Ideation Techniques to Facilitate System Design Compliant with Privacy Laws and Regulations

SAMEER PATIL, INDIANA UNIVERSITY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

Privacy Compliance by Design

Enhancing Industry Software Practices for Compliance with Privacy Laws and Regulations

Sameer Patil, *Ph.D.*

Assistant Professor

Indiana University Bloomington

INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING

Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

Quad Chart for: Cybersecurity Transition To Practice (TTP) Acceleration **Privacy Compliance by Design**

Challenge:

Bridge the gap between privacy policy makers and software professionals.

Solution:

- Ideation cards for facilitating privacy compliant solutions.
- Cards represent key US privacy laws and regulations.

Value proposition:

- Translate laws and regulations into tools accessible to and actionable by software professionals.
- Facilitate privacy compliance at all stages of system design & development.
- Highlight important similarities and differences across jurisdictions.

What we need to TTP

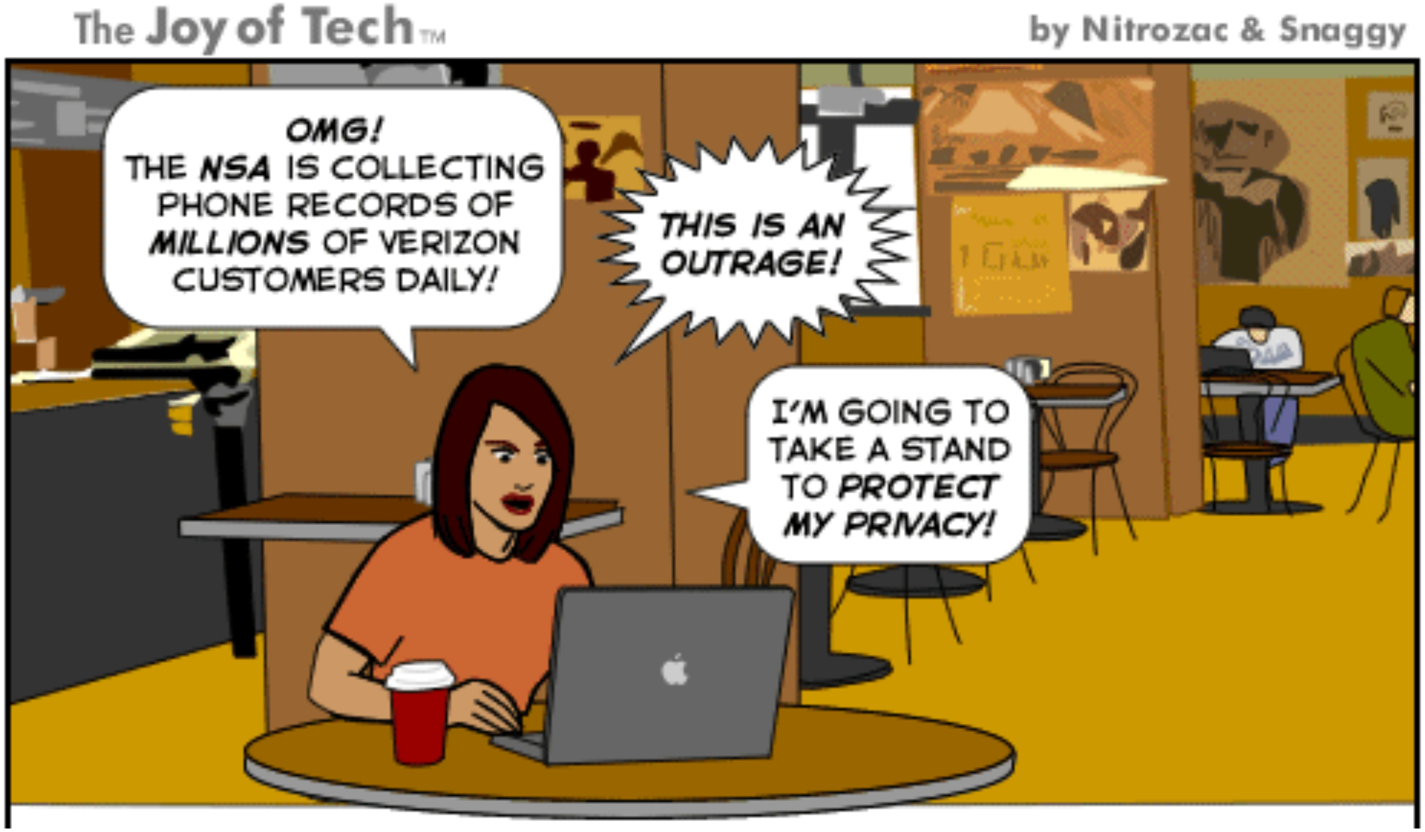
- Opportunities to pilot the research
- Real-world case studies
- Feedback

