

# Security and Privacy

Lorrie Cranor

lorrie@cmu.edu  
lorrie.cranor.org  
@lorrietweet

Carnegie Mellon University



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

CyLab Usable Privacy & Security Laboratory

## What is computer security?

- Protecting information systems against misuse and interference
- “Building systems to remain dependable in the face of malice, error or mischance”  
(Ross Anderson)



Created by Gan Khoo Lay  
from Noun Project

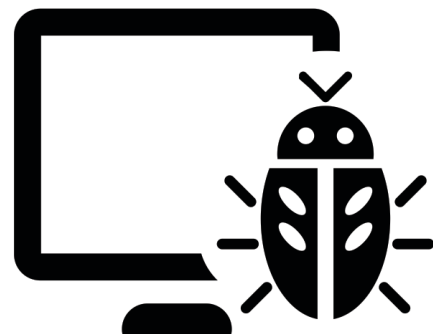
# Properties of a secure system

- Confidentiality
  - Information is protected from unintended disclosure (secrecy, privacy, access control)
- Integrity
  - System and data are maintained in a correct and consistent condition
- Availability
  - Systems and data are usable when needed (includes timeliness)

3

# Attackers exploit bugs

- Software bugs
- Hardware bugs
- Humans (social engineering)
- Unintended characteristics (e.g., side channels, poor sources of randomness)



Created by iconoci  
from Noun Project

4

# Modeling the attacker

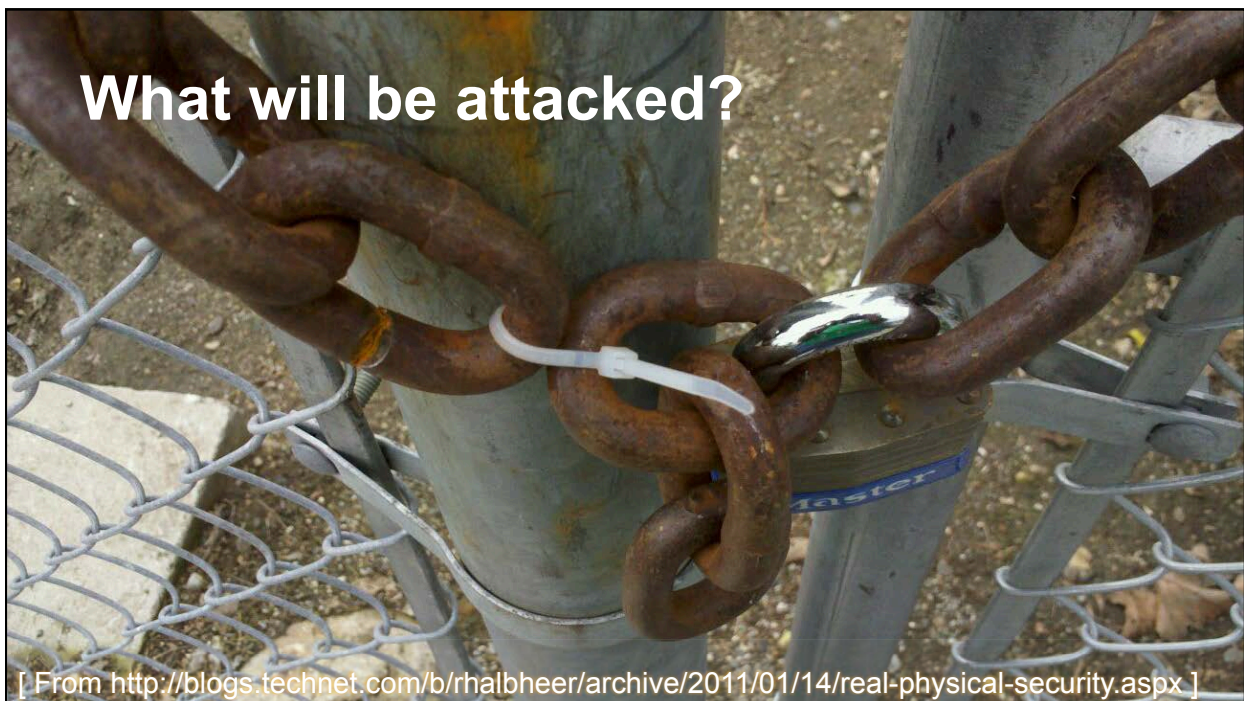
- What type of action will they take?
  - Passive (look, but don't touch)
  - Active (look and inject messages)
- How sophisticated are they?
- How much do they care? What resources do they have?
  - How much time/money will they spend?
- How much do they already know?
  - External / internal attacker?



