

Max Planck Institute for Security and Privacy | Mar 1, 2022

Improving People's Security and Privacy Behaviors

Yixin Zou, Ph.D. Candidate



yixinz@umich.edu



yixinzou.github.io

Security and privacy in a digital world



People care about their security and privacy

PEW RESEARCH CENTER | NOVEMBER 15, 2019



Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information

Majorities think their personal data is less secure now, that data collection poses more risks than benefits, and believe it is not possible to go through daily life without being tracked

...but struggle to **take action**

60% Password Reuse: Password Security Needs a Forced Reset

📅 July 22, 2021 👤 Brian Barr 🏷️ Account Takeover, Password Security

Even Google engineers are confused about Google's privacy settings

"The current UI feels like it is designed to make things possible, yet difficult enough that people won't figure it out."

By [Elizabeth Lopatto](#) | [@mslopatto](#) | Aug 26, 2020, 6:30pm EDT

Taking action is difficult



“Users' rejection of the security advice they receive is **entirely rational** from an economic perspective.”

-- Cormac Herley, 2009

“Consider whether the game has been **designed** and **rigged** so that they can't care about privacy.”

-- Alessandro Acquisti, 2013



Why motivating actions?

Why motivating actions?

SPEND

Consumers lost \$56 billion to identity fraud last year—here's what to look out for

Published Tue, Mar 23 2021•12:56 PM EDT

Oct 11, 2019, 11:32am EDT | 16,344 views

Social Media Is Fostering A Big Rise In Real-World Stalking

**Goal: improving people's security & privacy
(S&P) behaviors**

What

prevents people from
adopting S&P behaviors?

How

can we improve people's
S&P behaviors?

**Understand
Hurdles**

**Develop
Solutions**

**Generate
Impacts**

Understand Hurdles

Develop Solutions

Generate Impacts

Qualitative methods

Consumer reactions to breaches [SOUPS'18]
In-lab study on privacy controls [CHI'20a]
Child safety in smart homes [CSCW'21]

Quantitative methods

Consumer reactions to breaches [USENIXSec'21a]
Behavior adoption & abandonment [CHI'20b]

Artifact analysis

Usability of breach notifications [CHI'19a]
Usability of privacy controls [SOUPS'19a]

Understand
Hurdles

Develop
Solutions

Generate
Impacts

**Qualitative
methods**

Consumer reactions to breaches [SOUPS'18]
In-lab study on privacy controls [CHI'20a]
Child safety in smart homes [CSCW'21]

**Quantitative
methods**

Consumer reactions to breaches [USENIXSec'21a]
Behavior adoption & abandonment [CHI'20b]

**Artifact
analysis**

Usability of breach notifications [CHI'19a]
Usability of privacy controls [SOUPS'19a]

**Design &
Evaluation**

Phishing warnings [CHI'19b]
Privacy controls for smart speakers [PoPETs'20]
Privacy icons [CHI'21]
Support for abuse survivors [USENIXSec'21b]

Understand
Hurdles



Drive changes in
product design



Shape privacy
regulations

Develop
Solutions



Generate
Impacts

Lead public-facing
educational efforts

Improving people's security and privacy behaviors



Understanding
consumer reactions
to data breaches

What



Designing
icons to convey
privacy controls



Supporting
survivors of tech-
enabled abuse

How

Data Breaches

Privacy Icons

Help Survivors

Future work

Improving people's security and privacy behaviors



Understanding
consumer reactions
to data breaches



Designing
icons to convey
privacy controls



Supporting
survivors of tech-
enabled abuse

Content warning: intimate partner violence, stalking, harassment

Improving people's security and privacy behaviors



Understanding
consumer reactions
to data breaches



Designing
icons to convey
privacy controls



Supporting
survivors of tech-
enabled abuse

The number of data breaches in 2021 has already surpassed last year's total

BY CHRIS MORRIS

October 6, 2021 3:30 PM EDT

The number of data breaches in 2021 has already total

BY CHRIS MORRIS

October 6, 2021 3:30 PM EDT

Identity thieves raked in billions with your data, even as breaches fell in 2020

On Data Privacy Day, here's a reminder that breaches can affect you long after your data is stolen.