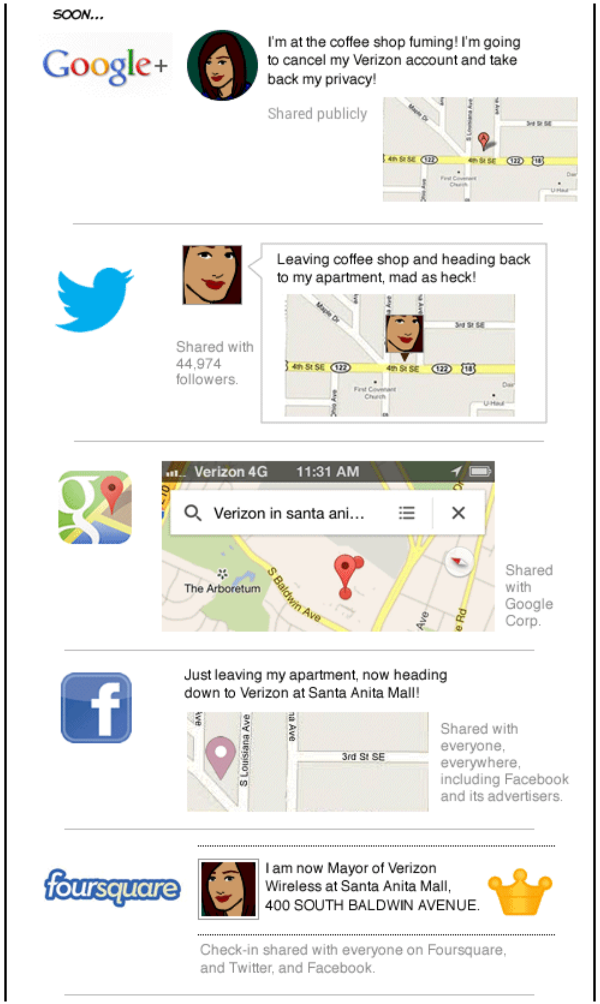
NSF EAGER #CNS-1548779
Privacy Compliance by Design
Ideation Techniques to Facilitate System Design Compliant with Privacy Laws and Regulations

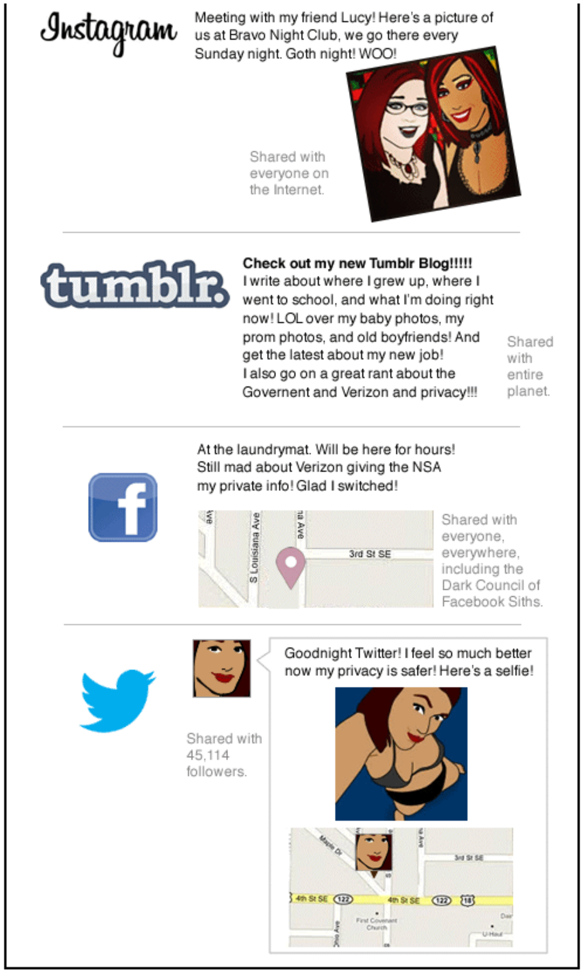
PI: Sameer Patil

Contact:

Sameer Patil
patil@indiana.edu


The Joy of Tech™
by Nitrozac & Snaggy
OMG! THE NSA IS COLLECTING PHONE RECORDS OF MILLIONS OF VERIZON CUSTOMERS DAILY!
THIS IS AN OUTRAGE!
I'M GOING TO TAKE A STAND TO PROTECT MY PRIVACY!

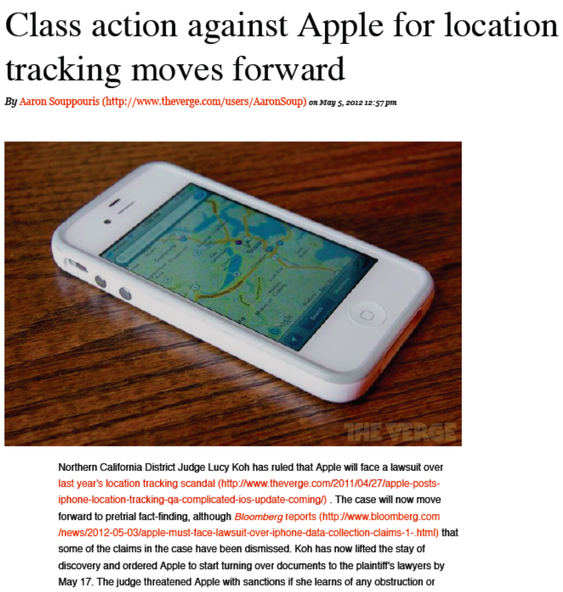

SOON...
Google+
I'm at the coffee shop fuming! I'm going to cancel my Verizon account and take back my privacy!
Shared publicly
Leaving coffee shop and heading back to my apartment, mad as heck!
Shared with 44,974 followers.
Verizon 4G 11:31 AM
Verizon in santa ani...
The Arboretum
S Baldwin Ave
Shared with Google Corp.
Just leaving my apartment, now heading down to Verizon at Santa Anita Mall!
Shared with everyone, everywhere, including Facebook and its advertisers.
foursquare
I am now Mayor of Verizon Wireless at Santa Anita Mall, 400 SOUTH BALDWIN AVENUE.
Check-in shared with everyone on Foursquare, and Twitter, and Facebook.


Instagram
Meeting with my friend Lucy! Here's a picture of us at Bravo Night Club, we go there every Sunday night. Goth night! WOO!
Shared with everyone on the Internet.
tumblr.
Check out my new Tumblr Blog!!!!! I write about where I grew up, where I went to school, and what I'm doing right now! LOL over my baby photos, my prom photos, and old boyfriends! And get the latest about my new job! I also go on a great rant about the Government and Verizon and privacy!!!
Shared with entire planet.
At the laundrymat. Will be here for hours! Still mad about Verizon giving the NSA my private info! Glad I switched!
Shared with everyone, everywhere, including the Dark Council of Facebook Siths.
Goodnight Twitter! I feel so much better now my privacy is safer! Here's a selfie!
Shared with 45,114 followers.

© 2013 Geek Culture

joyoftech.com

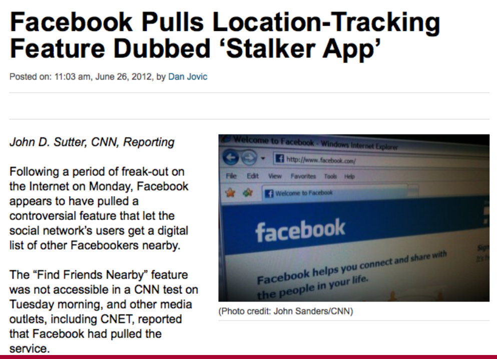
“We are committed to the privacy of our users …”



Class action against Apple for location tracking moves forward

By Aaron Souppouris (http://www.theverge.com/users/AaronSoup) *on May 5, 2012 12:57 pm*

