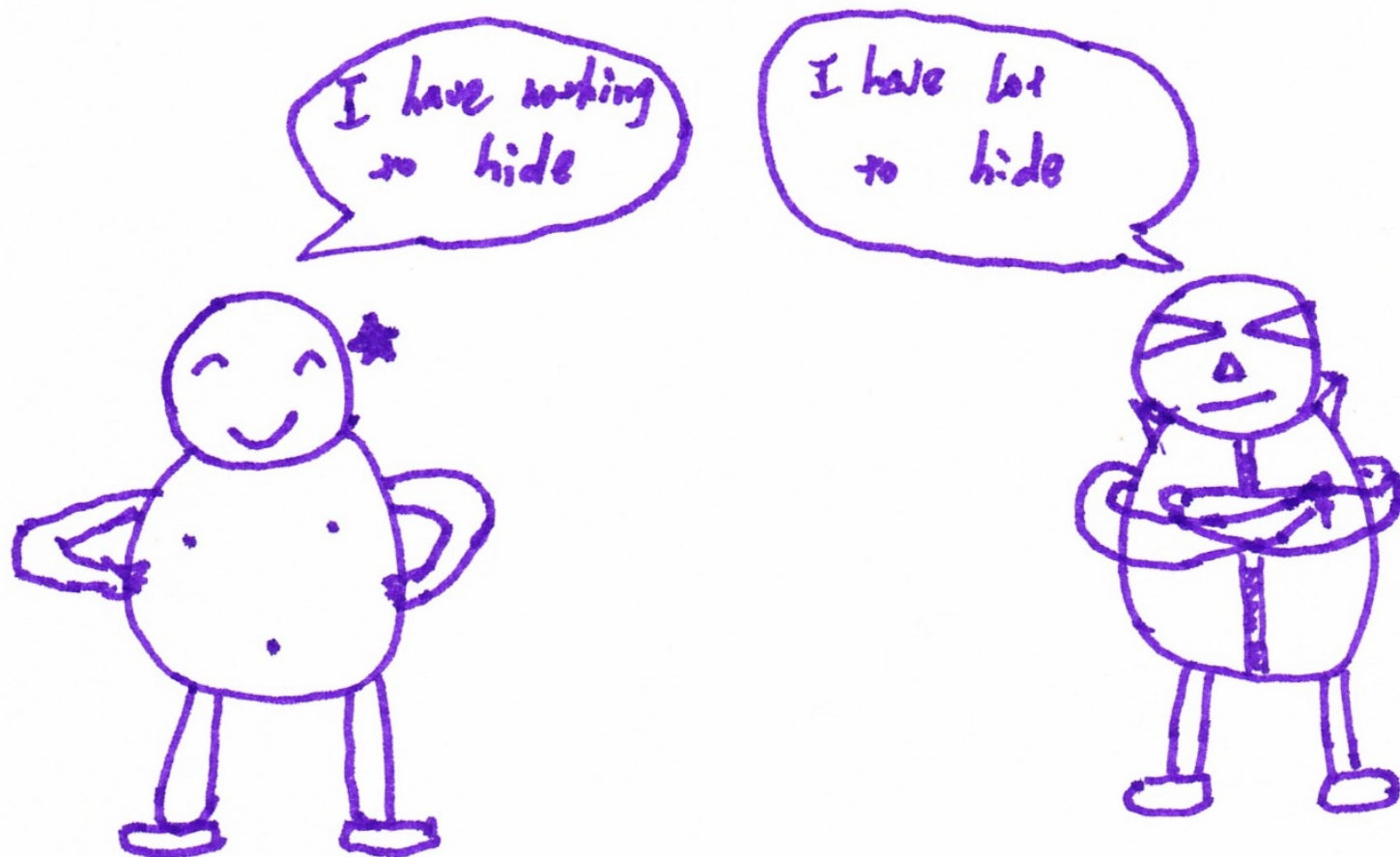
Sharon Monica Rajkumar

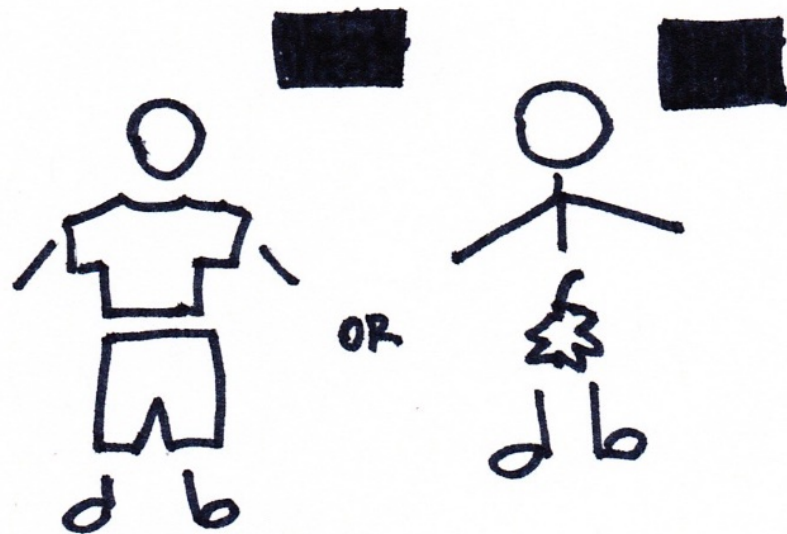






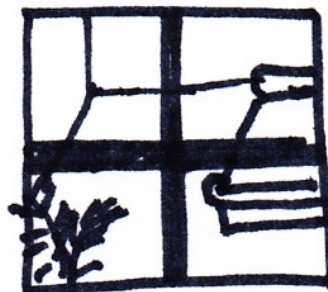






" PRIVACY IS BEING  
ABLE TO COVER YOURSELF  
OR YOUR THINGS AS MUCH  
AS YOU WANT."

Hi, MY NAME IS [REDACTED] . OR  
Hi, MY NAME IS BOBBY .



OR

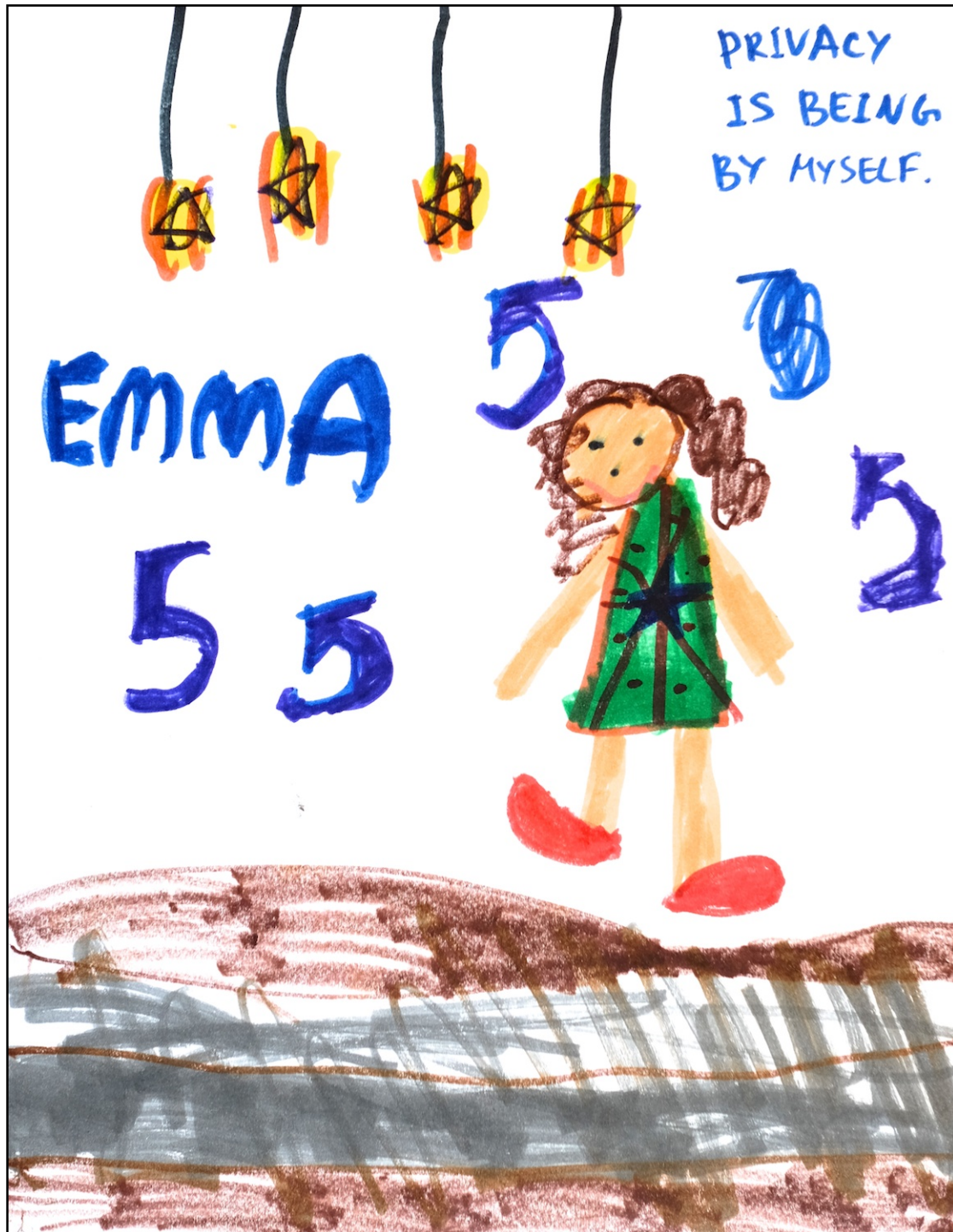




Privacy means  
having a safe  
space knowing  
that no one will  
be able to see it  
w/o my  
permission.







the right to  
be let alone

– Samuel D. Warren  
& Louis D. Brandeis  
*The Right to Privacy*  
December, 1890



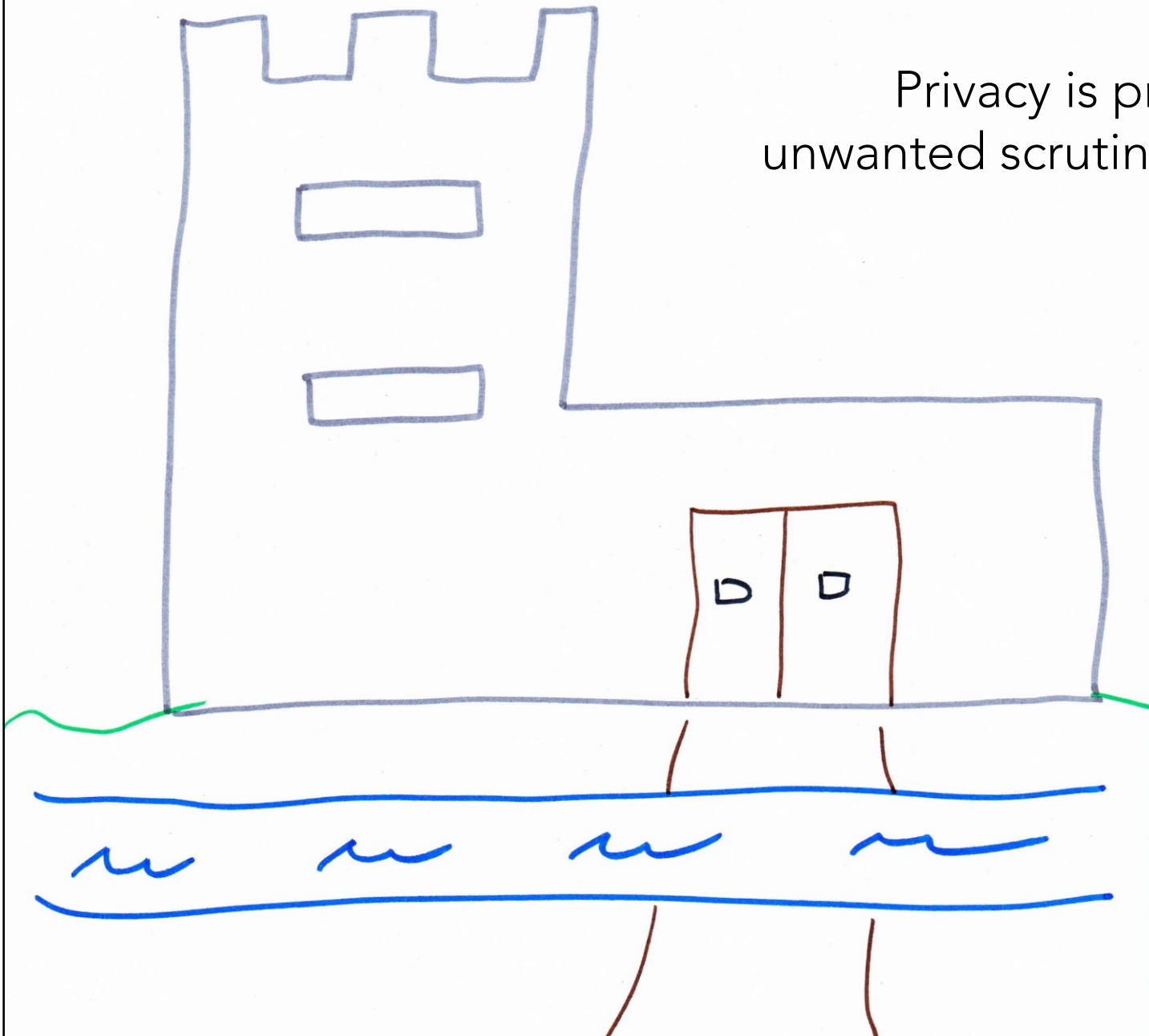




Privacy is the right to be by yourself. Privacy is isolation.  
– Kevin, age 28

Privacy is protection from  
unwanted scrutiny or attention.

–RMF, age 54



This is me in my privacy room in my basement. I go in there when I want to be alone. I can calm down and breathe.







My clubhouse in my basement is private. My  
Brothers and me have secret meetings. Felicity 5





Being safe in my room....  
Curtains on my windows, a  
lock on my door, and my  
computer protected by a  
firewall

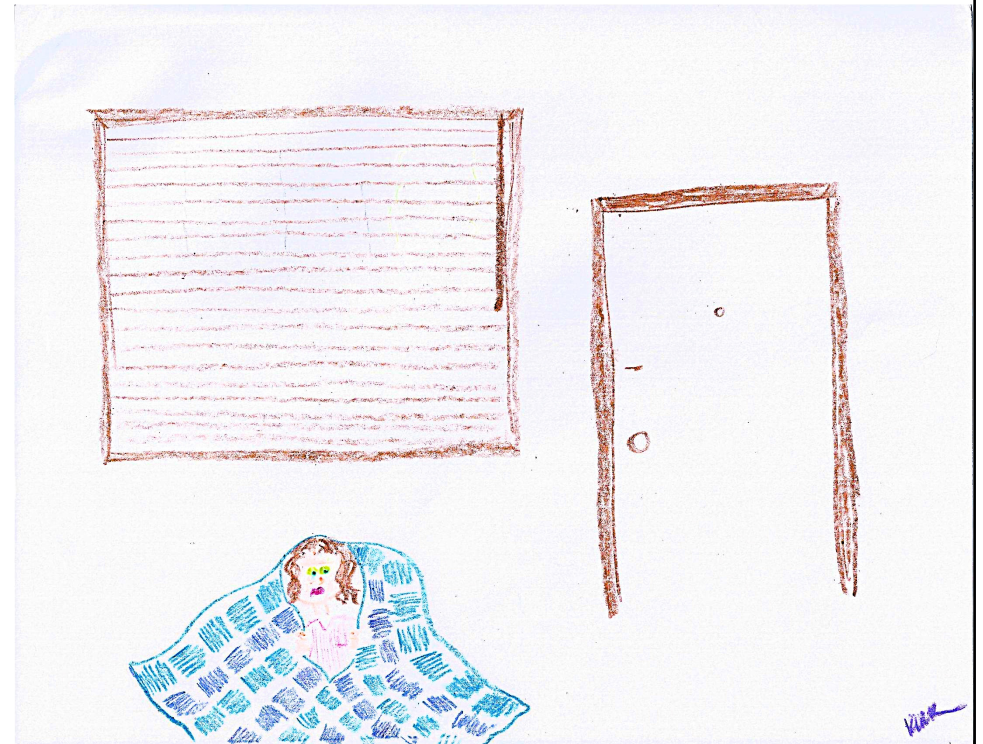
– Mori, age 26

# CEILING

This is my room.



This is me under  
the covers.



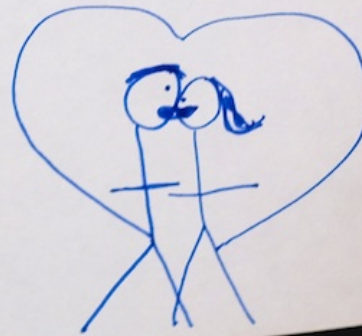
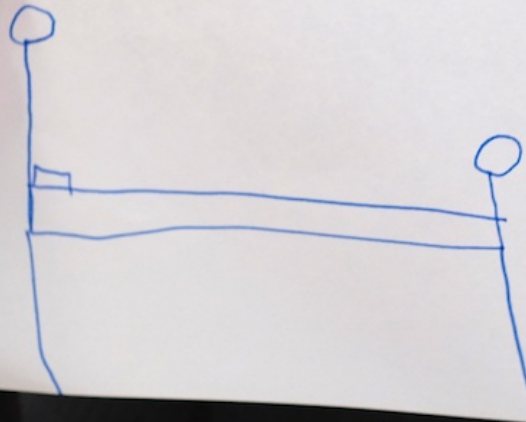
My drawing shows physical and emotional privacy. The blanket symbolizes a barrier to openness.