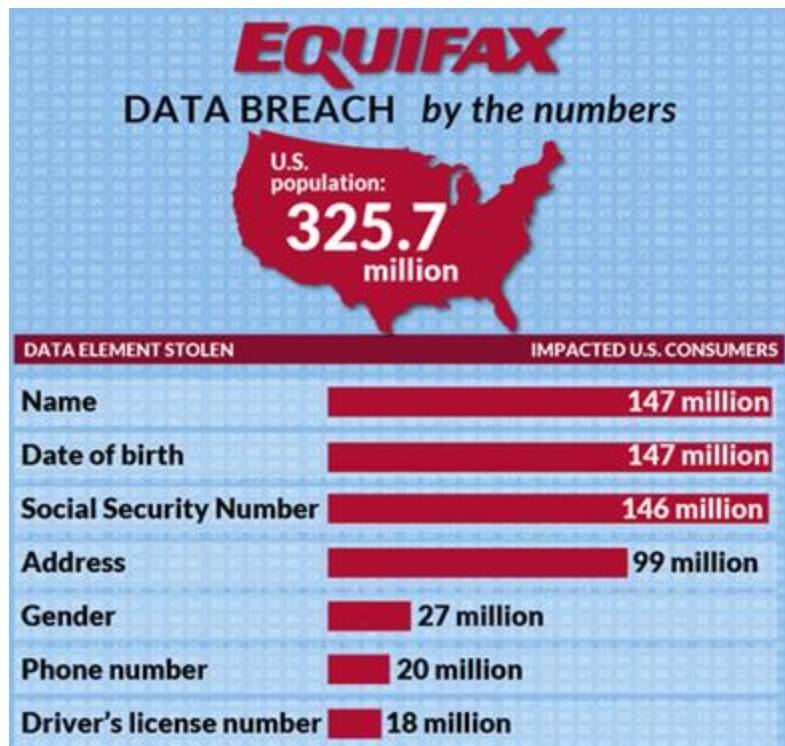


Laura Hautala 

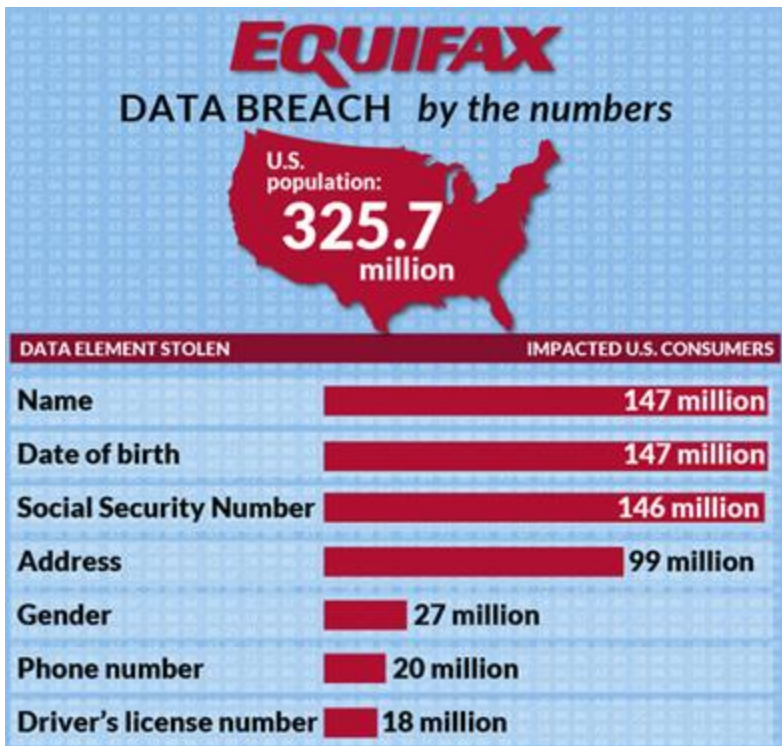
Jan. 28, 2021 1:25 p.m. PT

▶ LISTEN - 02:53





"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach
Y. Zou, A. Mhaidli, A. McCall, F. Schaub. SOUPS 2018. *[Distinguished Paper Award]*



Aware of risks, limited action



Optimism bias



Tendency to delay



Misconceptions regarding protective measures

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach
Y. Zou, A. Mhaidli, A. McCall, F. Schaub. SOUPS 2018. [Distinguished Paper Award]

Can we quantify consumer reactions to data breaches?

→ An online survey on consumers' responses to real-world breaches that had **exposed their personal information**

"Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them
P. Mayer*, Y. Zou*, F. Schaub, A. Aviv. USENIX Security 2021. [** co-first authorship*]

Methodological innovation

Prior work

- **Recall** past experiences w/ breaches
- **Imagine** reactions in hypothetical scenarios

Our method

Present participants w/ specific breaches that exposed their info:



High ecological validity



Low recall bias

We recruited 413 participants from Prolific, a platform for crowdsourcing behavioral research.

Please enter your most commonly used email address

You may search for another email address later, but for now, we are primarily interested in breaches that may have involved your most commonly used email address.

Please enter your email address here:

Our method

Present participants w/
specific breaches that
exposed their info



Breach 1 of 2

Your email address was part of the following breach

KICKSTARTER

Kickstarter (kickstarter.com)

In February 2014, the crowdfunding platform [Kickstarter](#) announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

Compromised data: Email addresses, Passwords

Example questions for individual breaches

Awareness

“Prior to the study, were you aware that you’re affected by this breach?”