Northern California District Judge Lucy Koh has ruled that Apple will face a lawsuit over last year's location tracking scandal (http://www.theverge.com/2011/04/27/apple-posts-iphone-location-tracking-qa-complicated-ios-update-coming/) . The case will now move forward to pretrial fact-finding, although *Bloomberg* reports (http://www.bloomberg.com/news/2012-05-03/apple-must-face-lawsuit-over-iphone-data-collection-claims-1-.html) that some of the claims in the case have been dismissed. Koh has now lifted the stay of discovery and ordered Apple to start turning over documents to the plaintiff's lawyers by May 17. The judge threatened Apple with sanctions if she learns of any obstruction or



Facebook Pulls Location-Tracking Feature Dubbed 'Stalker App'

Posted on: 11:03 am, June 26, 2012, by Dan Jovic

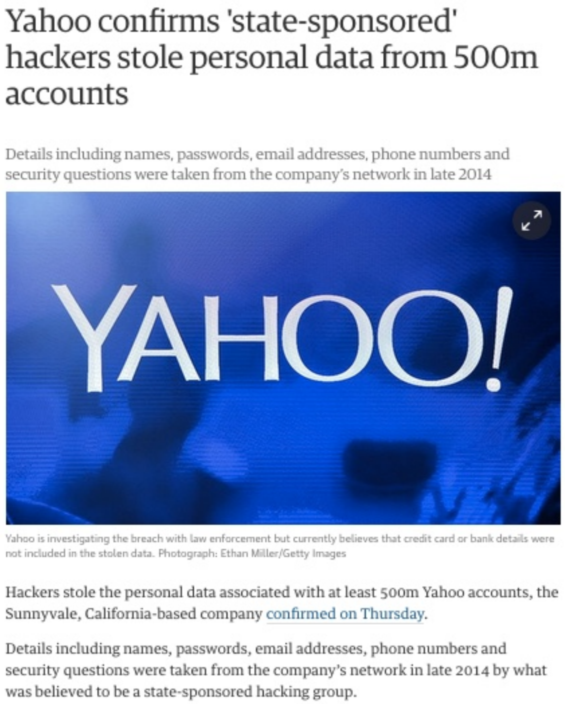
John D. Sutter, CNN, Reporting

Following a period of freak-out on the Internet on Monday, Facebook appears to have pulled a controversial feature that let the social network's users get a digital list of other Facebookers nearby.

The "Find Friends Nearby" feature was not accessible in a CNN test on Tuesday morning, and other media outlets, including CNET, reported that Facebook had pulled the service.

Welcome to Facebook - Windows Internet Explorer
http://www.facebook.com/
File Edit View Favorites Tools Help
Welcome to Facebook
facebook
Facebook helps you connect and share with the people in your life.

(Photo credit: John Sanders/CNN)



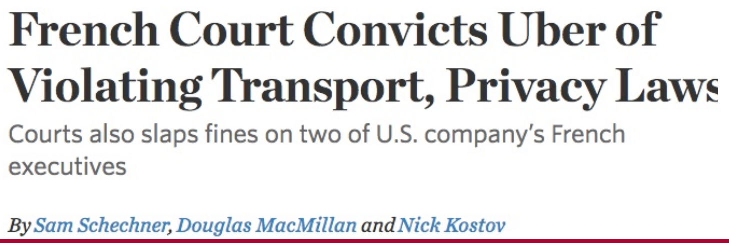
Yahoo confirms 'state-sponsored' hackers stole personal data from 500m accounts

Details including names, passwords, email addresses, phone numbers and security questions were taken from the company's network in late 2014

Yahoo is investigating the breach with law enforcement but currently believes that credit card or bank details were not included in the stolen data. Photograph: Ethan Miller/Getty Images

Hackers stole the personal data associated with at least 500m Yahoo accounts, the Sunnyvale, California-based company confirmed on Thursday.