– Kelly, age 36



Ava 8 years old

open up!



Danette age 8



mom nicole  
is bothering

stop nicole







It is a women changing clothes. She is behind a privacy screen so no one can see her changing. – Alessa, age 32

TAYNSHAN W ✓

SPIDERMAN  
NEEDS  
PRIVACY  
TO PUT HIS  
COSTUME  
ON.

SIDORE



Sally, 5

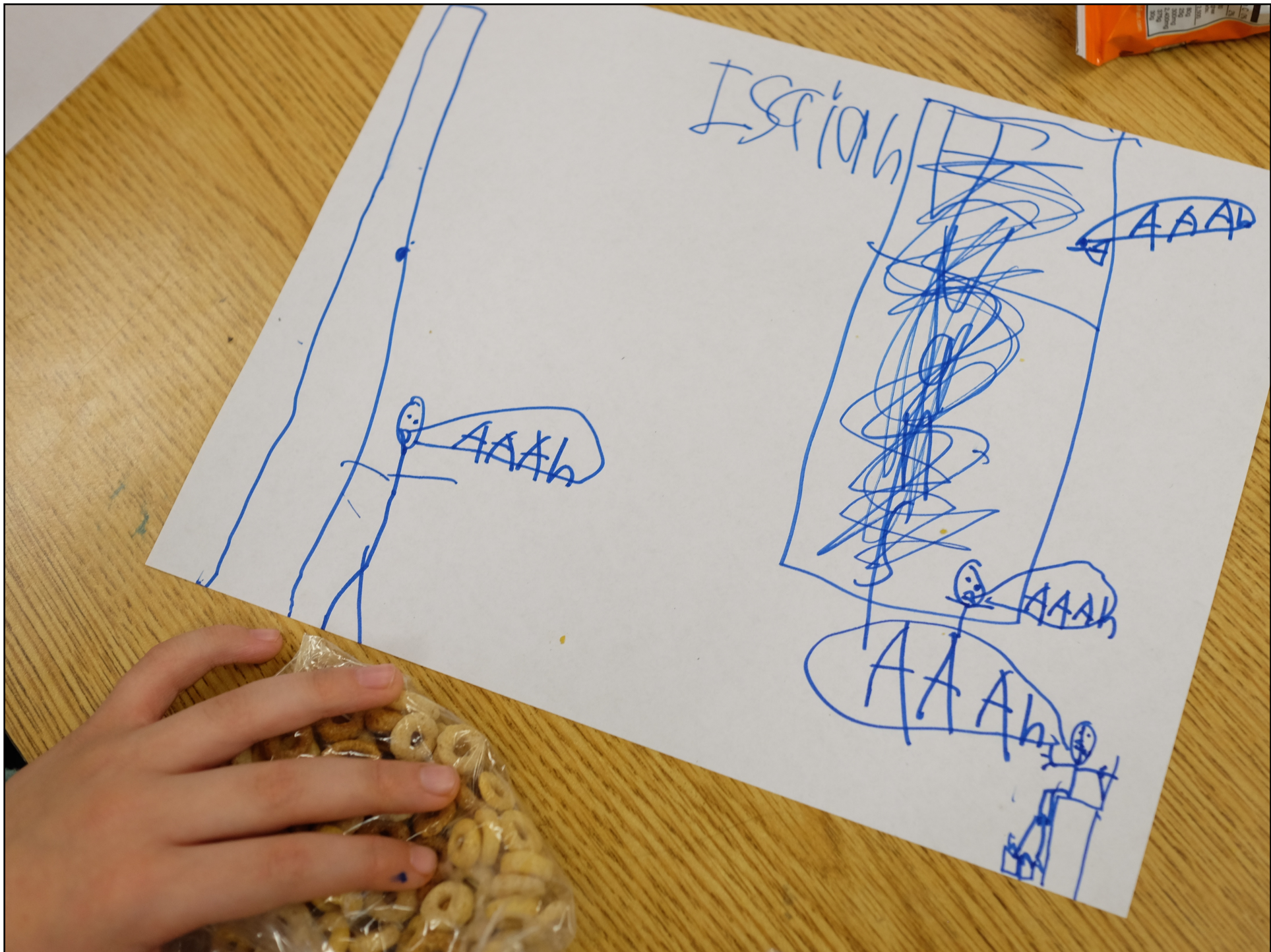


Someone going to the bathroom.

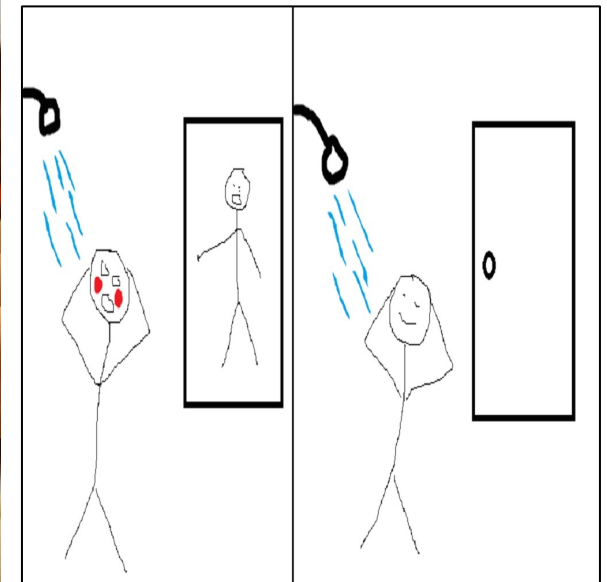
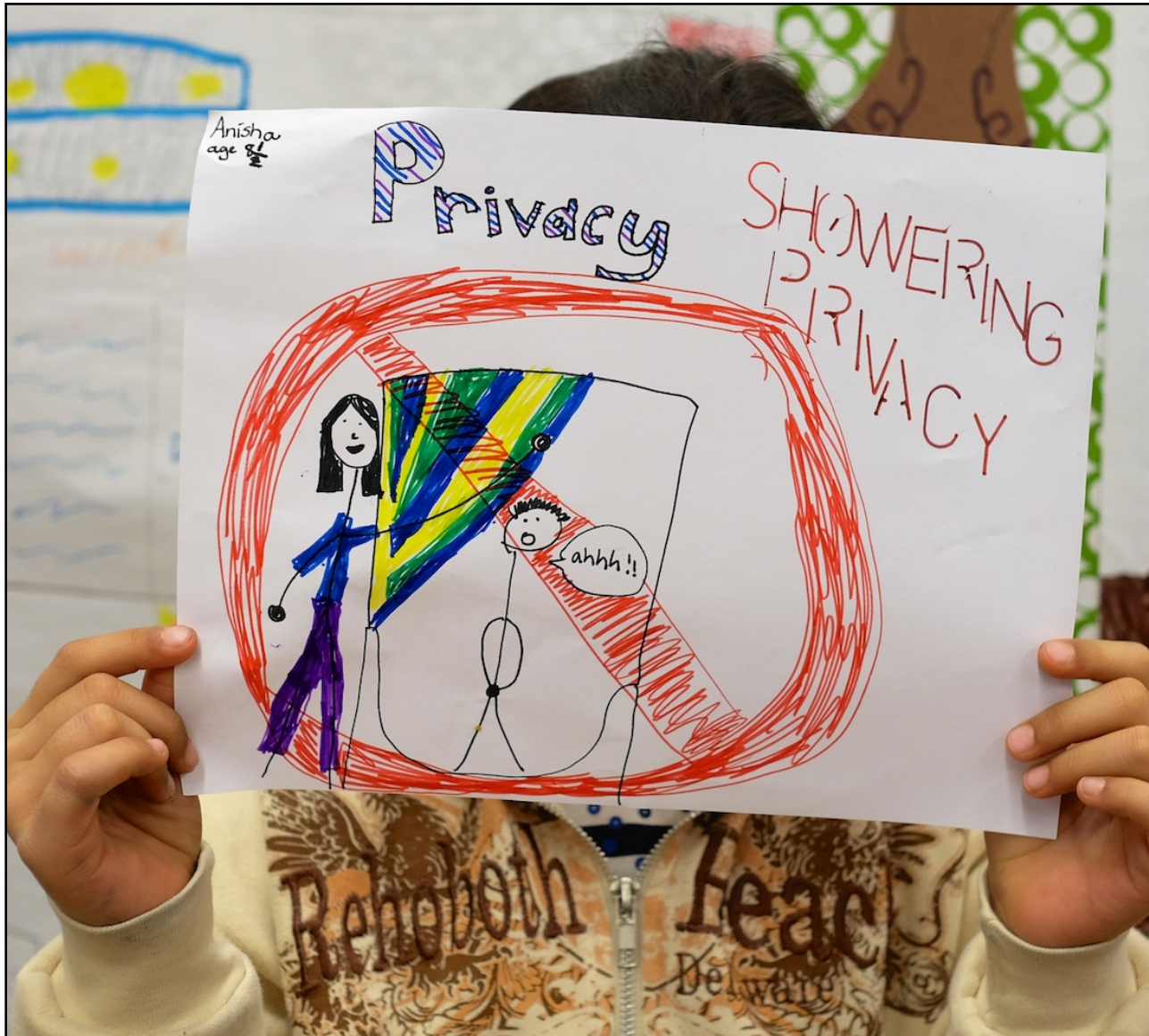
My kitty in the bathroom.

PRIVACY  
PRIVACY









Privacy means I can do things and not face public ridicule or judgment. Like taking a shower, who wants to have an audience while taking a shower? – Chris, age 37

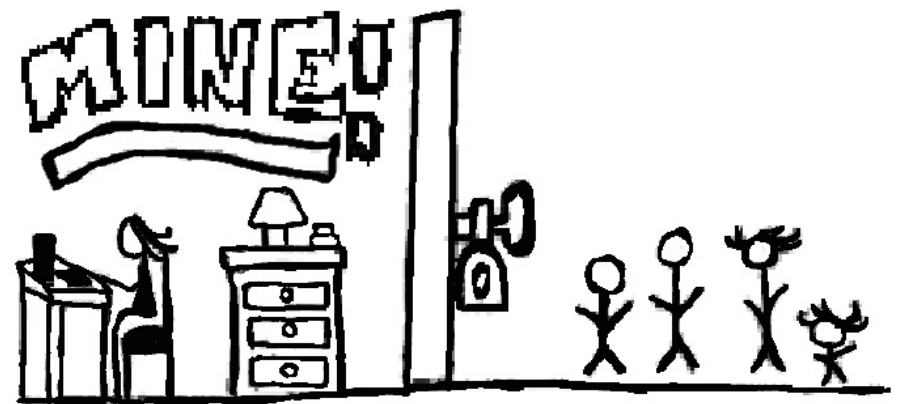


This is me enjoying my privacy. This is the only time during the day, where I am truly alone and nothing bothers me. No man, no children, no dogs.

– Cindy, age 54

I have four children, two of which I share a bedroom with. Privacy, to me, is to have a space to yourself that no one is allowed in to keep whatever it is you want to keep for yourself.

– Karin, age 26



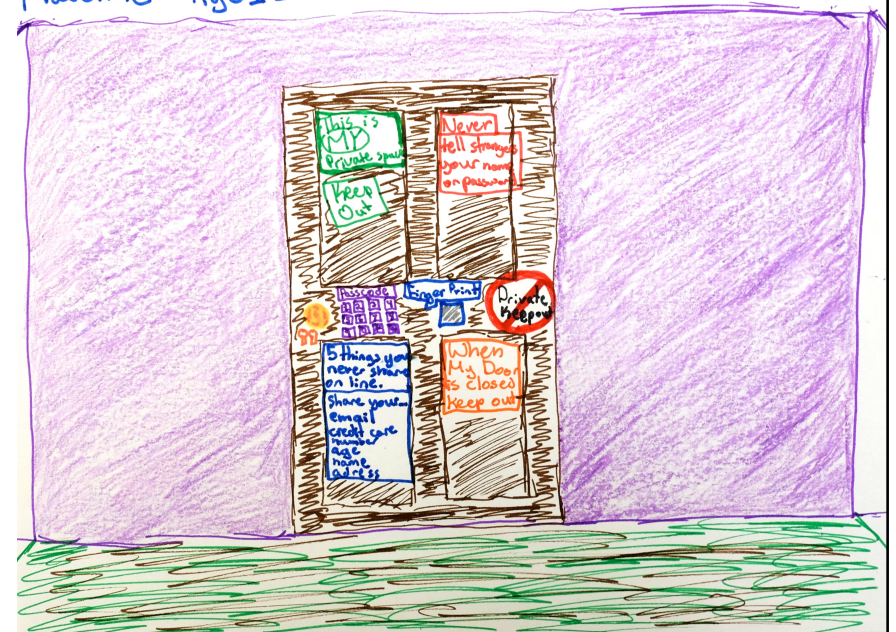




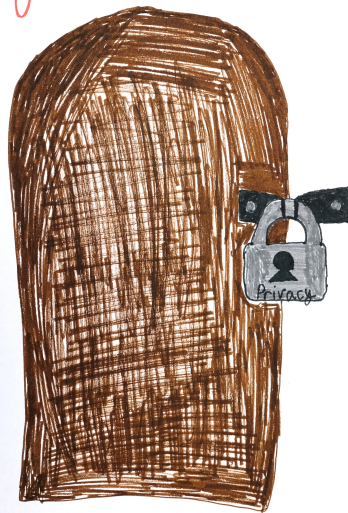
My room. Door is closed.

LOAFLET

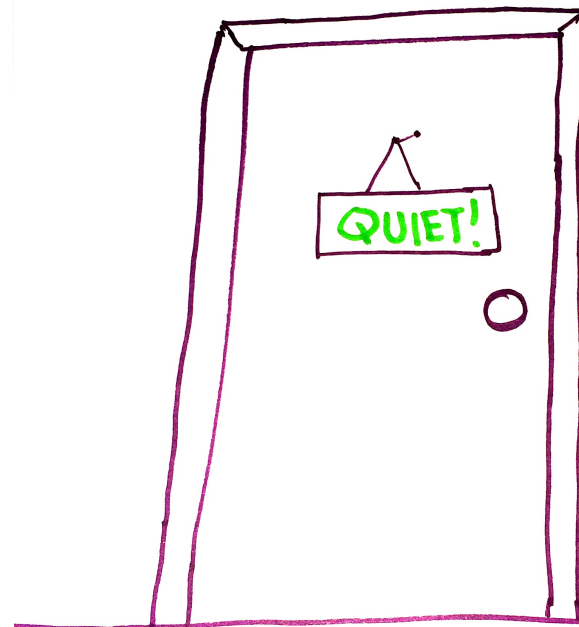
Madeline Age 11



Privacy Protects Whats



Behind Closed Doors  
Patricia 16



I feel privacy is behind this closed door. No one can hear you or see you and you can be alone with your thoughts.

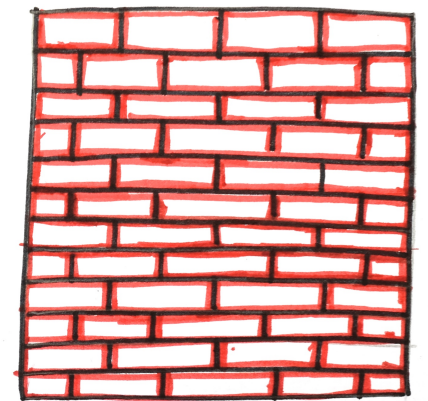
– Tracy, age 34



I believe a fence is a sign of privacy. This picture shows enough of my house to show that I don't mind some people to see me, but I prefer a barrier when it comes to some things.