Created by Jorge Reyes  
from the Noun Project

5

## What will be attacked?



[ From <http://blogs.technet.com/b/rhalbheer/archive/2011/01/14/real-physical-security.aspx> ]

**What was being protected?**



[ From <https://flic.kr/p/amsEr6> (creative commons) ]

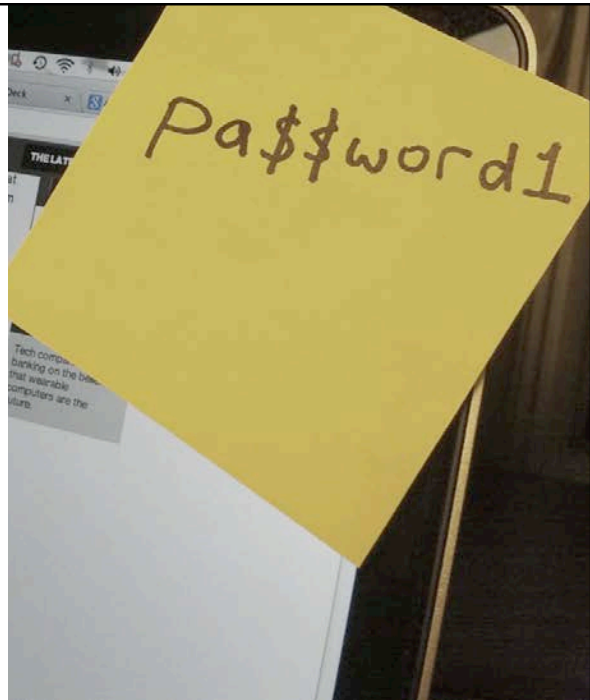
7

**How do attackers  
guess passwords?**

8

# Password vulnerabilities

- Shoulder surfing attacks
- Online attacks
- Offline attacks





## Large numbers of passwords leaked

	Affected users	Date
Sony	25,000,000	2011
Dropbox	68,000,000	2012
LivingSocial	50,000,000	2013
Sega	1,300,000	2011
Booz Allen Hamilton	90,000	2011
Evernote	50,000,000	2013
Drupal	1,000,000	2013
Ashley Madison	32,000,000	2015

11

## How do attackers steal so many passwords?

- Attackers break in and steal entire password database
- Database usually scrambled with hash function
- Attackers make billions of guesses to try to recover as many scrambled passwords as they can



12

## Dumb attacker

aaaaaaaa

aaaaaaab

aaaaaaac

aaaaaaad

aaaaaaae

...

## Smart attacker

123456789

password

iloveyou

princess

12345678

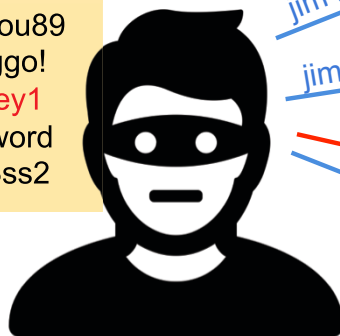
...

13

## Attackers exploit password reuse

### CRACKED PASSWORDS

UserID	Password
jane	iloveyou89
jami	godoggo!
jim	monkey1
kar	pa\$\$word
katie	princ3ss2



jim monkey1

jim monkey1

jim monkey2

jim monkey1

Online Store

Bank

Employer

14

How can we help users pick passwords that are easy to remember, but hard for an attacker to guess?

15

amazonmechanical turk

Artificial Intelligence

Your Account

HITS

Qualifications

Introduction | Dashboard | Status | Account Settings

Already have an account?  
Sign in as a Worker | Requester

**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.

**476,446 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

Find an interesting task

Work

Earn money

Find HITS Now

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. [Register Now](#)

**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

Fund your account

Load your tasks

Get results

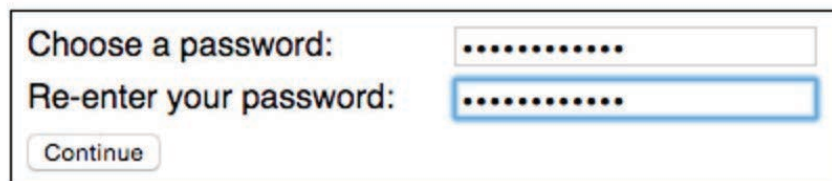
Get Started

16



## Participant tasks

- Create password under a randomly assigned condition
- Take a survey
- Recall password
- Return 2 days later to recall password and take survey



Choose a password: .....  
Re-enter your password: .....