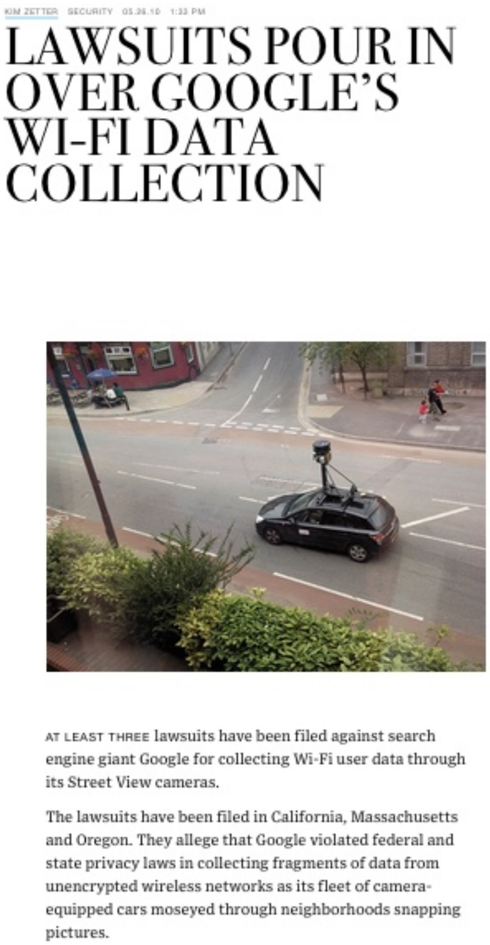
Details including names, passwords, email addresses, phone numbers and security questions were taken from the company's network in late 2014 by what was believed to be a state-sponsored hacking group.



French Court Convicts Uber of Violating Transport, Privacy Laws

Courts also slaps fines on two of U.S. company's French executives

By Sam Schechner, Douglas MacMillan and Nick Kostov



KIM ZETTER SECURITY 05.26.10 1:33 PM

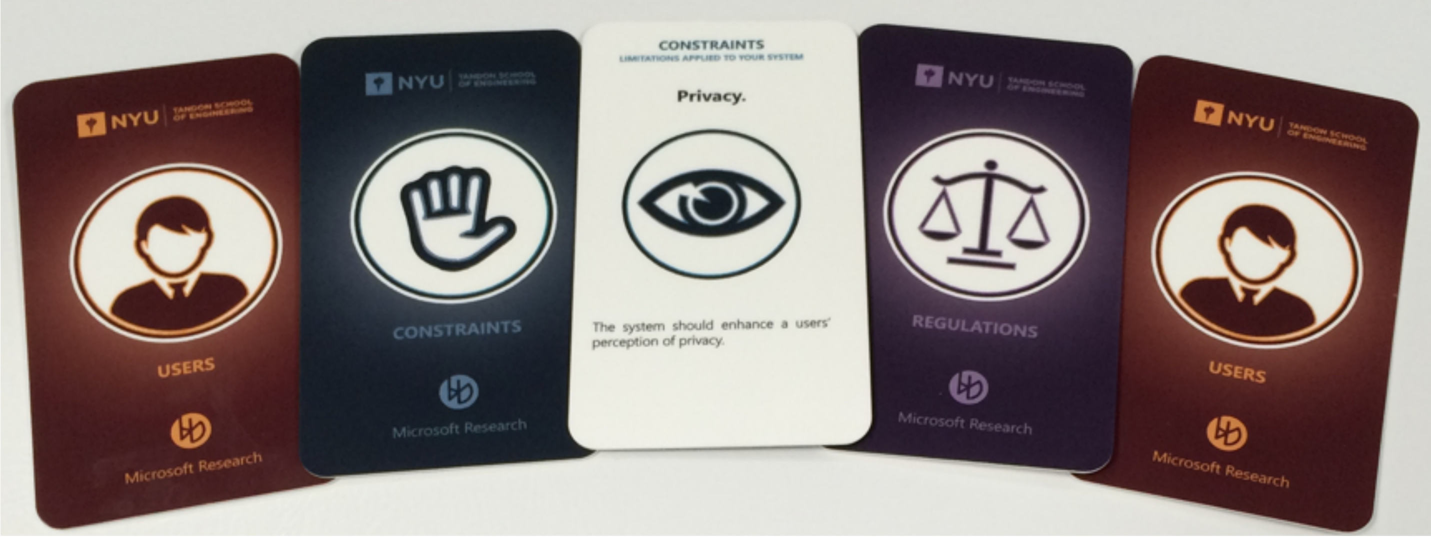
LAWSUITS POUR IN OVER GOOGLE'S WI-FI DATA COLLECTION

AT LEAST THREE lawsuits have been filed against search engine giant Google for collecting Wi-Fi user data through its Street View cameras.