– Shanna, age 32

Ryan [redacted] 18

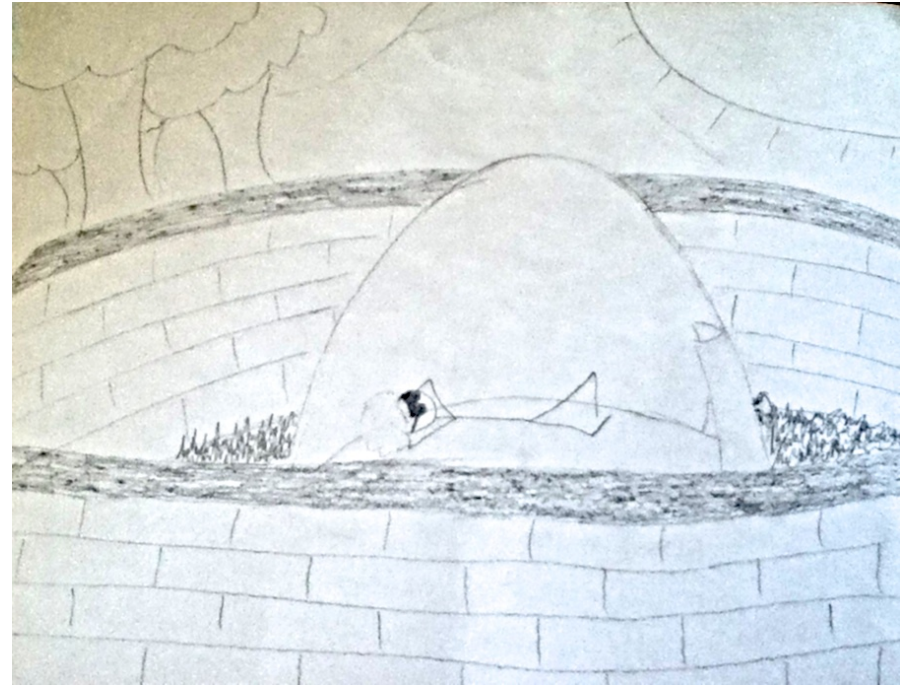




Nasmi  
age 9

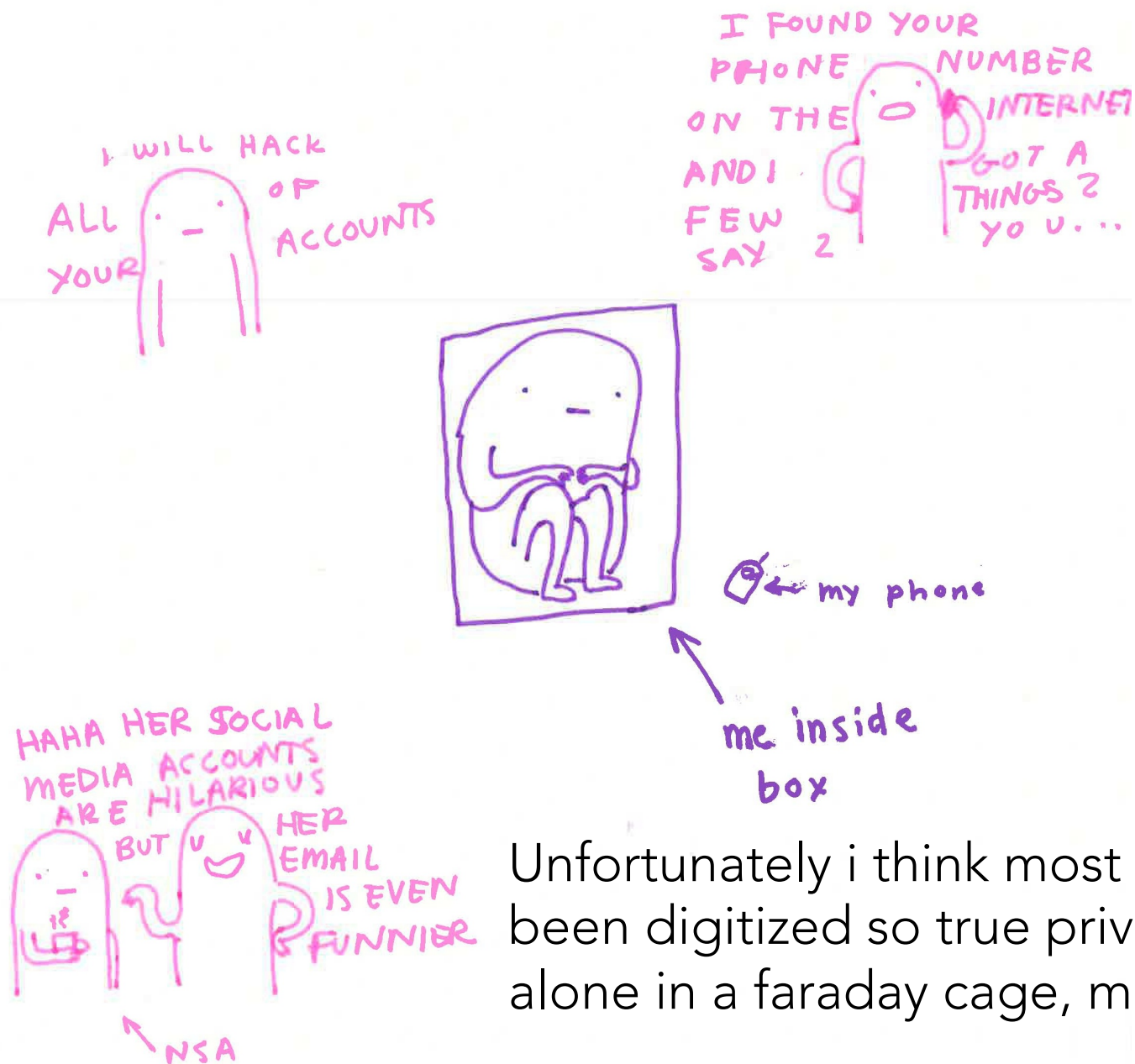
# PERSONAL BUBBLE

(Privacy project)



Privacy for me is like a place with a one-sided mirror. I can see outside but no one can see in unless I open the door. Also an extra wall on the outside just in case.

– Kim, age 21



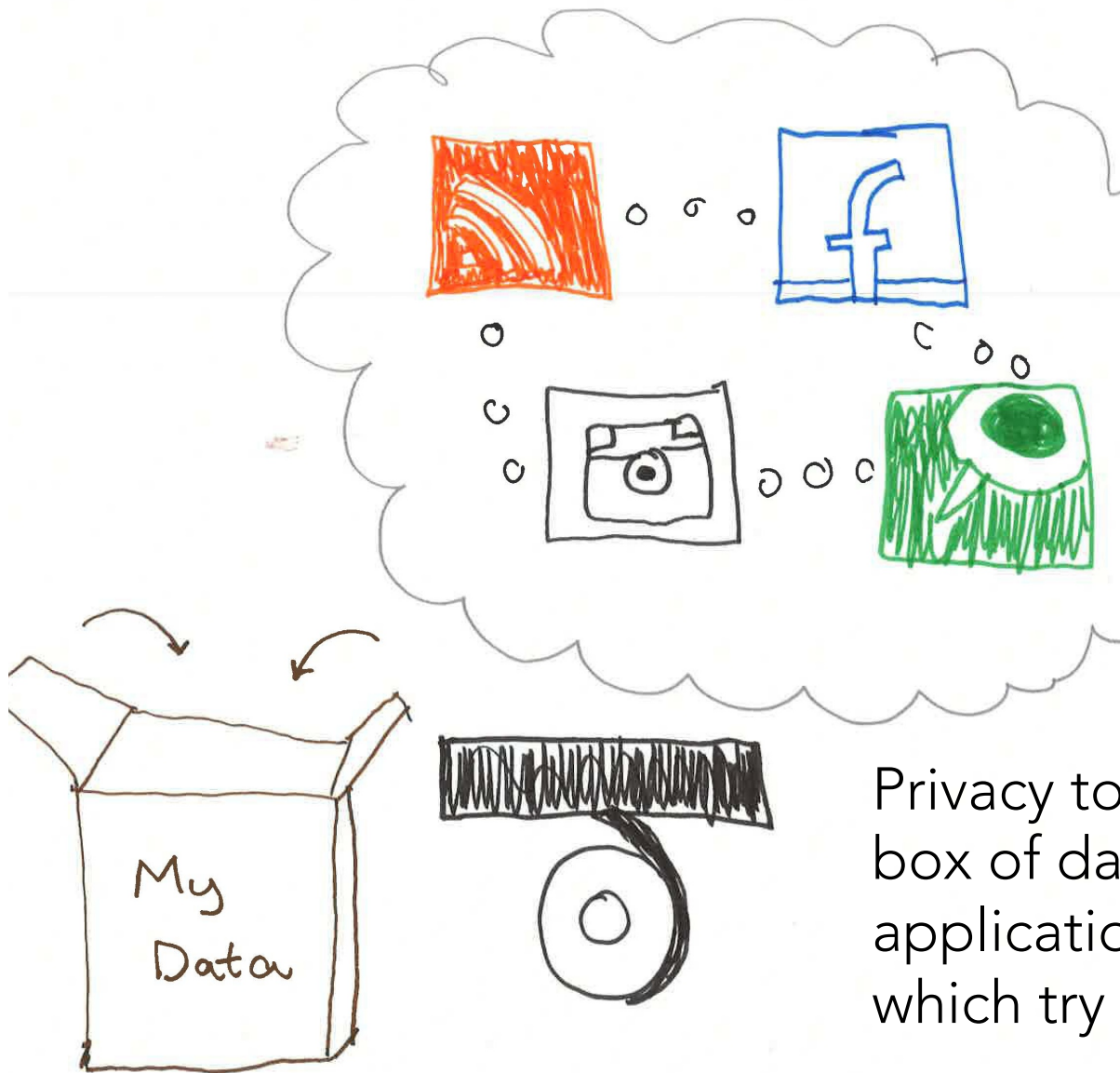
Unfortunately i think most of my life has been digitized so true privacy would be me alone in a faraday cage, maybe napping.

– Maddy, age 20



It's a turtle huddled up inside its shell. – John



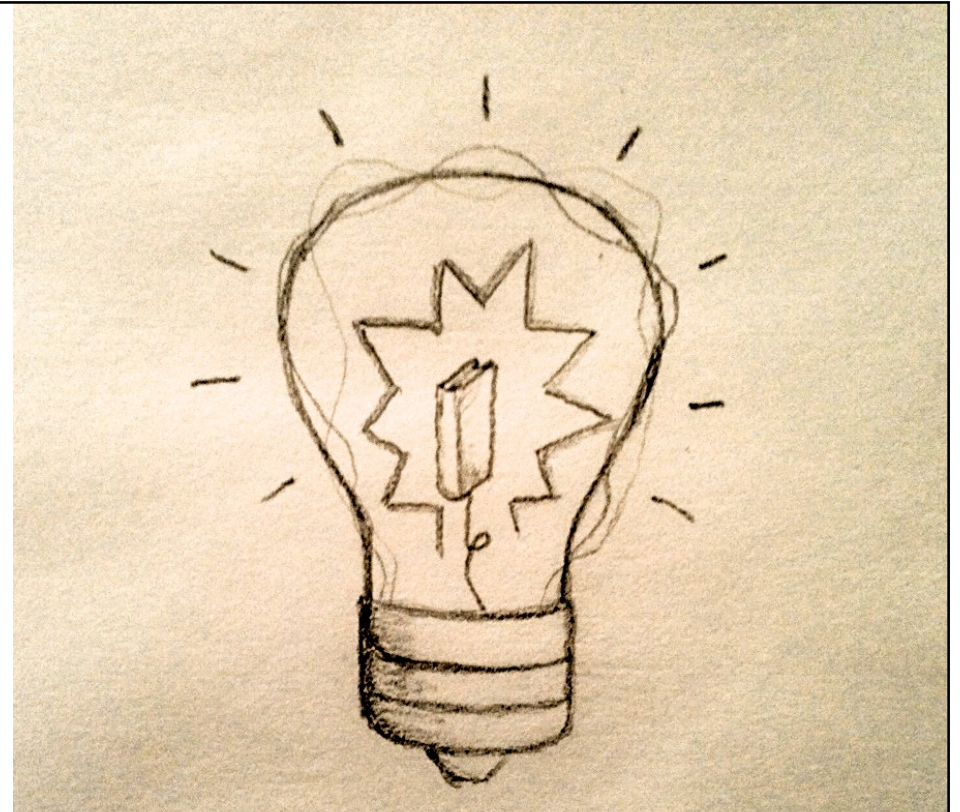


Privacy to me is sealing my box of data from web applications and services which try to collect it.

– Hana H., age 23

Privacy means that the thoughts in my brain are locked away.

– Thomas, age 19



This is a metaphor for the privacy of the thoughts in my head, although they radiate out you cannot get into it while its still working.

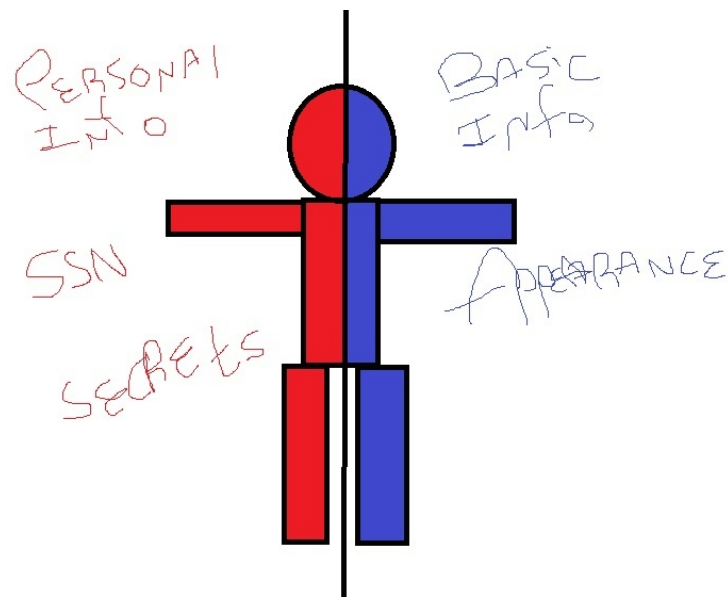
– Kay, age 25

# Control

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.

– Alan Westin,  
Privacy and Freedom, 1967



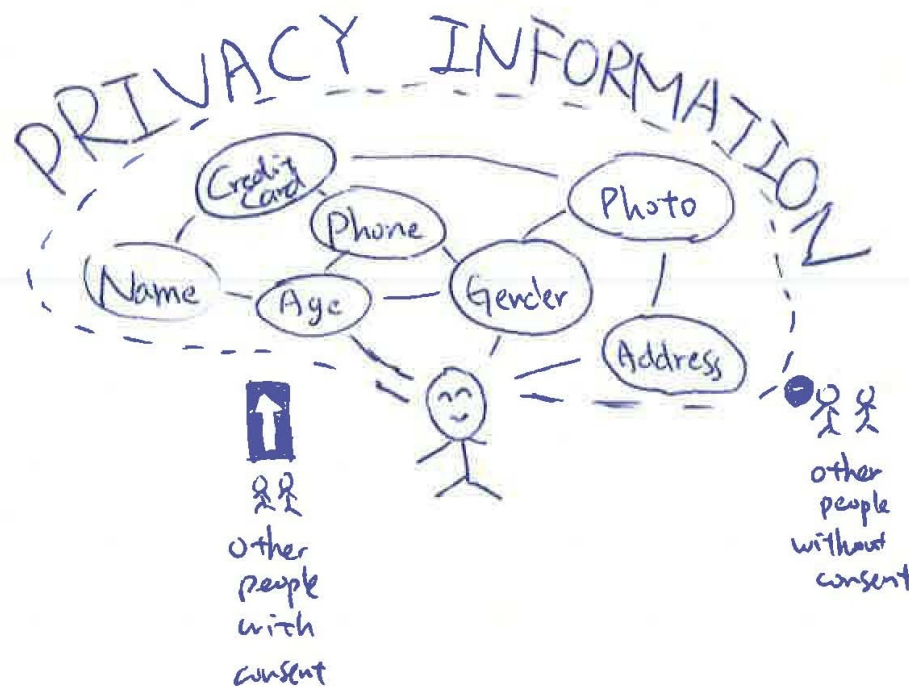


It is the difference between what the average person wants other people to see, and what they don't want other people to see. Privacy and personal protection separates those two things.

– CJ, age 20

I can decide who I'd like to share my privacy information!