17

## Password policies

### Policy

### Example password

Basic8

**password**

Dictionary8

**sapsword**

Comprehensive8

**Sapsword1!**

Basic16

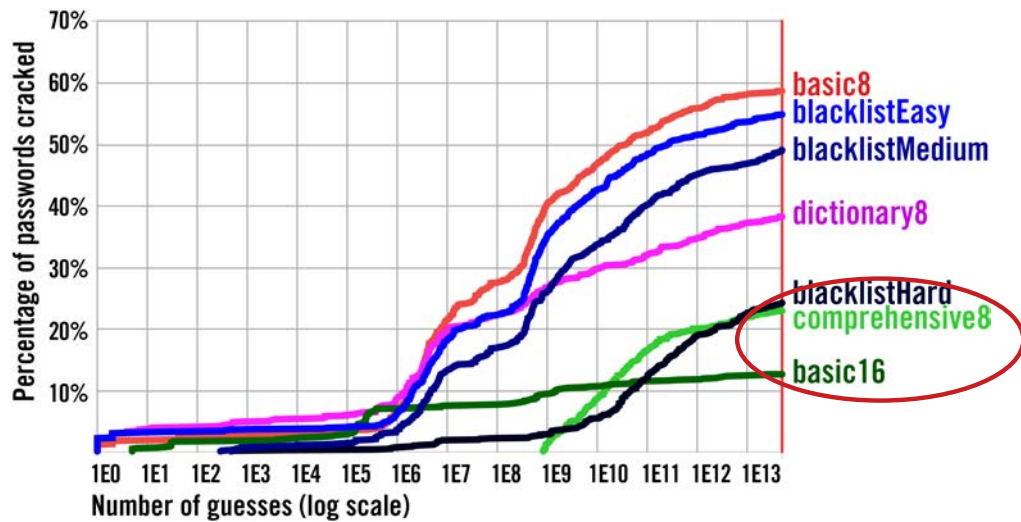
**passwordpassword**

---

S. Komanduri, R. Shay, P.G. Kelley, M.L. Mazurek, L. Bauer, N. Christin, L.F. Cranor, and S. Egelman. Of passwords and people: Measuring the effect of password-composition policies. CHI 2011.