The lawsuits have been filed in California, Massachusetts and Oregon. They allege that Google violated federal and state privacy laws in collecting fragments of data from unencrypted wireless networks as its fleet of camera-equipped cars moseyed through neighborhoods snapping pictures.

We need tools and techniques to facilitate privacy *compliance*

by design.


NYU TANDON SCHOOL OF ENGINEERING
USERS
Microsoft Research
NYU TANDON SCHOOL OF ENGINEERING
CONSTRAINTS
Microsoft Research
NYU TANDON SCHOOL OF ENGINEERING
REGULATIONS
Microsoft Research
NYU TANDON SCHOOL OF ENGINEERING
USERS
Microsoft Research

CONSTRAINTS
LIMITATIONS APPLIED TO YOUR SYSTEM

Privacy.

The system should enhance a users' perception of privacy.

Ewa Luger

Lachlan Urquhart

Michael Golembewski

Tom Rodden

Lesley Fosh

REGULATIONS

LEGAL REQUIREMENTS FOR YOUR SYSTEM

Explicit Consent.

You should only collect personal data after the user has given explicit and informed consent to data collection for a specific purpose. How does your system go about obtaining users’ explicit consent?

REGULATIONS

LEGAL REQUIREMENTS FOR YOUR SYSTEM

Notice.

You should provide notice to users about what data is to be collected, how it will be used and disseminated, and how it will be maintained. How will your system do that?

REGULATIONS

LEGAL REQUIREMENTS FOR YOUR SYSTEM

Data Minimization.

You should only collect personal data that is directly relevant and necessary to accomplish the purposes specified at the time of collection. How does your system ensure this is so?

REGULATIONS

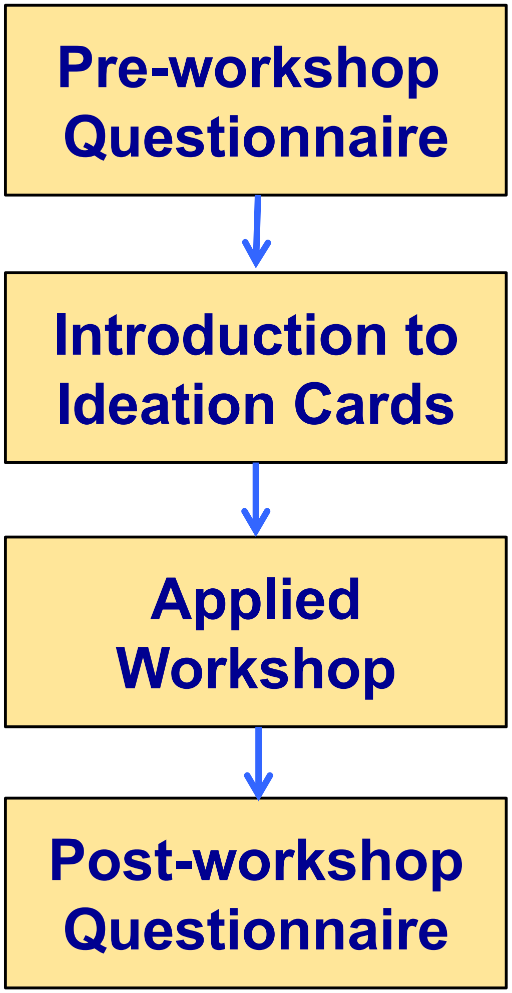
LEGAL REQUIREMENTS FOR YOUR SYSTEM

Breach Notification.

You are required to inform users of data breaches (loss, damage, or illicit access) without undue delay. What measures do you have in place for such a scenario?

Janice Tsai
MICROSOFT

Jonathan Fox
CISCO



Pre-workshop Questionnaire

Introduction to Ideation Cards

Applied Workshop

Post-workshop Questionnaire

5 *mins*	**High level system design**
5 *mins*	**User card**
5 *mins*	**Constraint card 1**
5 *mins*	**Constraint card 2**
5 *mins*	**Regulation card 1**
5 *mins*	**Regulation card 2**
10-15 *mins*	**Integrated design**
10-15 *mins*	**Wrap-up Interview**

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Older People.