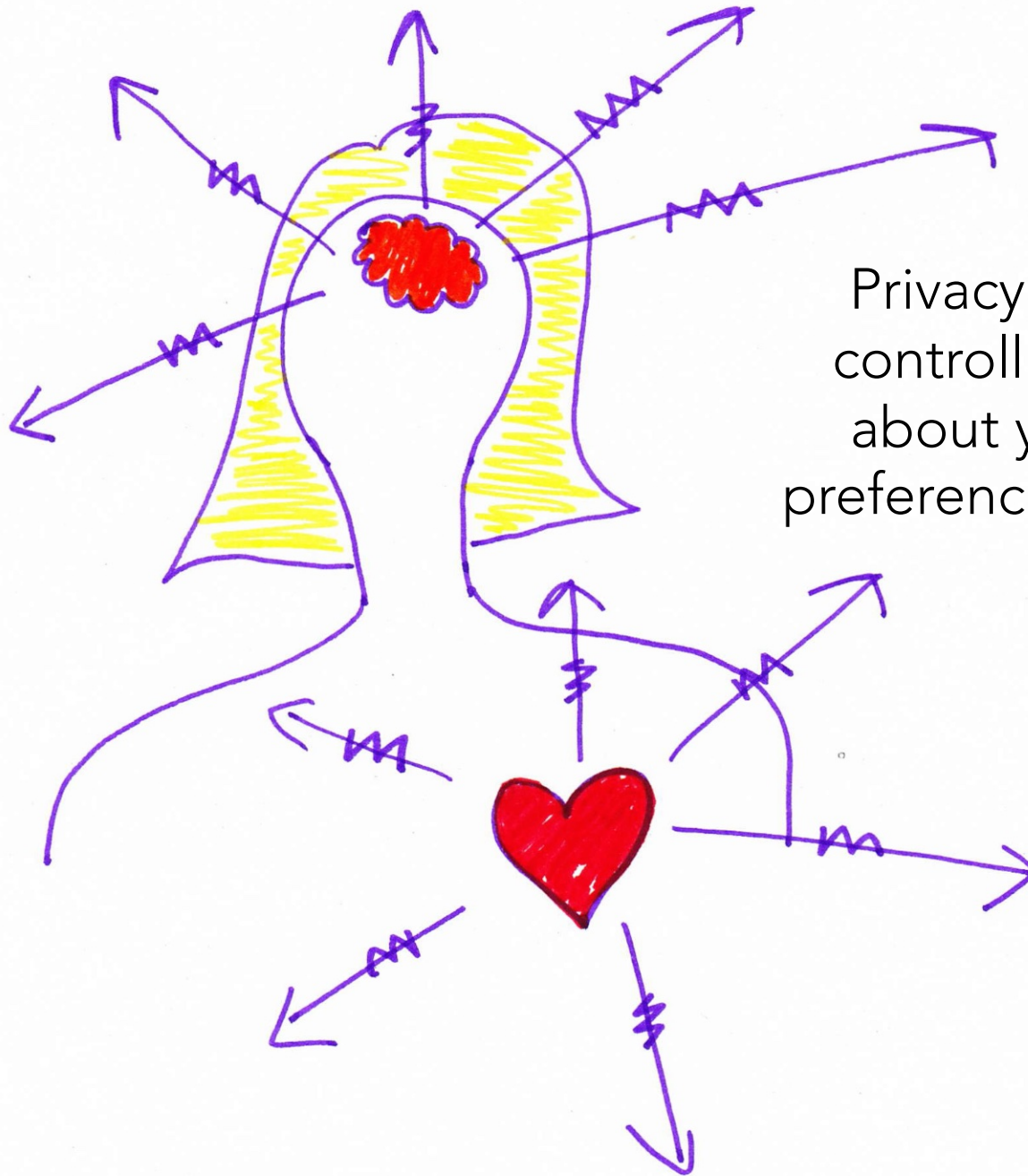
– H, age 26





– Allison Lefrak,  
Senior Staff  
Attorney,  
Federal Trade  
Commission  
Division of  
Privacy and  
Identity  
Protection





Privacy is about control –  
controlling what is shared  
about your thoughts and  
preferences, the things that  
make you you.

– KRB, age 39

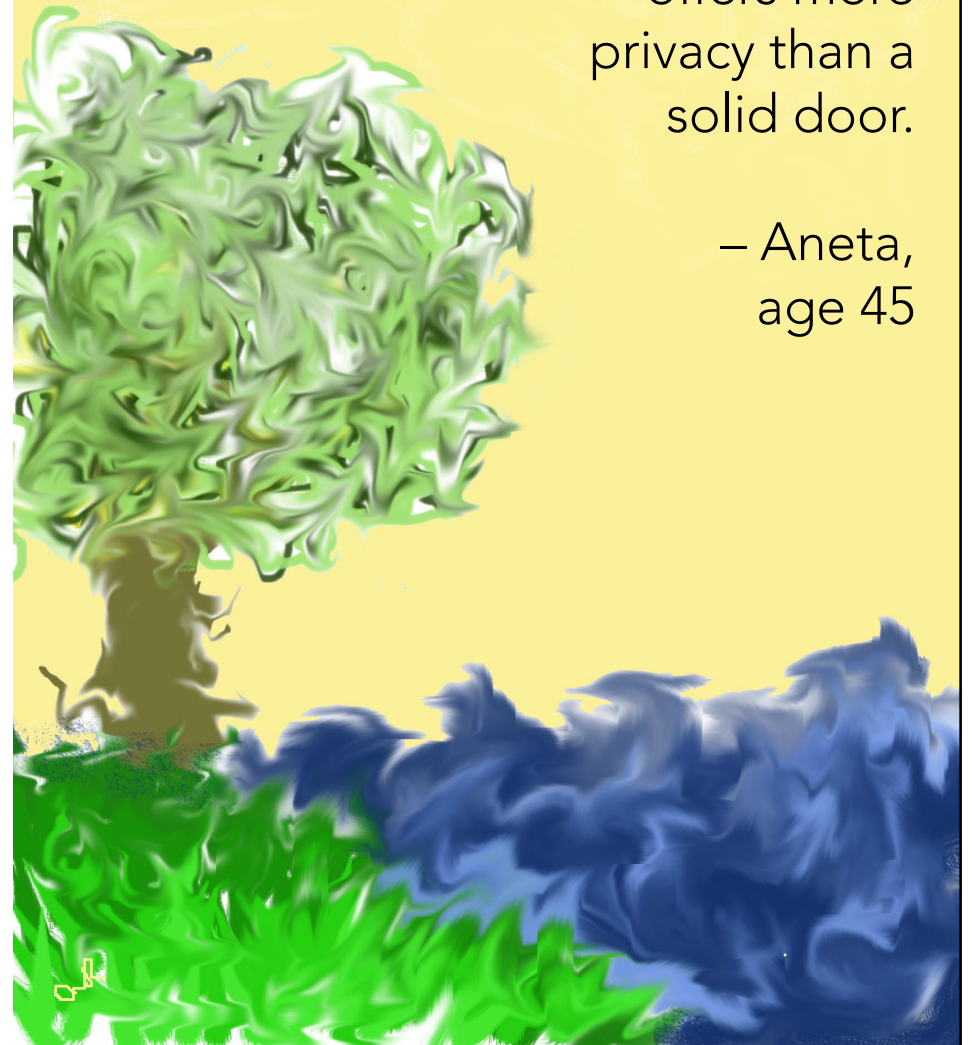
Sometimes the only way to have privacy is to just get up and leave.

– Paula, age 62



A curtain of rain  
offers more  
privacy than a  
solid door.

– Aneta,  
age 45



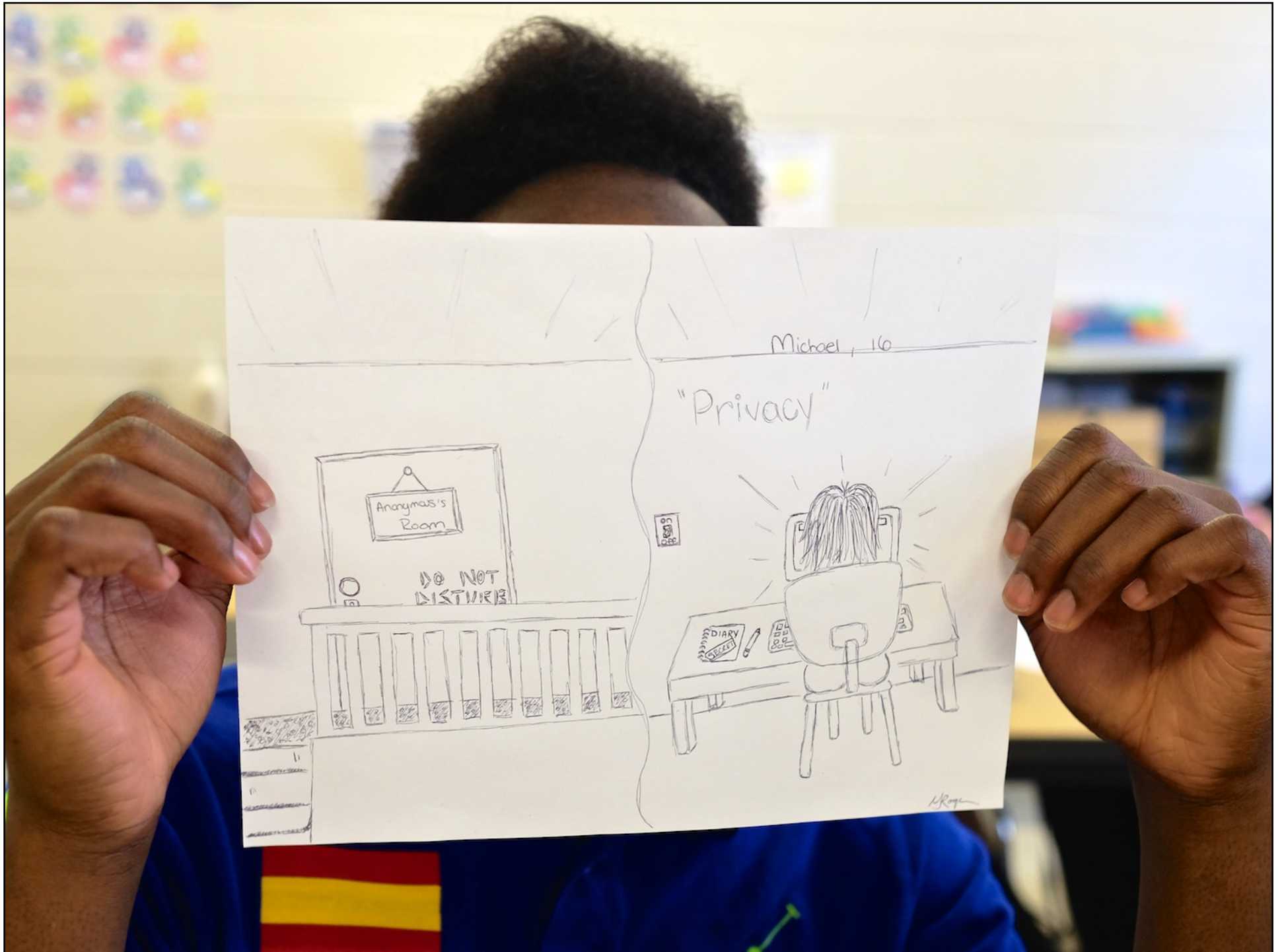


Alina Age 8

ALONE

TEXTING!



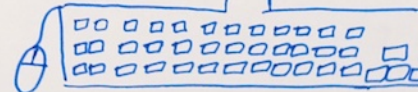
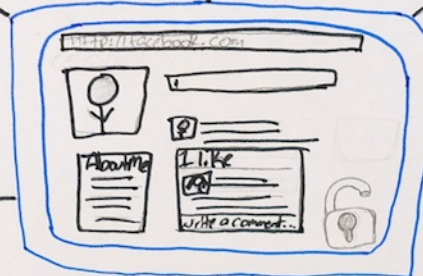




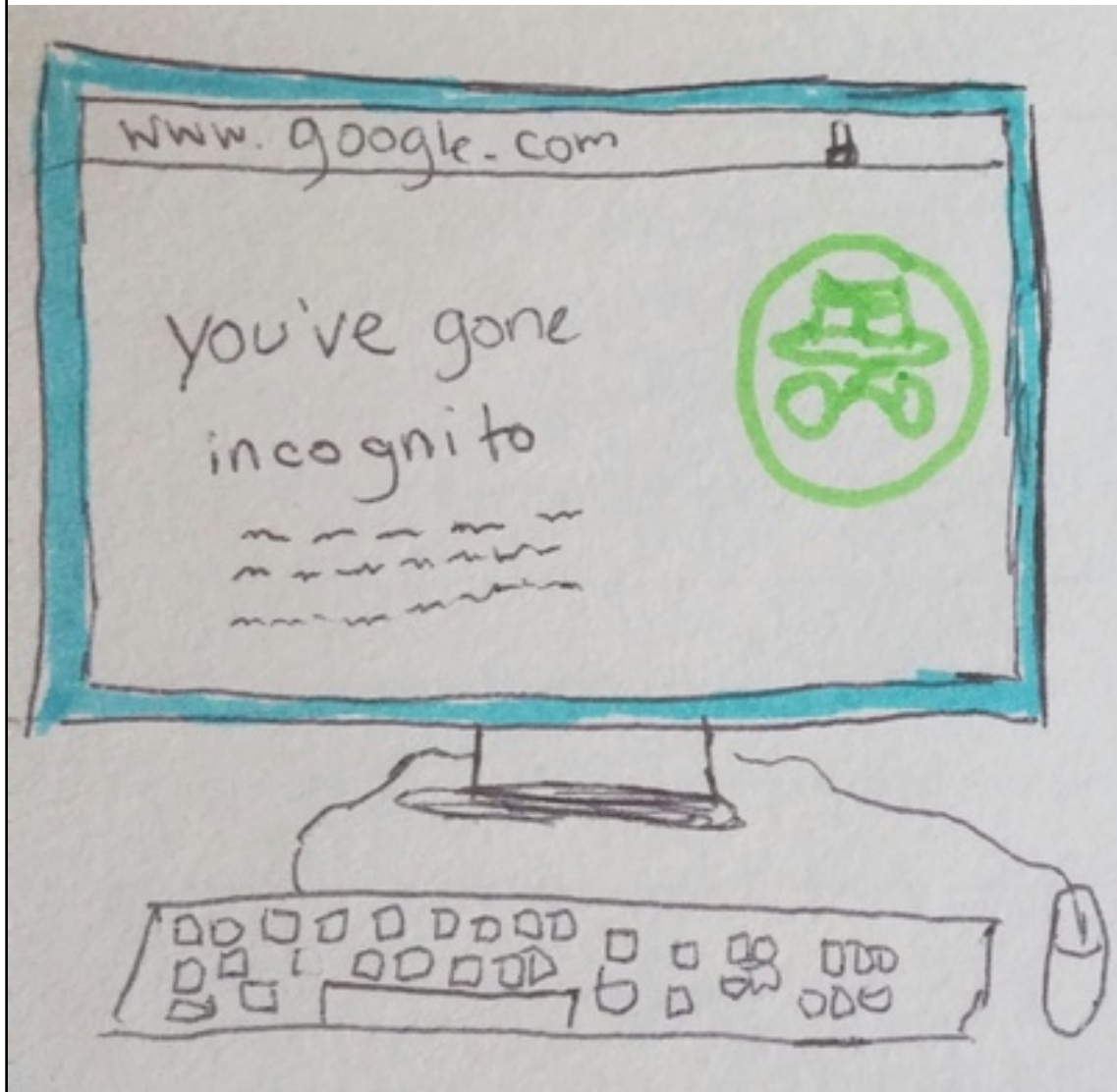
Jordyn, 16



...



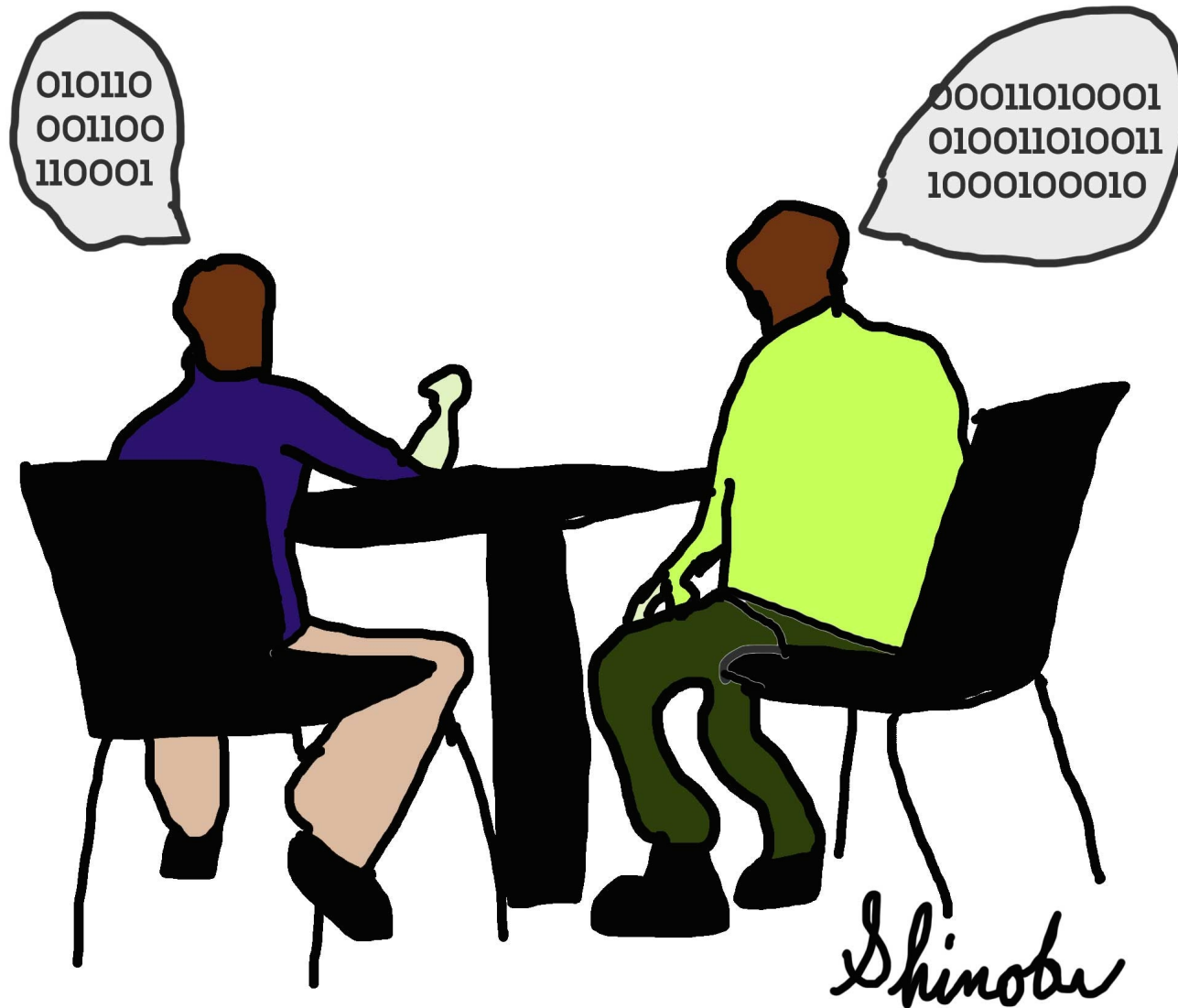
How many people can see what you're doing? Make your pages private!