18

# Password policy strength

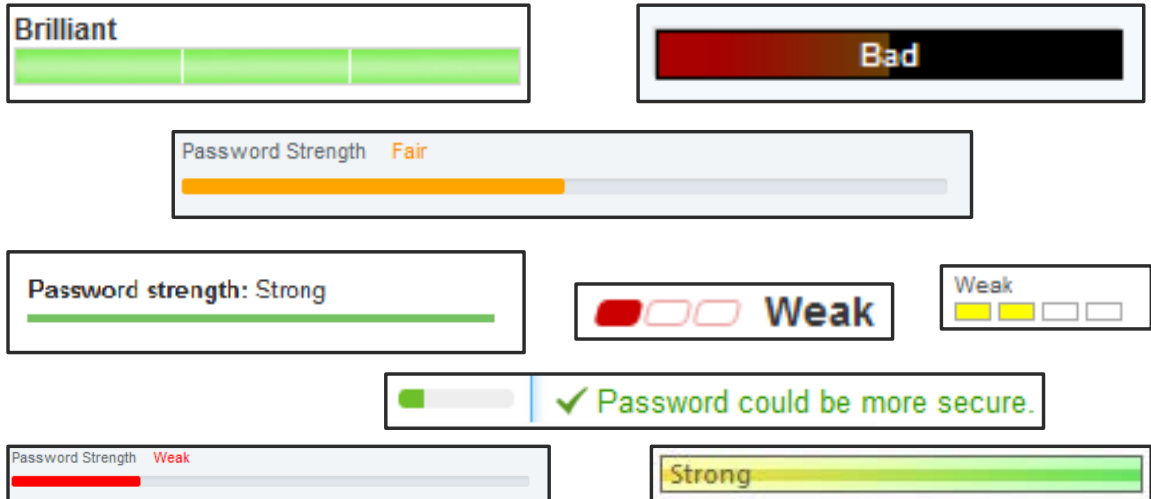


19

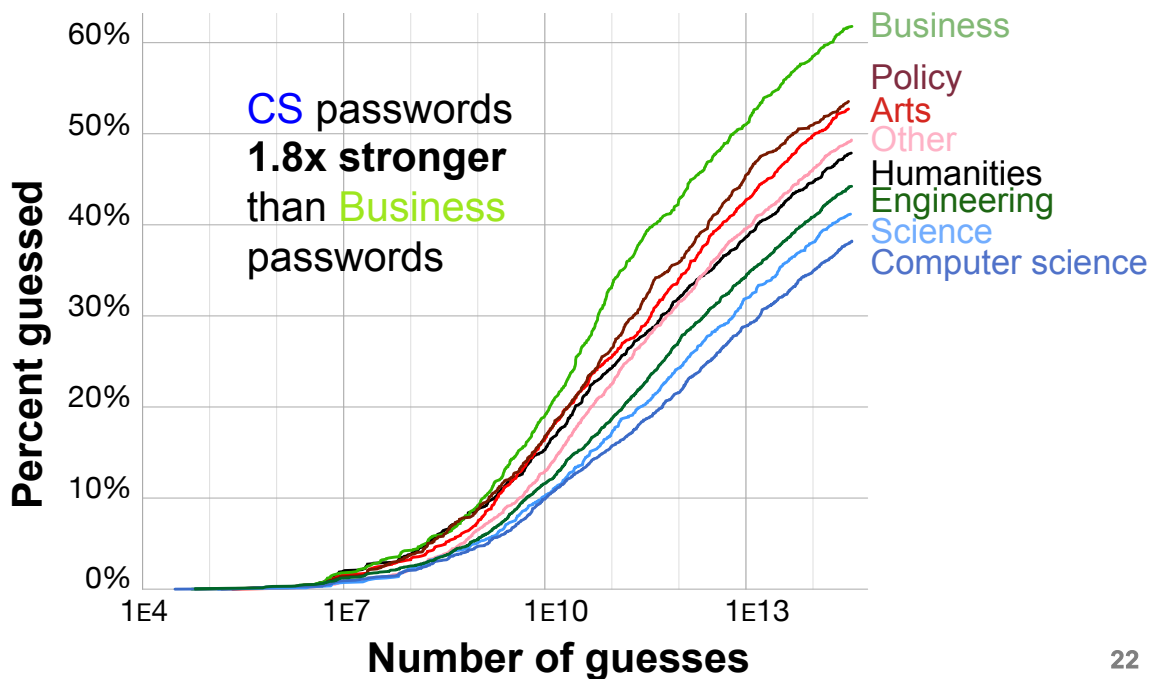
We all like monkeys

CC BY-NC-SA 2.0 by Joseph Younis  
<http://www.flickr.com/photos/strike1/4782099435>

# Do password meters help?



21



22

# What is privacy?

23



"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)

24



Privacy is being  
by myself.

– Emma, age 5

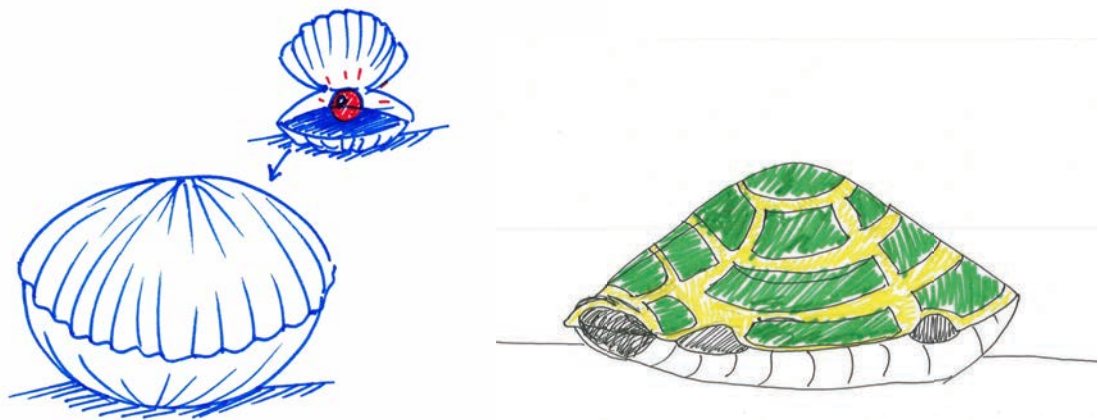
25



Privacy is the  
right to be by  
yourself.  
Privacy is  
isolation.