Your users might be age 65 or older.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Visual Impairment.

Your users might be blind, or have other visual impairments that could impact their use of the system.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Second Language.

Your users might understand English as a second or third language, at varying levels of fluency.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Country of Residence.

Your users might reside in a country other than your own.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Low Cost.

The system should be designed as inexpensively as possible.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Data Maximization.

The system should collect as much data as possible about the user.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Minimal Distraction.

The system should not distract the user from primary goals or day-to-day activities.

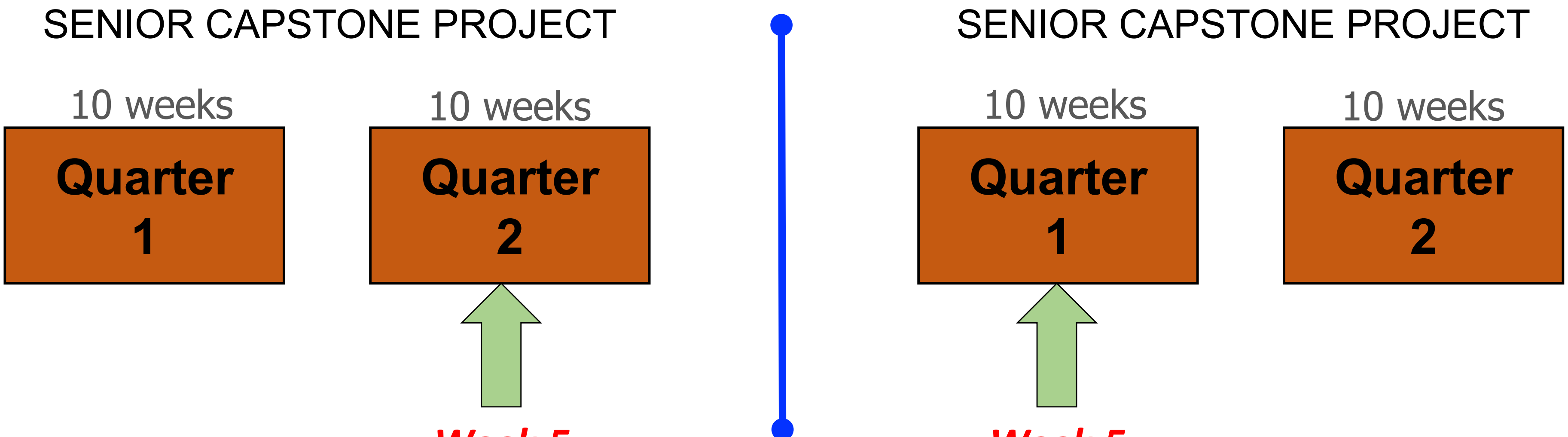
CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Social Sharing.

The system should engage with third party social media services.

We need a developer workforce with privacy knowledge and training.



SENIOR CAPSTONE PROJECT

10 weeks

Quarter 1

10 weeks

Quarter 2

Week 5

2015-16

SENIOR CAPSTONE PROJECT

10 weeks

Quarter 1

10 weeks

Quarter 2

Week 5

2016-17

Hadar Ziv

UC IRVINE

NYU TANDON SCHOOL OF ENGINEERING
USERS
Microsoft Research
NYU TANDON SCHOOL OF ENGINEERING
CONSTRAINTS
Microsoft Research
CONSTRAINTS
LIMITATIONS APPLIED TO YOUR SYSTEM
Privacy.
The system should enhance a users' perception of privacy.
NYU TANDON SCHOOL OF ENGINEERING
REGULATIONS
Microsoft Research
NYU TANDON SCHOOL OF ENGINEERING
USERS
Microsoft Research

https://pages.iu.edu/~patil/privacyideationcards.pdf

Sameer Patil

patil@indiana.edu

http://www.sameerpatil.net

NSF

CISCO™

Microsoft

NYU Center for Cybersecurity

horizon DIGITAL ECONOMY RESEARCH

INDIANA UNIVERSITY
SCHOOL OF INFORMATICS AND COMPUTING