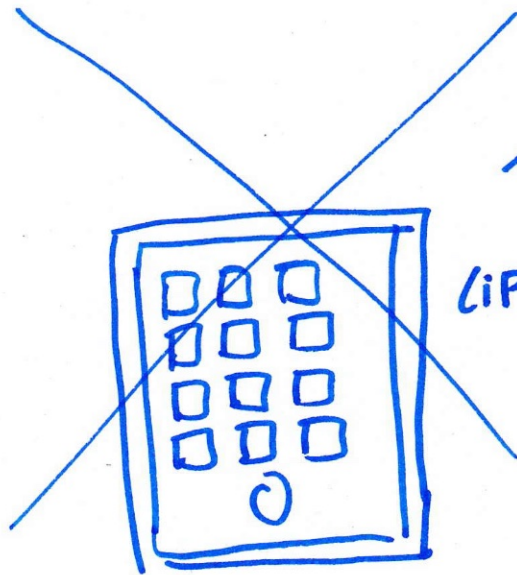
Privacy means having the ability to not be 'seen' online, to not be tracked or have all of your information remembered.... I think the 'incognito mode' on a browser helps with privacy because your history or cookies aren't tracked.

– George, age 18





... having a conversation out in the open, however, their language is being encrypted with binary code so other people can't tell what they are speaking. – Shinobu, age 24



(iPhone/iPAD)

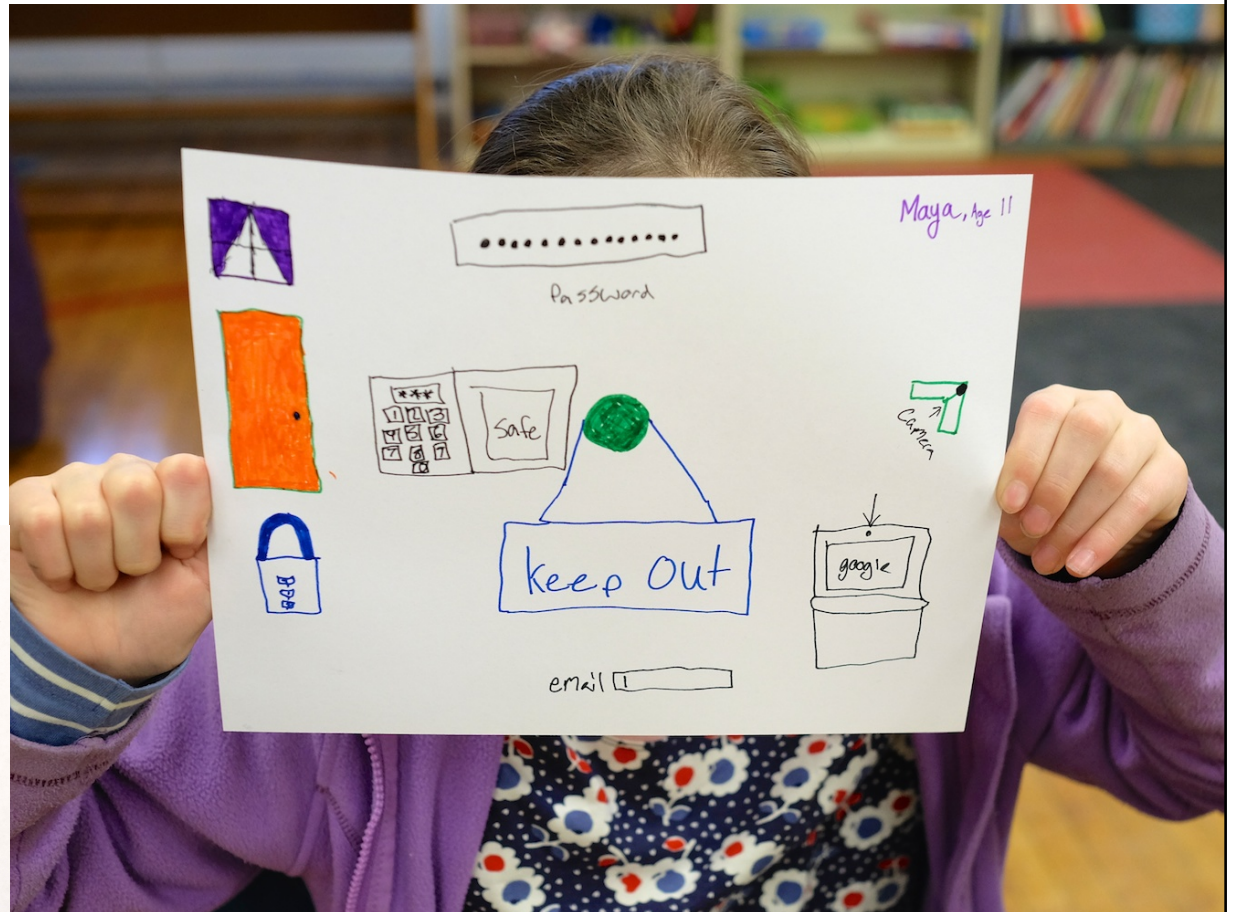
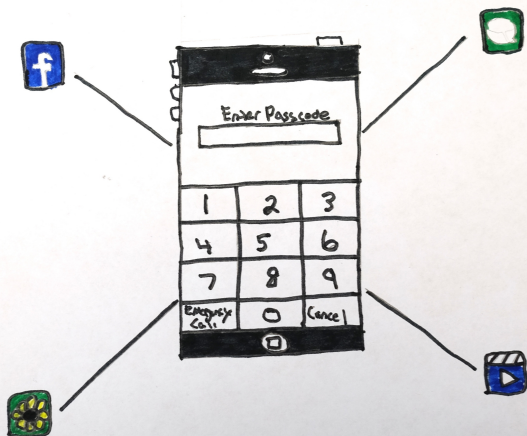
Privacy is protecting your  
devices that collect and  
store information.

–Sarah S., age 23



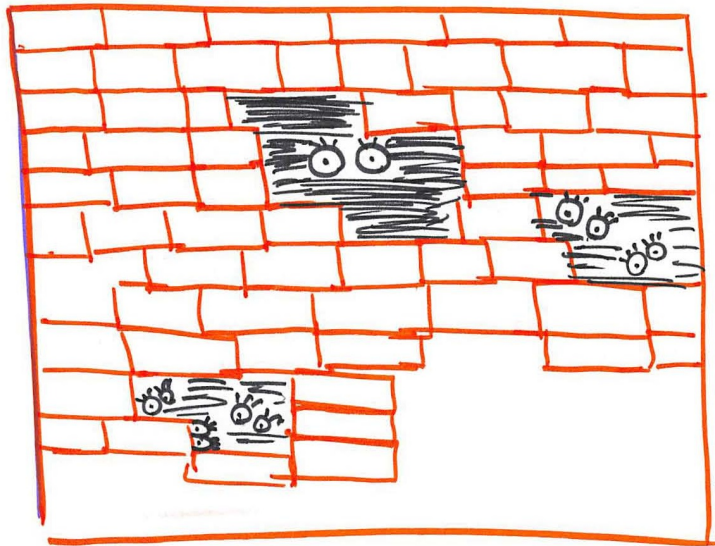
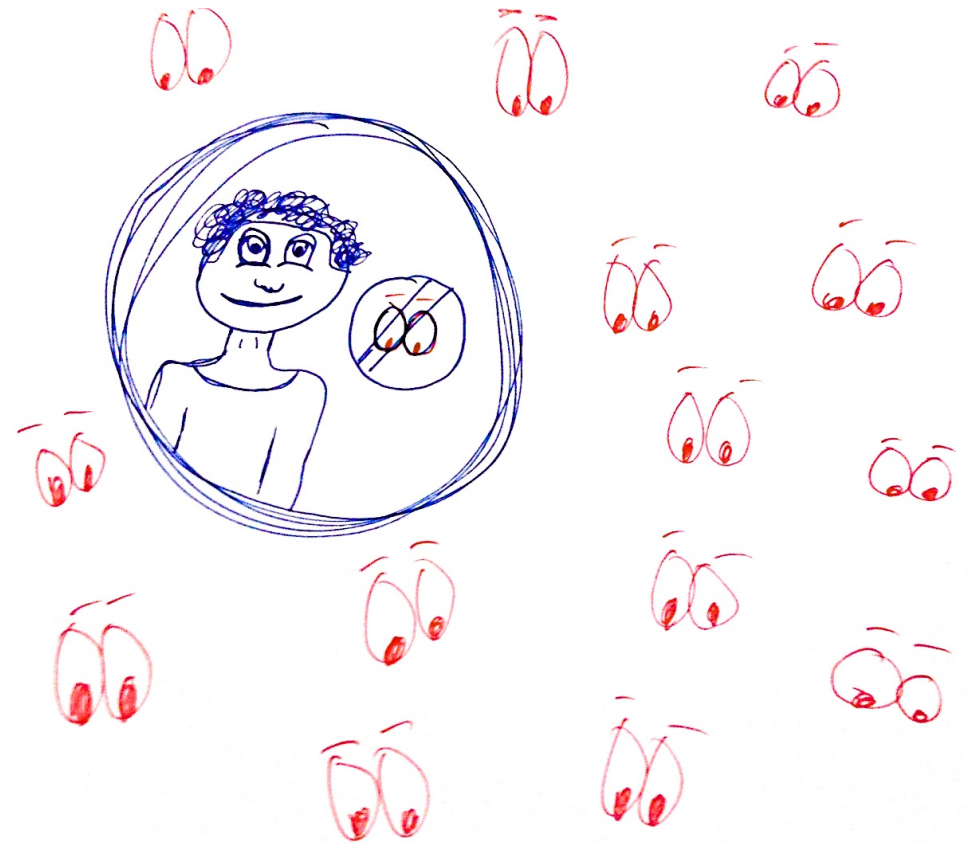


Doug 17







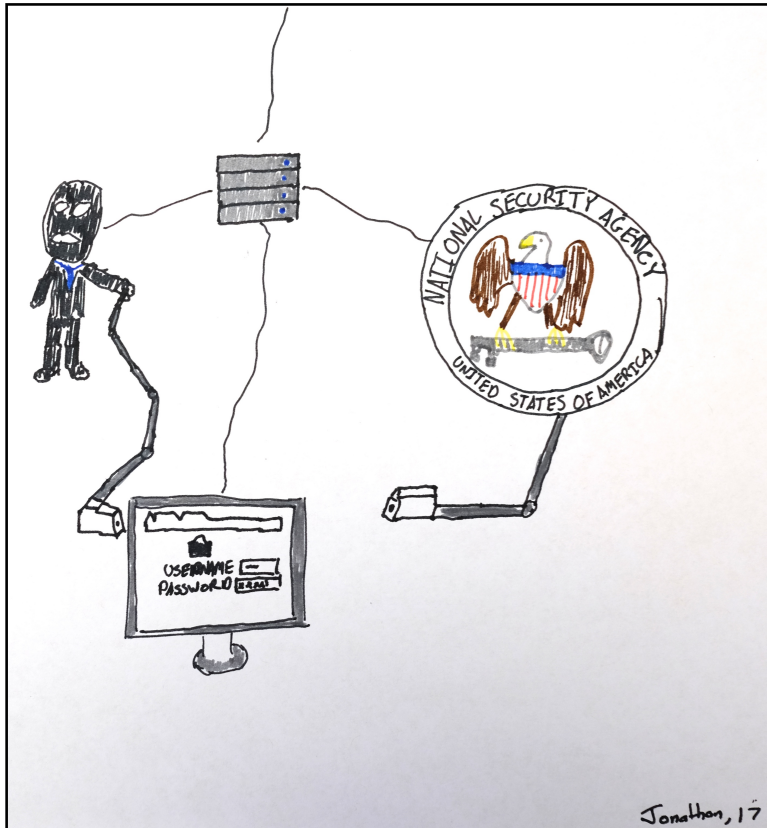


To me privacy means being able to get away from unwanted eyes.

– NotAnArtist, age 19



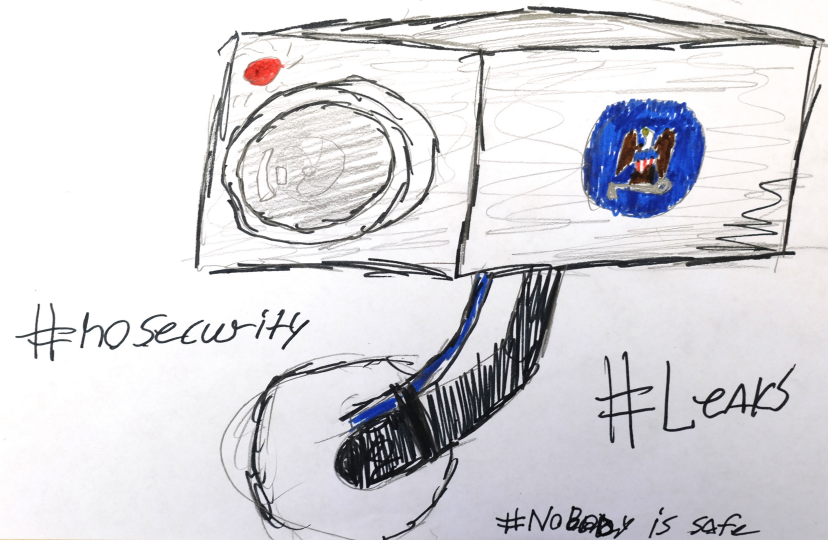




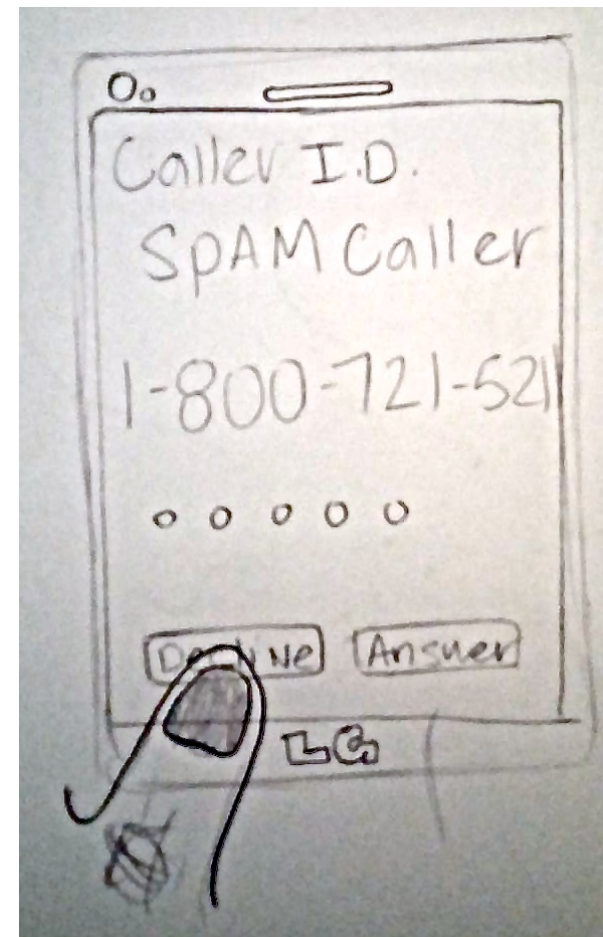
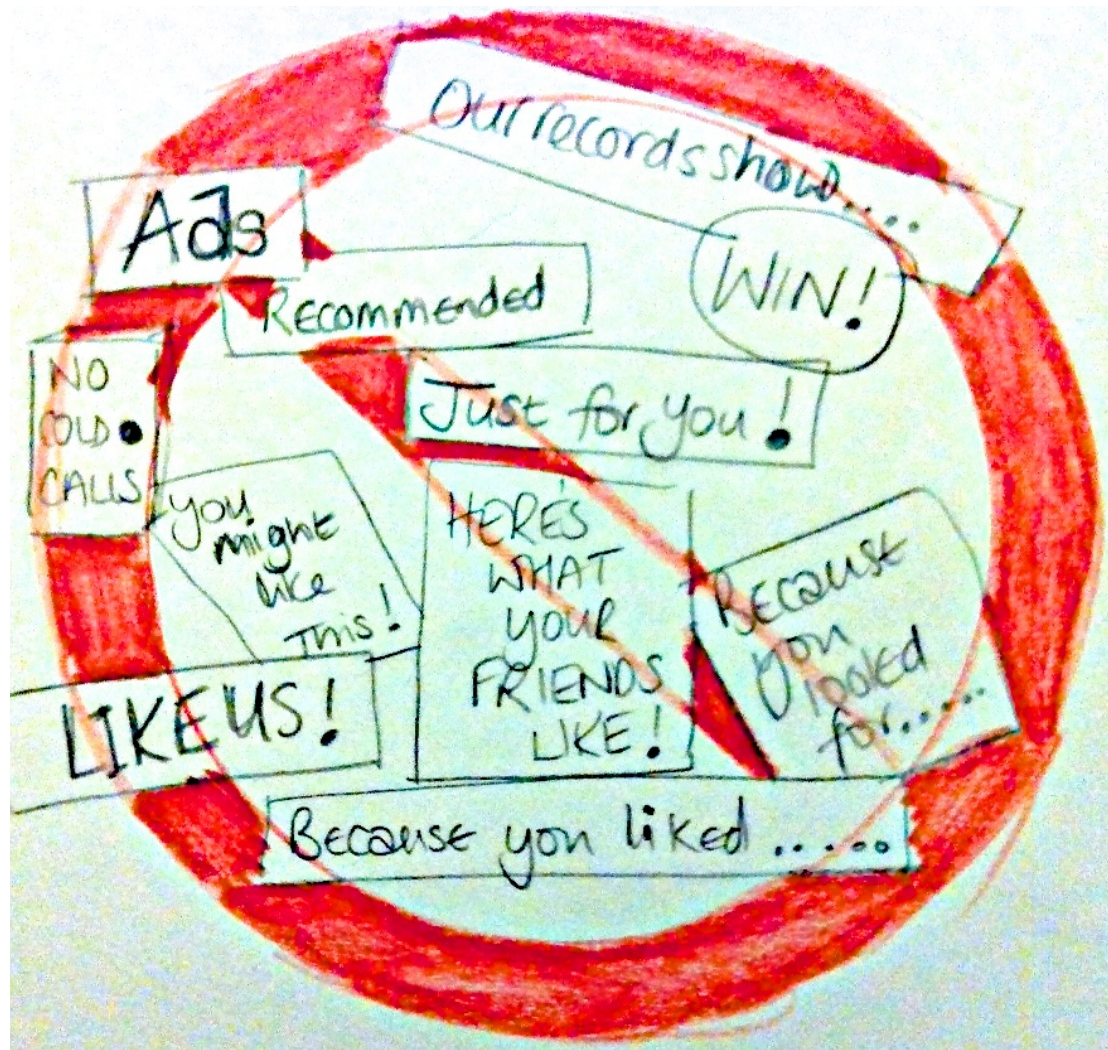
#TheFappening