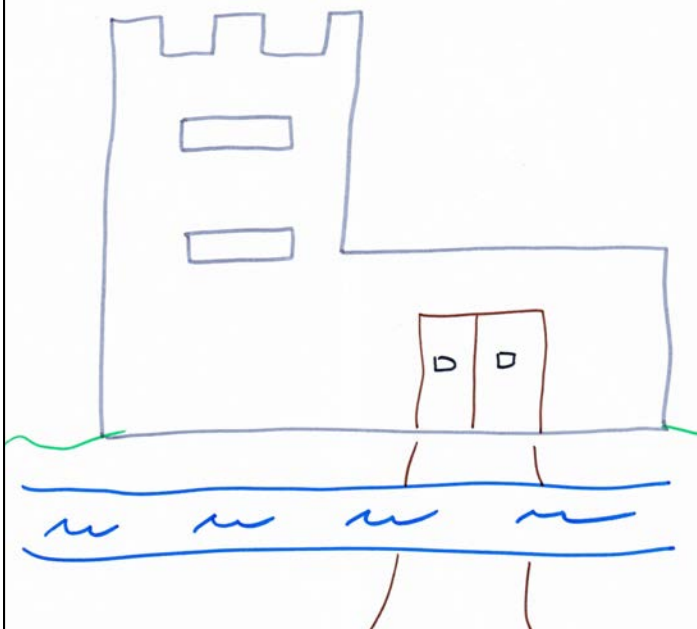
– Kevin, age 28

26



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!

27

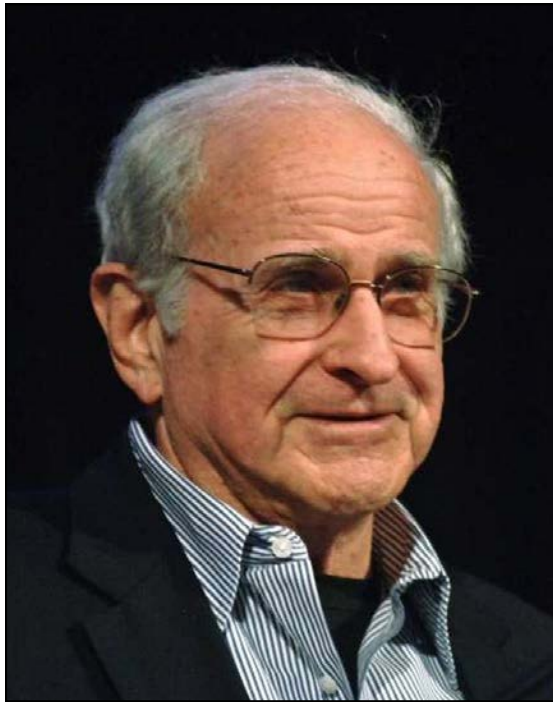


Privacy is protection from  
unwanted scrutiny or  
attention.

-RMF, age 54

28

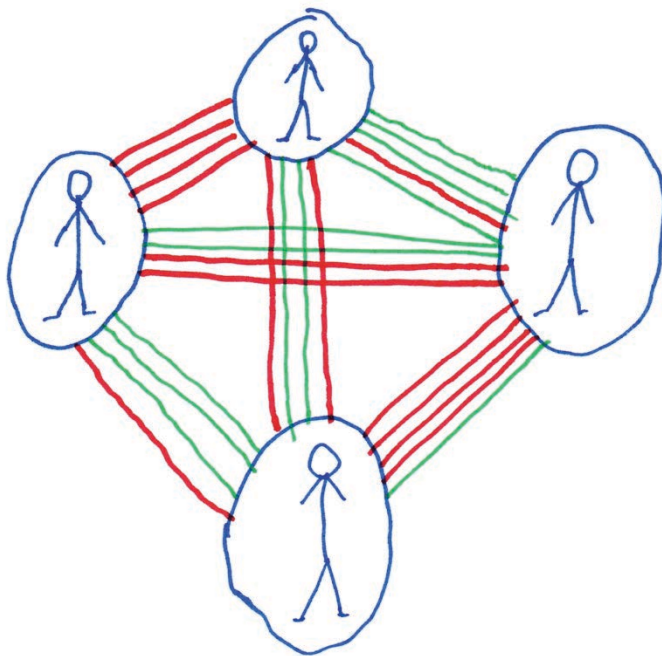




Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

– Alan Westin  
*Privacy and Freedom*, 1967


29



Privacy is a network: I share what I want with whom I want and trust and what matches with those in the network....