Concern

“Please describe how you think this breach has or will impact your life.”

Behavior

“Please select how likely you are to initiate each of the following actions within the next 30 days.”

At the end, we debriefed participants with a full list of breaches and available resources.

Finding: Most participants affected by breaches

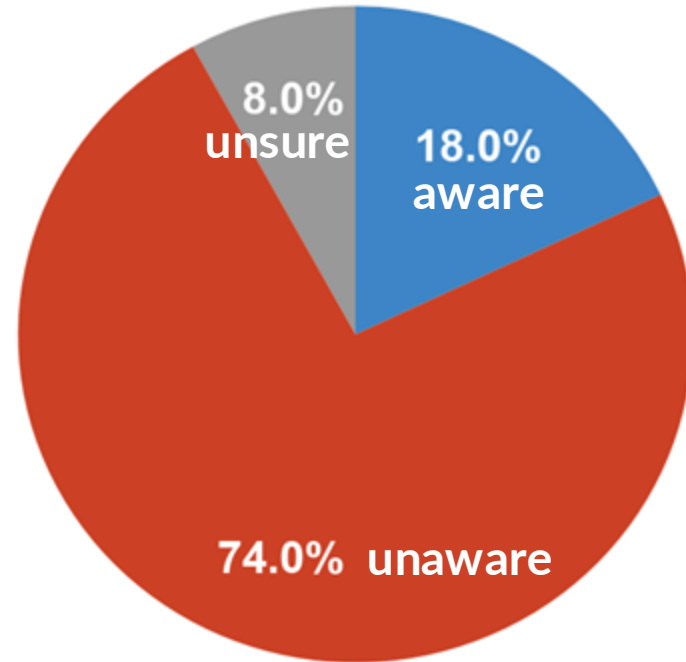
73%

of participants had one or more breaches for their provided email address.

5.4 breaches per participant on average.

Finding: Awareness of breaches was low

“Prior to this study, were you aware that you are affected by this breach?”
(n=792)



Finding: Limited perceived impact

In more than half of responses, participants assessed the breach's impact as **none** (343; 43%) or **very little** (85; 11%).

Finding: Limited perceived impact

In more than half of responses, participants assessed the breach's impact as **none** (343; 43%) or **very little** (85; 11%).

Experienced impact

"I receive phone calls constantly from scam artists [...] It has caused me to rarely ever answer my phone."

Anticipated impact

"The only thing is scammers occasionally attempt to access some of my older accounts that hold no sensitive information."

	Est.	OR	95% CI	p-value
(Intercept)	-3.27	0.04	[0.002, 0.61]	.02
Awareness yes (vs. no)	5.97	390.48	[45.72, 3334.79]	< 0.001
Breach age years	-0.03	0.97	[0.77, 1.21]	.77
Num. of types numeric	.12	1.13	[0.85, 1.50]	.39
Password yes (vs. no)	-0.18	0.84	[0.18, 3.79]	.82
Physical Addr. yes (vs. no)	-0.26	0.77	[0.16, 3.71]	.75
Phone Num. yes (vs. no)	-0.29	0.75	[0.19, 3.02]	.69
Date of birth yes (vs. no)	-0.24	0.79	[0.17, 3.62]	.76
IP Addr. yes (vs. no)	-0.20	0.82	[0.26, 2.64]	.74
Name yes (vs. no)	-0.19	0.83	[0.21, 3.22]	.79
Concern numeric	0.80	2.22	[1.28, 3.86]	.005

Finding: Awareness and concern motivated action

Logistic regression: predictors of having taken any of the ten provided actions

	Est.	OR	95% CI	p-value
(Intercept)	-3.27	0.04	[0.002, 0.61]	.02
Awareness yes (vs. no)	5.97	390.48	[45.72, 3334.79]	< 0.001
Breach age years	-0.03	0.97	[0.77, 1.21]	.77
Num. of types numeric	.12	1.13	[0.85, 1.50]	.39
Password yes (vs. no)	-0.18	0.84	[0.18, 3.79]	.82
Physical Addr. yes (vs. no)	-0.26	0.77	[0.16, 3.71]	.75
Phone Num. yes (vs. no)	-0.29	0.75	[0.19, 3.02]	.69
Date of birth yes (vs. no)	-0.24	0.79	[0.17, 3.62]	.76
IP Addr. yes (vs. no)	-0.20	0.82	[0.26, 2.64]	.74
Name yes (vs. no)	-0.19	0.83	[0.21, 3.22]	.79
Concern numeric	0.80	2.22	[1.28, 3.86]	.005

Finding: Awareness and concern motivated action

Being aware of the breach increases the odds of having taken action (OR=390.48, $p < .001$)