ISAAC, 17

#StopTheNSA

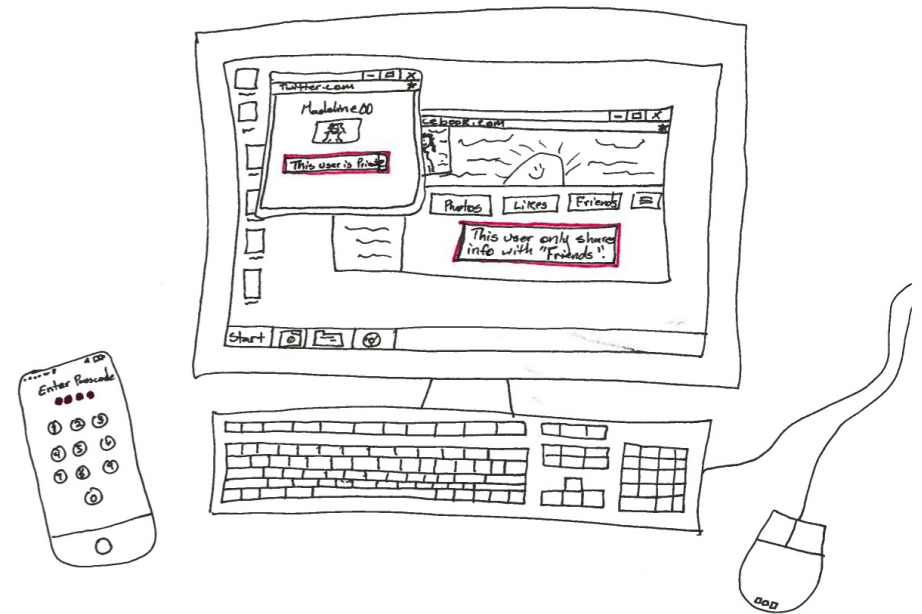






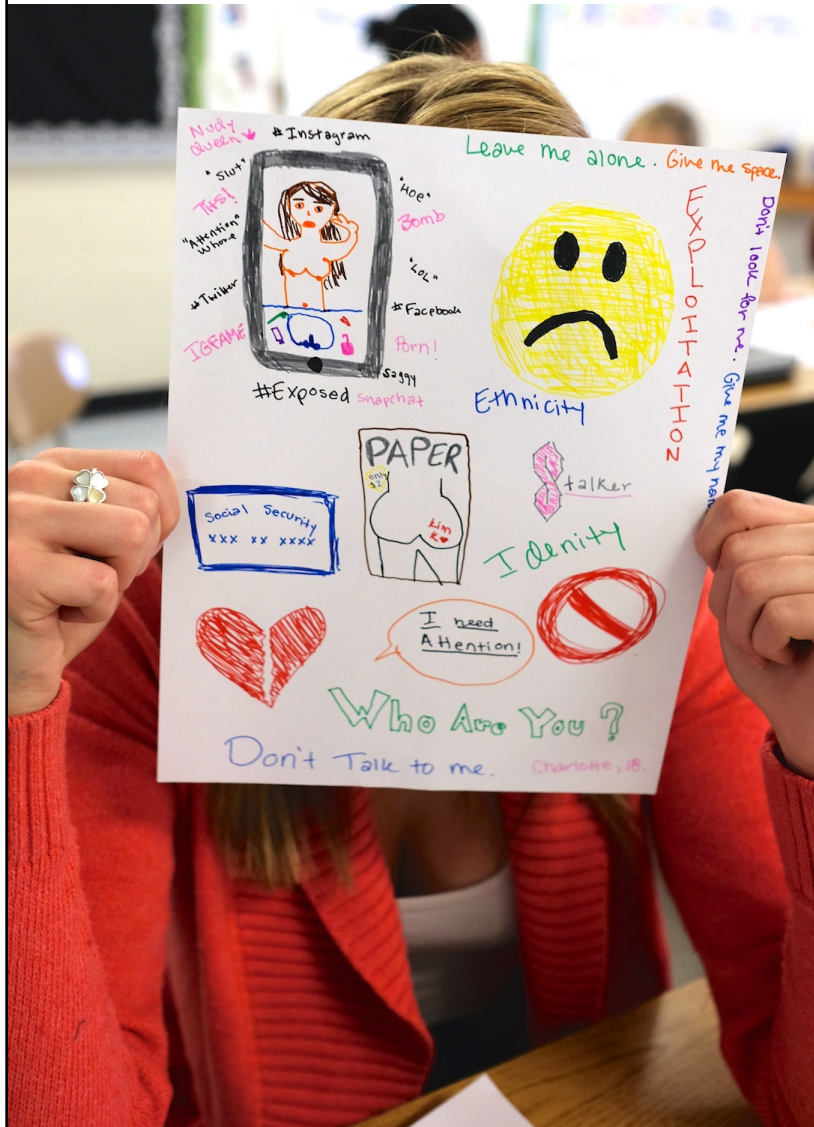
.... all the messages I see online every day that I feel invade my privacy and that I wish I could prevent. – Tiggy, age 52





My picture shows a computer with someone viewing social media sites. They can't see any private information due to privacy settings....

– Madeline 26

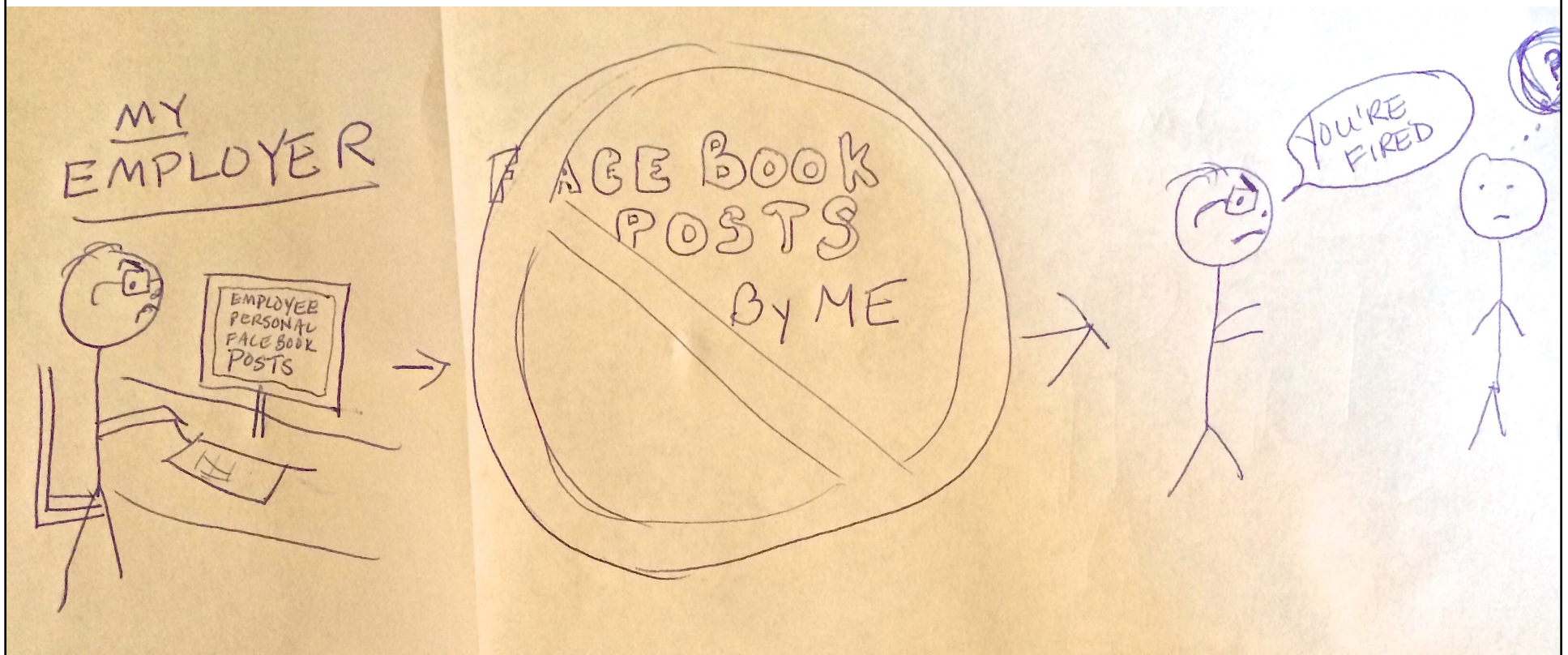


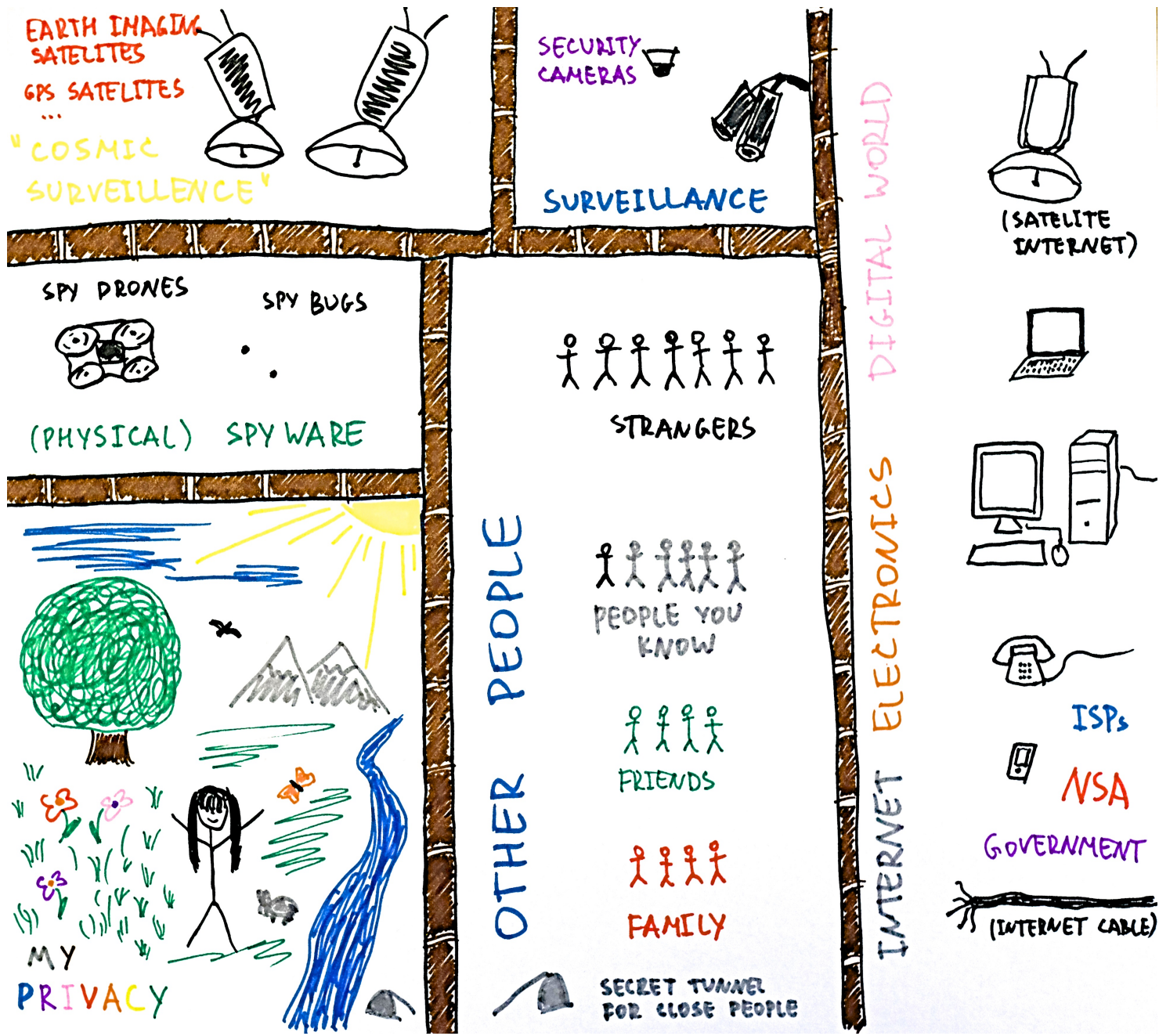
Private Parts Government  
 Dating / Home Life  
 What you do on the computer  
 Texts  
 Grades  
 Thoughts  
 Sexual Preference  
 Secrets  
 Wiring  
 Phones  
 Social Media  
 Relationship Status  
 Your House