Green = share.  
Red = don't.

30



There are bright sides, and there are dark sides. Some of them we'd love to share; some we don't, and they are called "privacy."

– Evan, age 21

31

## How privacy is protected

- Laws
- Self regulation
- Technology

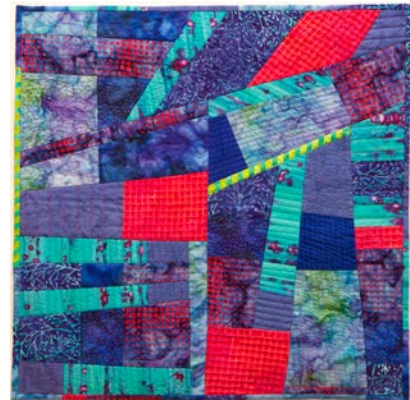
## EU has comprehensive privacy laws

- Privacy laws enacted in 1996
- New privacy laws enacted in 2018
  - General Data Protection Regulation
- Data protection commissioners in every country

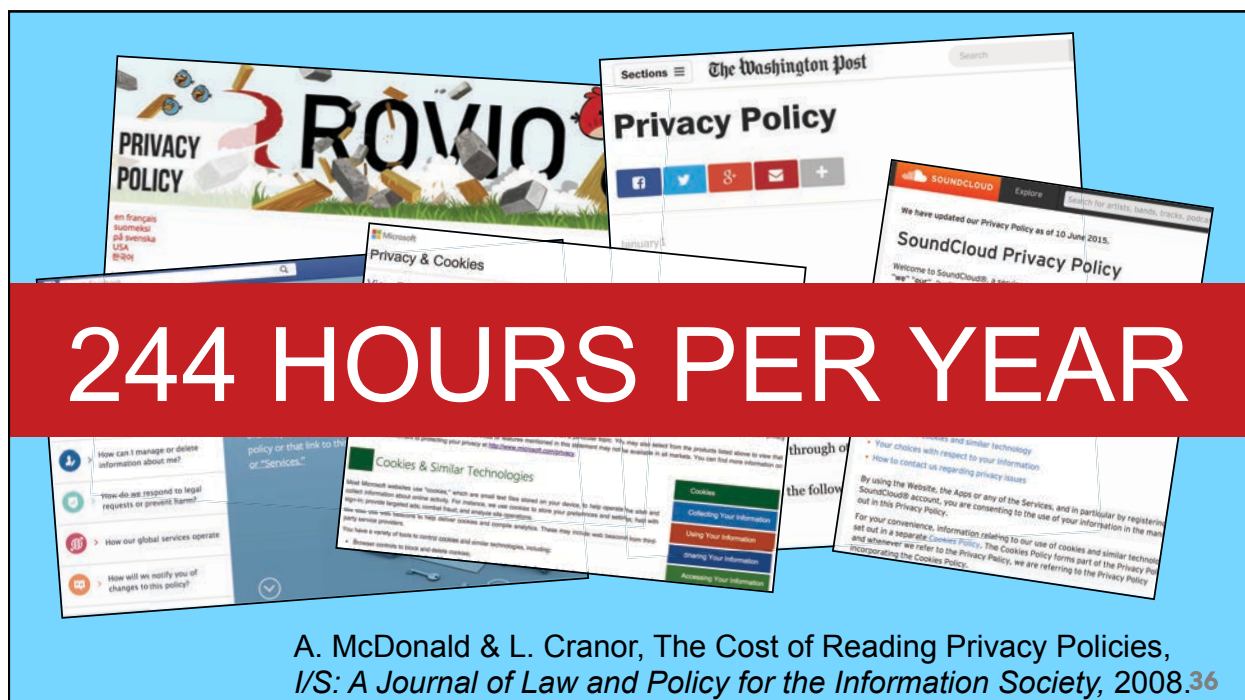
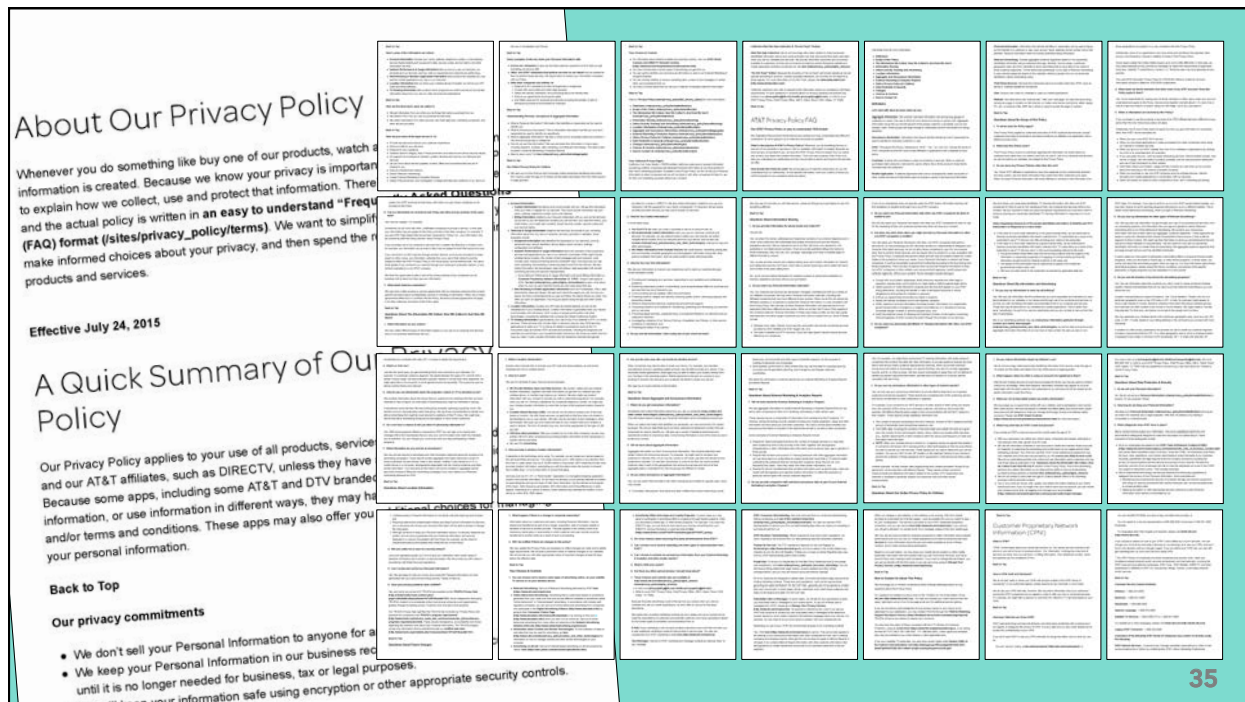
33