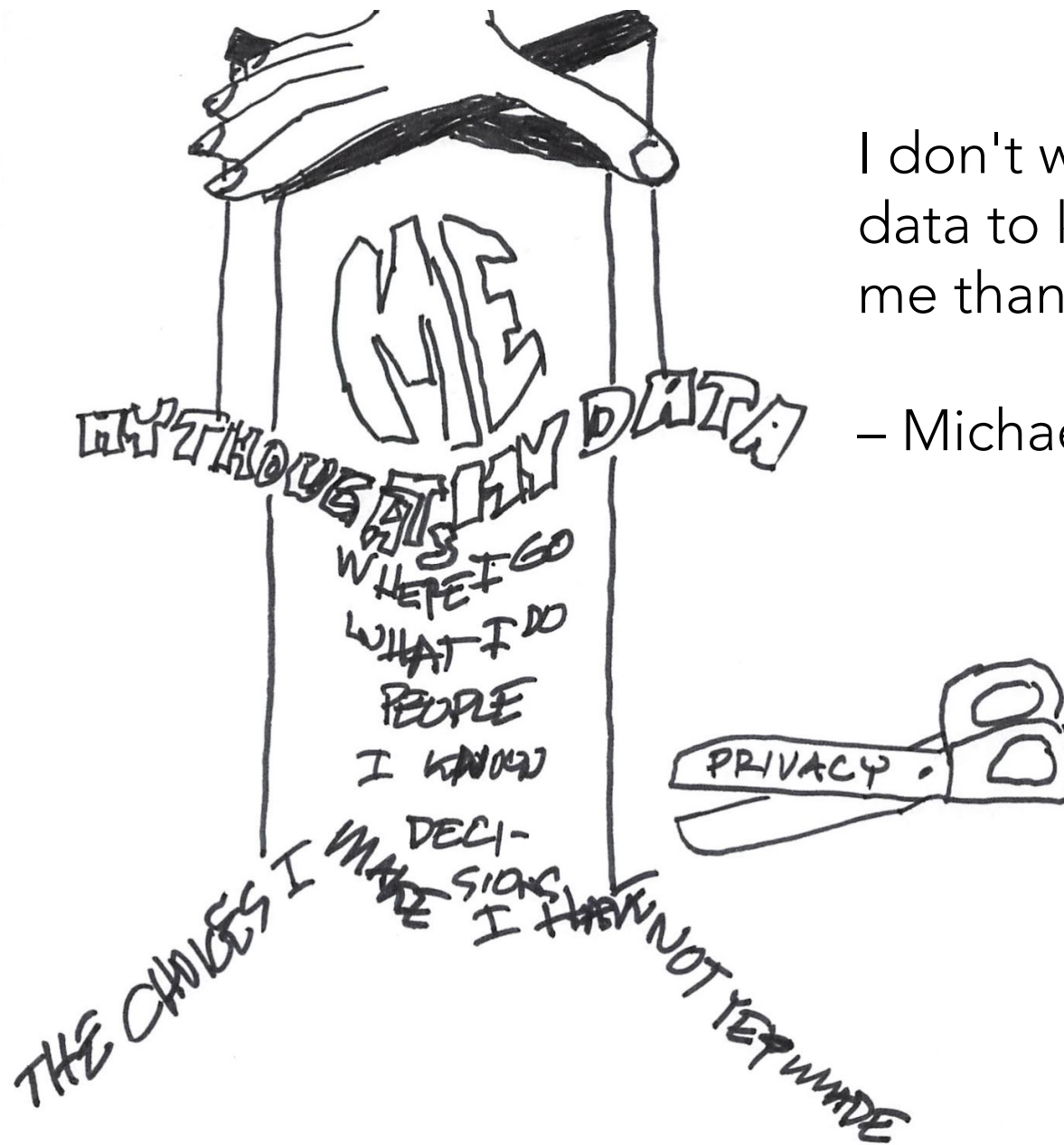
Lexie 17





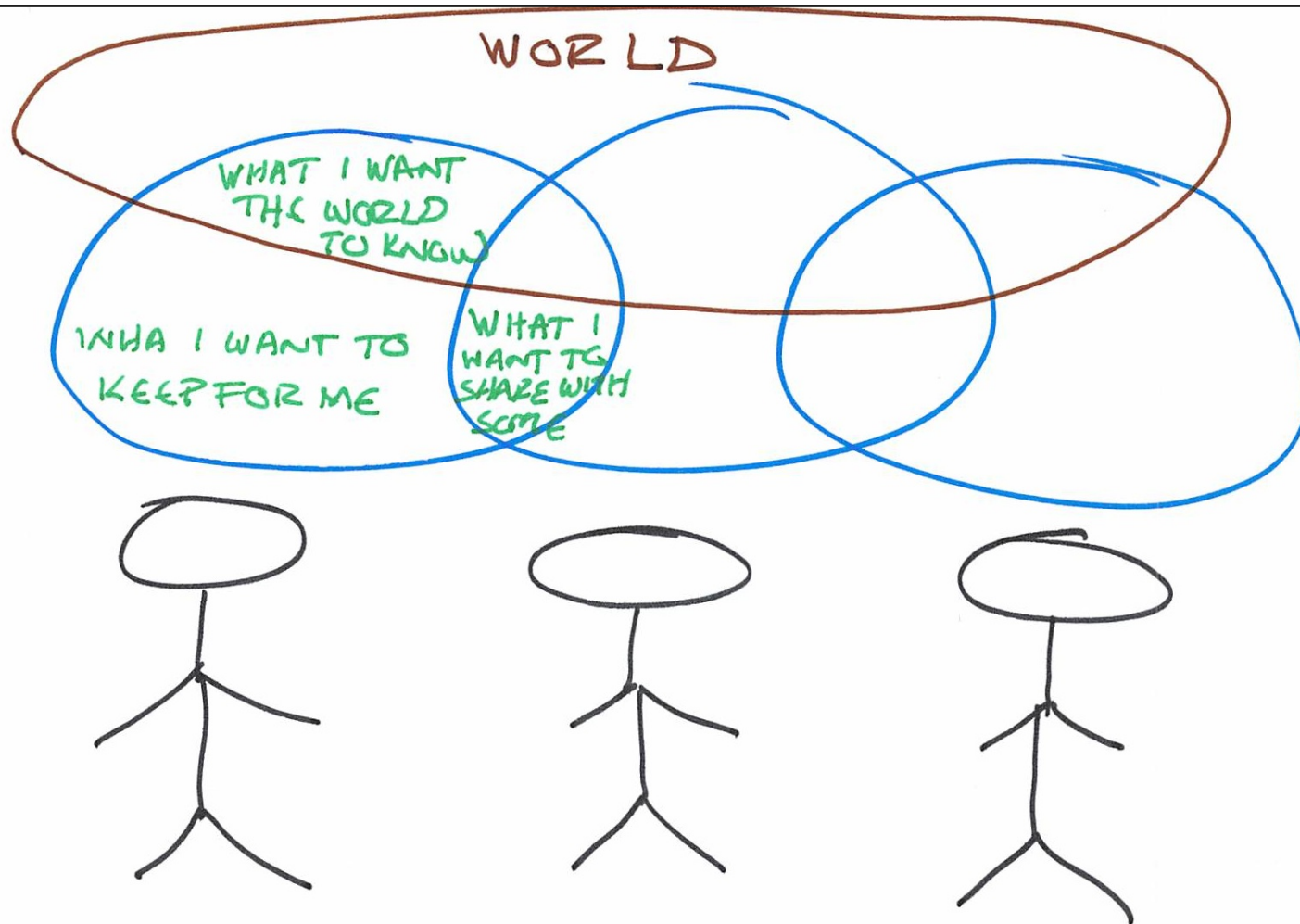






I don't want my collected data to know more about me than I do.

– Michael Farb, age 42



PRIVACY IS PERSONAL, CONTEXTUAL,  
AND UNIVERSAL

Privacy is a value that is very important to have in a society to work and progress – Pedro Leon, age 35





You will never outgrow  
your need for privacy!

– Gladys Lipton, age 91

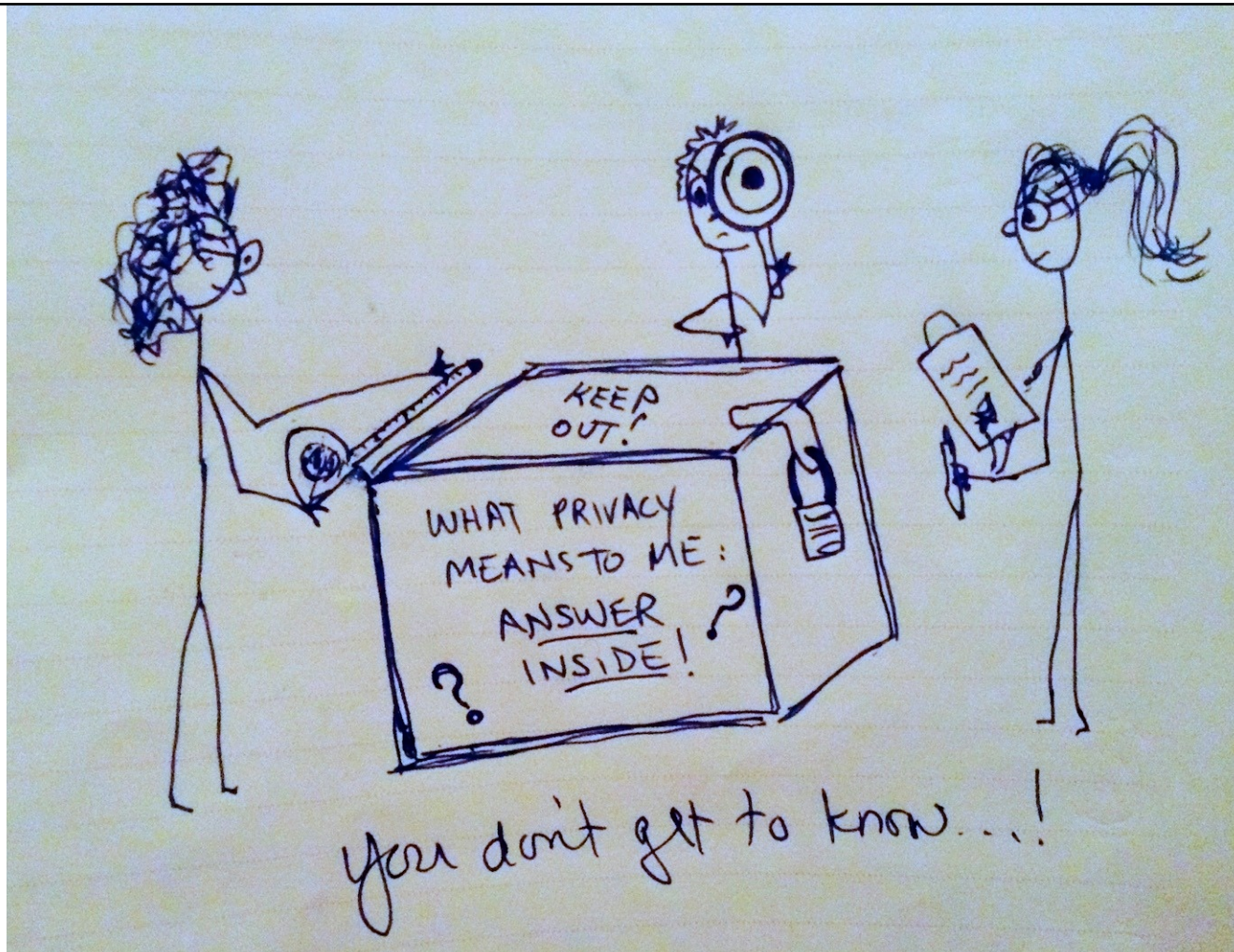




You have zero  
privacy anyway.  
Get over it.

– Scott McNealy,  
CEO of Sun  
Microsystems, 1999





It's a box containing the answer to "What privacy means to me." You researchers are measuring it and studying it, but can't actually get the answer, because it's PRIVATE.  
ha ha.... – Heather, age 44





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



## 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).

# Limited access to self



“Being alone.”

- Shane (age 4)

“the right to be let alone”

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

“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

# How does each goal relate to privacy?

*I want to have... I want to be....*

- Solitude, uninterrupted
- Unseen, unheard, unread
- Not talked about
- Not judged
- Not profiled, not targeted, not treated differently than others
- Not misjudged
- Free to try, practice, make mistakes, self-reflect
- Not surprised (contextual integrity)
- Not accountable
- Not required to reveal
- Unknown
- Forgotten
- Intimacy
- Control
- Boundaries
- Identity
- Security
- Safety
- Others?



# Measuring privacy

- Why is privacy hard to measure?
- Why are attitudes about privacy hard to measure?
- Why is the cost of privacy invasion hard to measure?

# How privacy is protected

- Laws, self regulation, technology
  - Notice and access
  - Control over collection, use, deletion, sharing
  - Collection limitation
  - Use limitation
  - Security and accountability



# Privacy laws around the world

- Privacy laws and regulations vary widely
- US has mostly sector-specific laws, minimal protections, often referred to as “patchwork quilt”
  - No explicit constitutional right to privacy or general privacy law
  - But some privacy rights inferred from constitution
  - Narrow regulations for health, financial, education, videos, children, etc.
  - Federal Trade Commission jurisdiction over fraud and deceptive practices
  - Federal Communications Commission regulates telecommunications
  - Some state and local laws
- European Data Protection Directive - EU countries must adopt similar comprehensive laws, recognize privacy as fundamental human right
  - Privacy commissions in each country

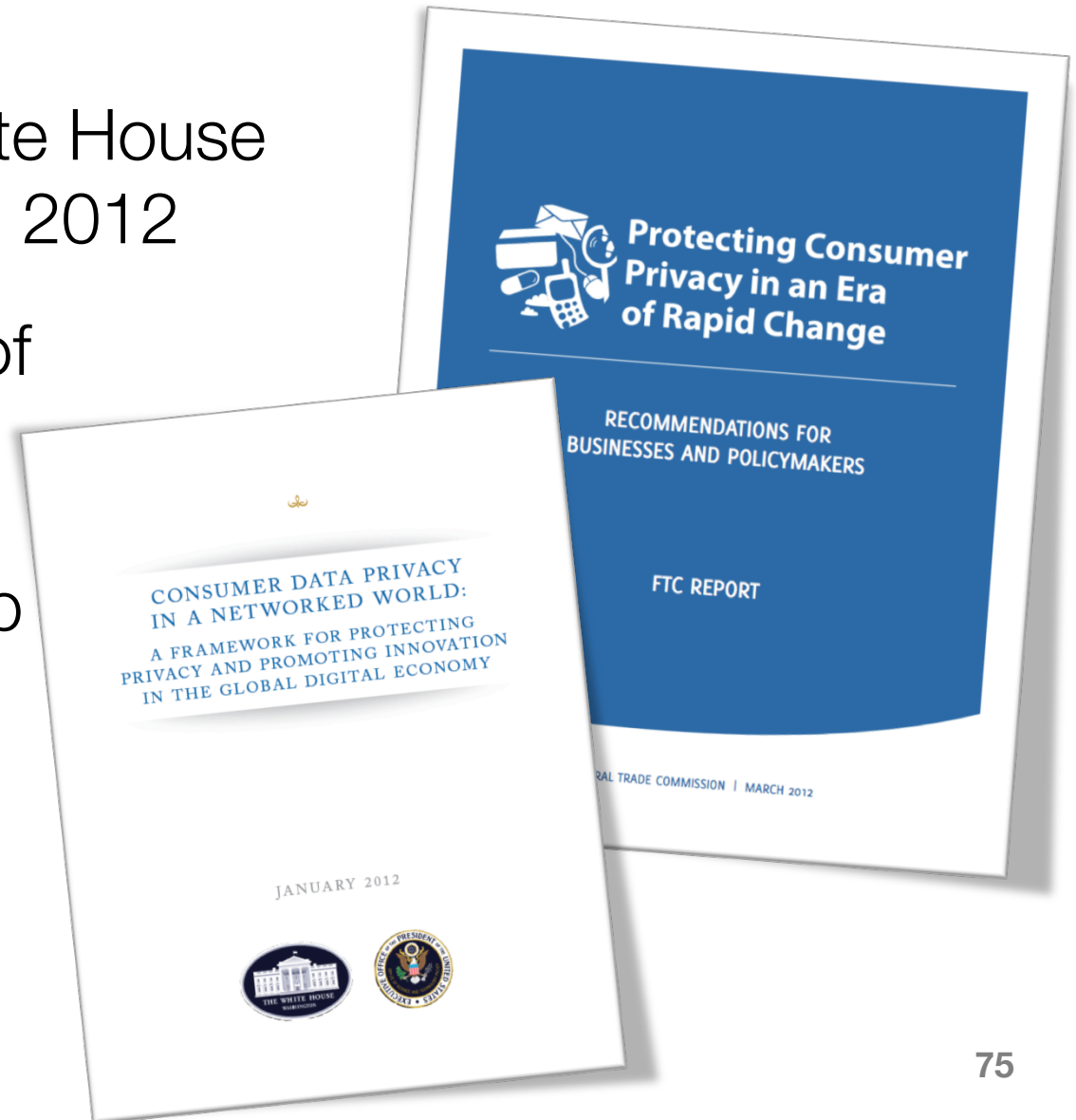
# OECD fair information principles

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability
- <http://www.privacyrights.org/ar/fairinfo.htm>

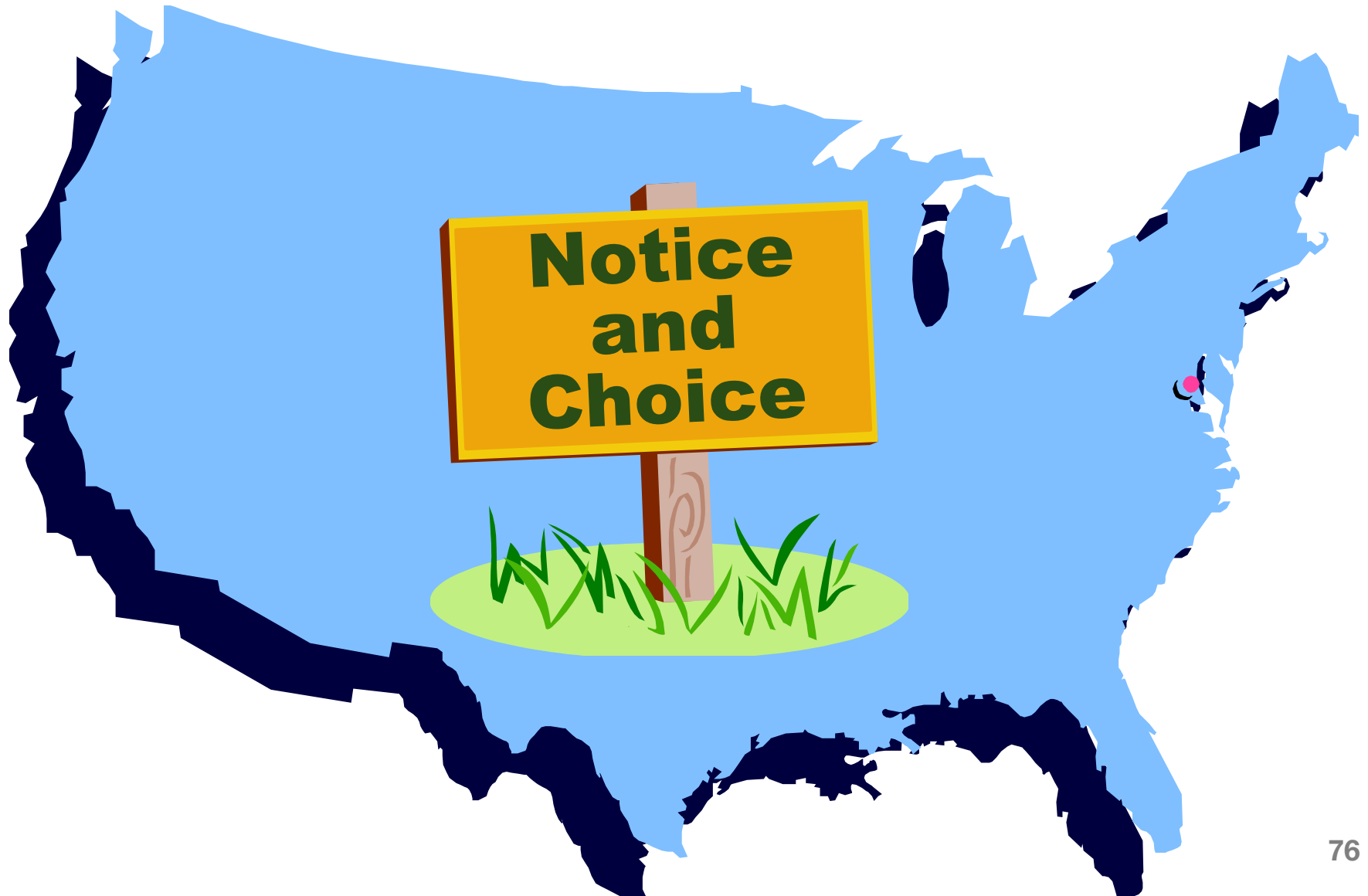


# US government privacy reports

- U.S. FTC and White House reports released in 2012
- U.S. Department of Commerce multi-stakeholder process to develop enforceable codes of conduct