## US privacy laws: a “patchwork quilt”

- No explicit constitutional right to privacy or general privacy law
- Mostly sector-specific laws
  - Narrow regulations for health, financial, education, children, etc.
- Federal Trade Commission jurisdiction over fraud + deceptive practices
- Some state and local laws



34



A. McDonald & L. Cranor, The Cost of Reading Privacy Policies, *I/S: A Journal of Law and Policy for the Information Society*, 2008.<sup>36</sup>

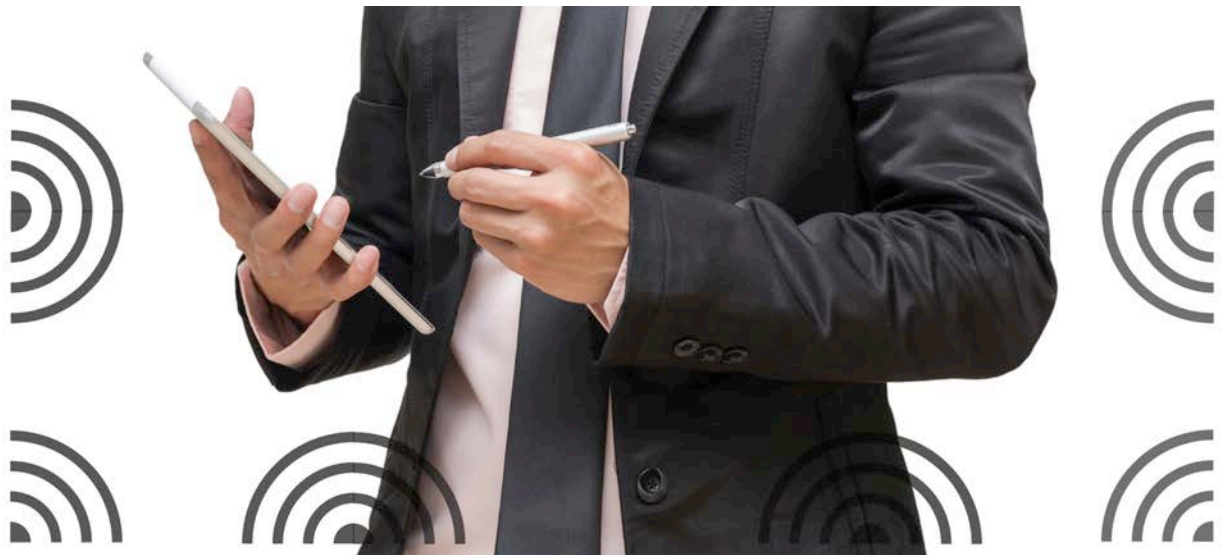
## Privacy enhancing technologies

- Encryption tools
- Anonymity tools
- Tracker blockers (and viewers)
- Opt-out tools
- Social network privacy controls

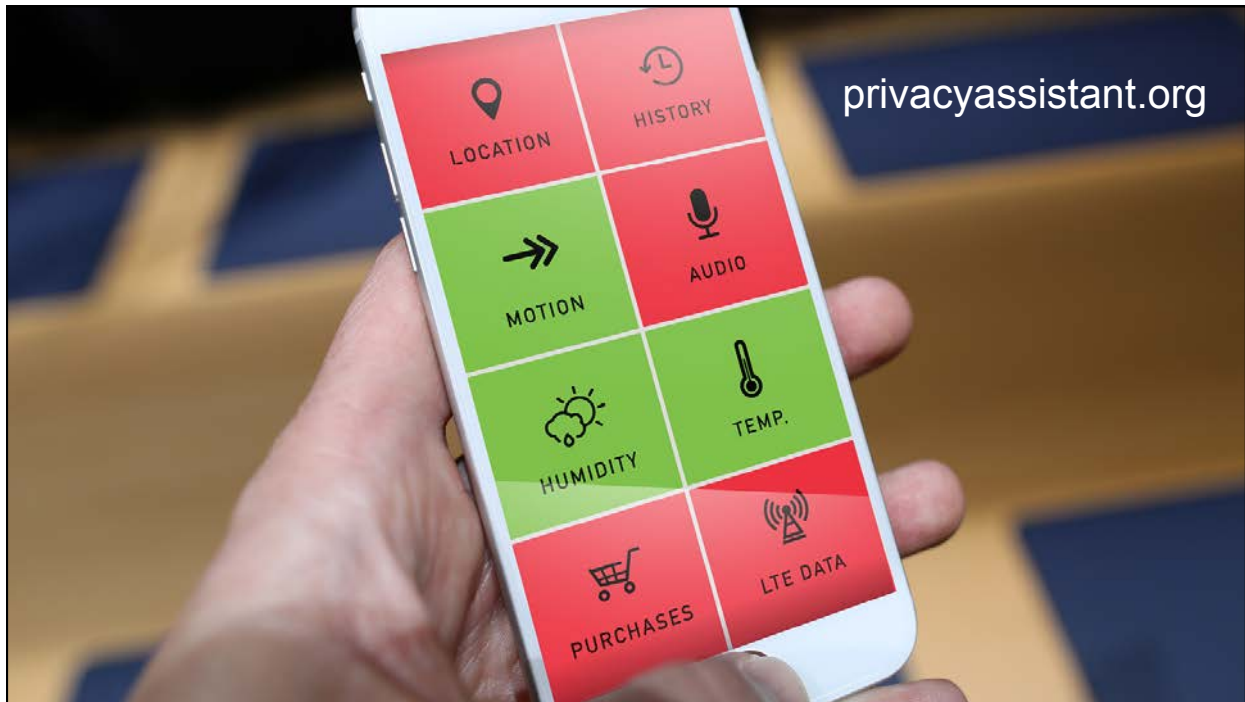


37

## Personal privacy assistants







## Security and privacy at CMU

- CyLab Security and Privacy Institute
- Undergraduate concentration in security and privacy for SCS and ECE students
- Minor in cybersecurity and international conflict (Institute for Politics and Strategy)
- Many masters programs and PhD opportunities
- Many research opportunities



# Security and privacy courses

- If you take 15-213:
  - 15-330 Introduction to computer security
- No prerequisites:
  - 17-303 Cryptocurrencies, Blockchains, and Applications
  - 17-331 Information security and privacy
  - 17-333 Privacy policy, law, and technology
  - 17-334 Usable privacy and security
- And many more....

41