# Privacy self regulation



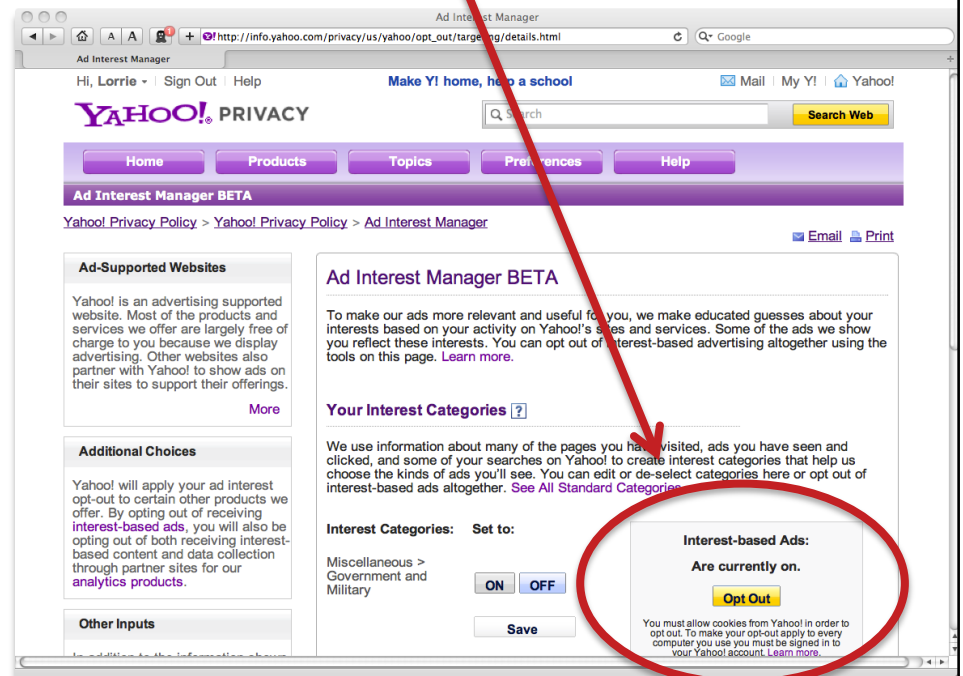
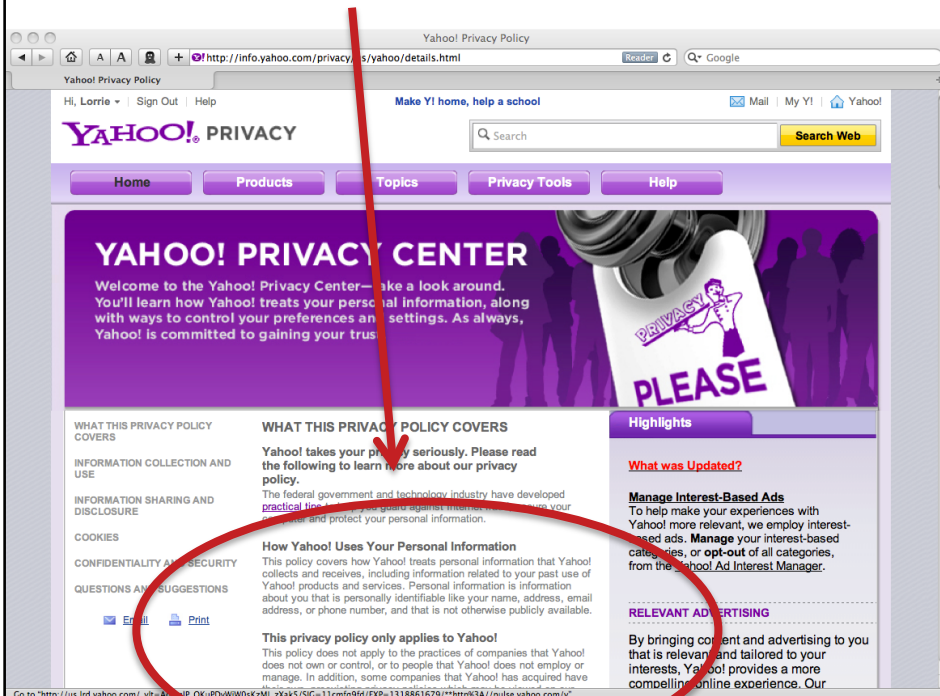


# Notice and choice

Protect privacy by giving people control over their information

**Notice** about data collection and use

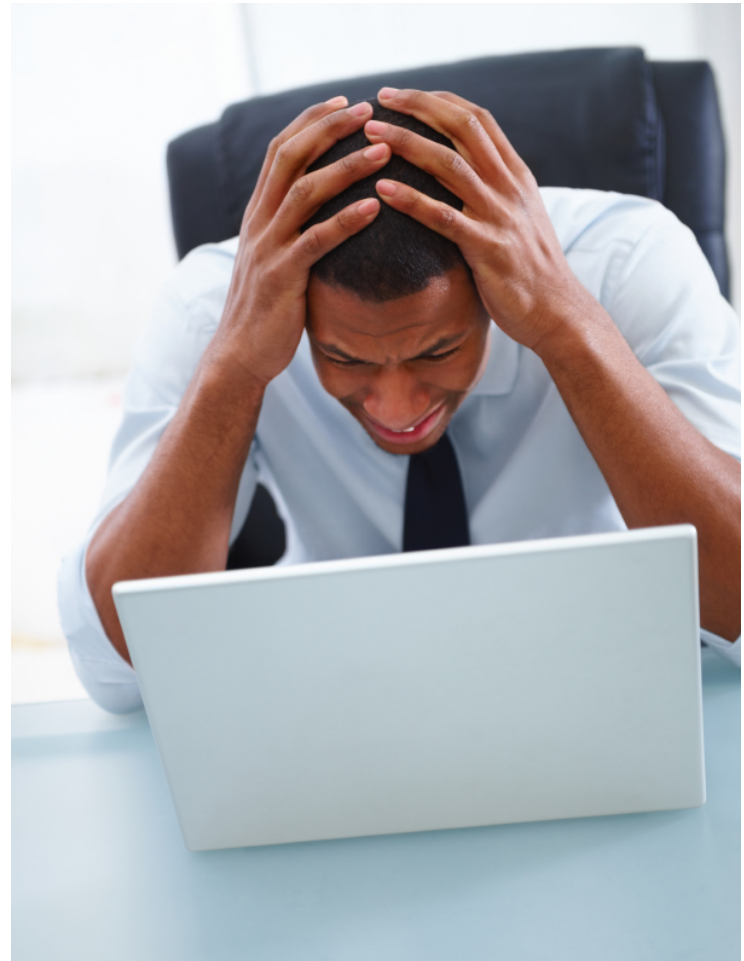
**Choices** about allowing their data to be collected and used in that way



# Nobody wants to read privacy policies

“the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand”

- *Protecting Consumer Privacy in an Era of Rapid Change*. Preliminary FTC Staff Report. December 2010.



# Cost of reading privacy policies

- What would happen if everyone read the privacy policy for each site they visited once per year?
- 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 Policies. I/S: A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review Issue. <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>





[illegible][illegible]

# **Privacy Facts**

[illegible]



# Towards a privacy “nutrition label”

- Standardized format
  - People learn where to find answers
  - Facilitates policy comparisons
- Standardized language
  - People learn terminology
- Brief
  - People find info quickly
- Linked to extended view
  - Get more details if needed



### Nutrition Facts

Serving Size 1-1/4 Cup (2 oz/55g)  
Servings Per Container About 12

Amount Per Serving	Cereal	With 1/2 Cup Vit. A & D Fortified Skim Milk
<b>Calories</b>	220	260
Calories from Fat	25	25
<b>% Daily Value**</b>		
<b>Total Fat</b> 2.5g*	<b>4%</b>	<b>4%</b>
Saturated Fat 0.5g	<b>2%</b>	<b>2%</b>
Trans Fat 0g		
<b>Cholesterol</b> 0mg	<b>0%</b>	<b>1%</b>
<b>Sodium</b> 250mg	<b>10%</b>	<b>12%</b>
<b>Potassium</b> 180mg	<b>5%</b>	<b>11%</b>
<b>Total Carbohydrate</b> 42g	<b>14%</b>	<b>16%</b>
Dietary Fiber 5g	<b>20%</b>	<b>20%</b>
Soluble Fiber 2g		
Insoluble Fiber 3g		
Sugars 11g		
<b>Protein</b> 6g		
Vitamin A	0%	6%
Vitamin C	35%	35%
Calcium	2%	15%
Iron	10%	10%
Vitamin E	8%	8%
Thiamin	10%	15%
Riboflavin	4%	10%
Niacin	6%	6%
Phosphorus	15%	30%
Magnesium	15%	20%
Zinc	10%	15%
Copper	10%	10%

\* Amount in cereal. One half cup skim milk contributes an additional 40 calories, 65mg sodium, 200mg potassium, 6g carbohydrate (6g sugars), and 4g protein.

\*\* Percent daily values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

	Calories: 2,000	2,500
Total Fat	Less Than 65g	80g
Sat Fat	Less Than 20g	25g
Cholesterol	Less Than 300mg	300mg
Sodium	Less Than 2,400mg	2,400mg
Total Carbohydrate	300g	375g
Dietary Fiber	25g	30g

Calories per gram:  
Fat 9 • Carbohydrate 4 • Protein 4

**Ingredients:** Whole Oat Flour, Whole Wheat Flour, Unsulphured Molasses, Malted Barley Extract, Baking Soda, Salt, Natural Vitamin E (Mixed Tocopherols [Soy]), Vitamin C.

*Contains wheat and soy. Made on equipment that also processes milk, almonds and hazelnuts.*

Distributed by: **Barbara's Bakery, Inc.®**, a Weetabix North America Company  
20 Cameron Street, Clinton, MA 01510  
www.BarbarasBakery.com  
Product of Canada



### Nutrition Facts

Serving Size 1 1/4 cup (55g)  
Servings per Container 8

Amount per Serving	
<b>Calories</b> 190	Calories from Fat 10
<b>% Daily Value*</b>	
<b>Total Fat</b> 1g	<b>2%</b>
Saturated Fat 0g	<b>0%</b>
Trans Fat 0g	
<b>Cholesterol</b> 0mg	<b>0%</b>
<b>Sodium</b> 115mg	<b>5%</b>
<b>Total Carbohydrate</b> 44g	<b>15%</b>
Dietary Fiber 9g	<b>36%</b>
Soluble Fiber less than 1g	
Insoluble Fiber 8g	
Sugars 9g	
<b>Protein</b> 6g	<b>12%</b>
Vitamin A 0%	• Vitamin C 130%
Calcium 4%	• Iron 30%
Thiamin 25%	• Riboflavin 25%
Niacin 25%	• Vitamin B6 25%
Folate 25%	• Vitamin B12 25%
Zinc 15%	

\* Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs:

	Calories: 2,000	2,500
Total Fat	Less than 65g	80g
Sat Fat	Less than 20g	25g
Cholesterol	Less than 300mg	300mg
Sodium	Less than 2,400mg	2,400mg
Total Carbohydrate	300g	375g
Dietary Fiber	25g	30g
Protein	50g	65g

**INGREDIENTS:** Organic Whole Grain Wheat Flour, Organic Wheat Bran, Organic Evaporated Cane Juice, Organic Oat Fiber, Sea Salt, Organic Caramel Color, Natural Vitamin E.

**NUTRITION BLEND:** Nicotinamide, Vitamin C, Niacin, Iron, Zinc, Vitamin B6, Riboflavin, Thiamin, Folate, Vitamin B12.

Our vendors follow Good Manufacturing Practices to segregate ingredients to avoid cross contact with allergens. Made on shared equipment with milk, tree nuts & soy. Facility processes eggs & peanuts.

Dist. & Sold Exclusively By:  
Trader Joe's, Monrovia, CA 91016

Certified Organic by  
Quality Assurance International (QAI).





# Iterative design process

- Series of studies
  - Focus groups
  - Lab studies
  - Online studies
- Metrics
  - Reading-comprehension (accuracy)
  - Time to find information
  - Ease of policy comparison
  - Subjective opinions, ease, fun, trust

P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder.  
A “Nutrition Label” for Privacy. SOUPS 2009.





P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor.  
Standardizing Privacy Notices: An Online Study  
of the Nutrition Label Approach. CHI2010.

Acme						
information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						


  

<b>Access to your information</b> This site gives you access to your contact data and some of its other data identified with you	acme.com 5000 Forbes Avenue Pittsburgh, PA 15213 United States Phone: 800-555-5555 help@acme.com
<b>How to resolve privacy-related disputes with this site</b> Please email our customer service department	

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

# Privacy label for Android



**Word Weasel**  
concreterose

Download

Next game starts in 33.3 seconds

Word Weasel

Wait for next game

Join game in progress

wink

Score 18

gone • wig • wise • wink • won

Last game: score 0

**Privacy score**

★★★★☆ 793

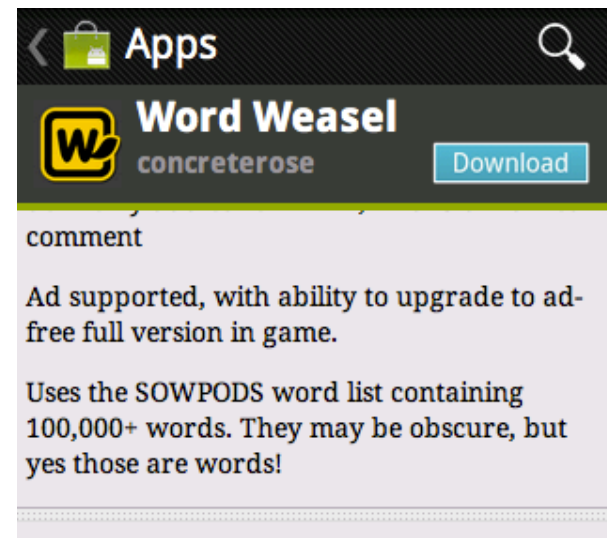
10,000+ downloads

1.9MB

**DESCRIPTION**

Like word games? Like weasels? This is the game for you. Word Weasel is a fast word game where you find as many words as you can from 9 letters in 50 seconds. Compete with everyone else playing at the same time, a new game starts every minute!

"The most fun you can have on your own with 9 random letters. Brilliantly simple, devilishly addictive." –Kim, Android Market comment



**Word Weasel**  
concreterose

Download

comment

Ad supported, with ability to upgrade to ad-free full version in game.

Uses the SOWPODS word list containing 100,000+ words. They may be obscure, but yes those are words!

**Privacy Facts**

THIS APP COLLECTS YOUR

- ☒ Personal information
- ☐ Contacts
- ☒ Location
- ☐ Calendars
- ☐ Credit card / financial
- ☐ Diet / nutrition
- ☐ Health / medical
- ☐ Photos

THIS APP USES

- ☐ Advertising
- ☒ Analytics

**REVIEWS**

**Average**

**4.6**

★★★★☆ 793

Stars	Count
5 stars	534
4 stars	210
3 stars	37
2 stars	5
1 star	7



Your Data is Used Only for the Intended Use



Your Data May be Used for Purposes You Do Not Intend



Your data is never given to advertisers.



Site gives your data to advertisers.



Your data is never bartered or sold.



Your data may be bartered or sold.



Data is given to law enforcement only when legal process is followed.



Data may be given to law enforcement even when legal process is not followed.



Your data is kept for less than 1 month.



Your data may be kept indefinitely.



More on privacy coming March 22

# Homework 1 presentations