Logistic regression: predictors of having taken any of the ten provided actions

	Est.	OR	95% CI	p-value
(Intercept)	-3.27	0.04	[0.002, 0.61]	.02
Awareness yes (vs. no)	5.97	390.48	[45.72, 3334.79]	< 0.001
Breach age years	-0.03	0.97	[0.77, 1.21]	.77
Num. of types numeric	.12	1.13	[0.85, 1.50]	.39
Password yes (vs. no)	-0.18	0.84	[0.18, 3.79]	.82
Physical Addr. yes (vs. no)	-0.26	0.77	[0.16, 3.71]	.75
Phone Num. yes (vs. no)	-0.29	0.75	[0.19, 3.02]	.69
Date of birth yes (vs. no)	-0.24	0.79	[0.17, 3.62]	.76
IP Addr. yes (vs. no)	-0.20	0.82	[0.26, 2.64]	.74
Name yes (vs. no)	-0.19	0.83	[0.21, 3.22]	.79
Concern numeric	0.80	2.22	[1.28, 3.86]	.005

Finding: Awareness and concern motivated action

For a one-unit increase in concern (5-point scale), the odds of having taken action increase by a factor of 2.2 ($p=.005$)

Logistic regression: predictors of having taken any of the ten provided actions

Implication: Issues with data breach notifications

Data breach notifications are **legally required**

- Unclear in communicating risks
- Overload consumers with too many actions



You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications
Y. Zou, S. Danino, K. Sun, F. Schaub. CHI 2019.

Implication: Innovation in notification methods

74% of breaches were new to participants



Notify consumer of breaches as part of their browsing experience

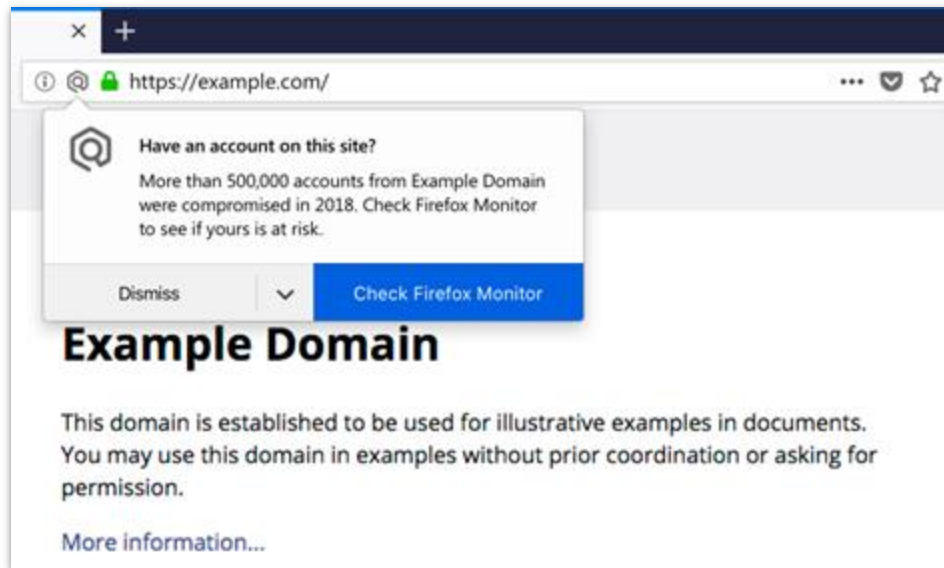
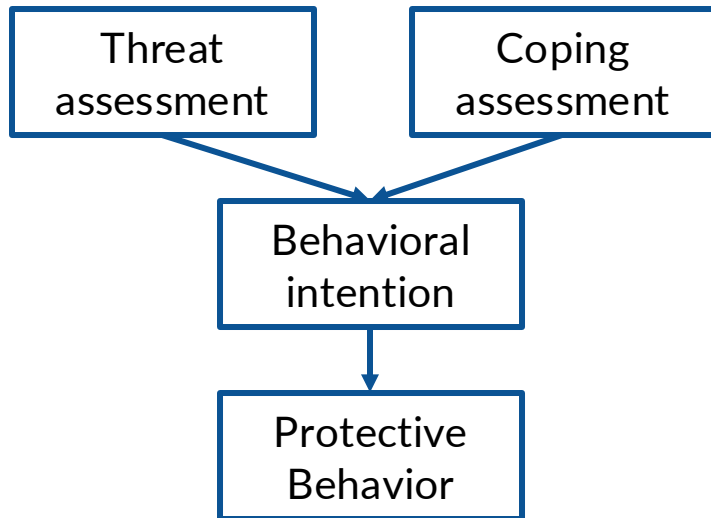


Image: Firefox's website breach notification feature; source: Tech Crunch

Ongoing work on improving breach notifications

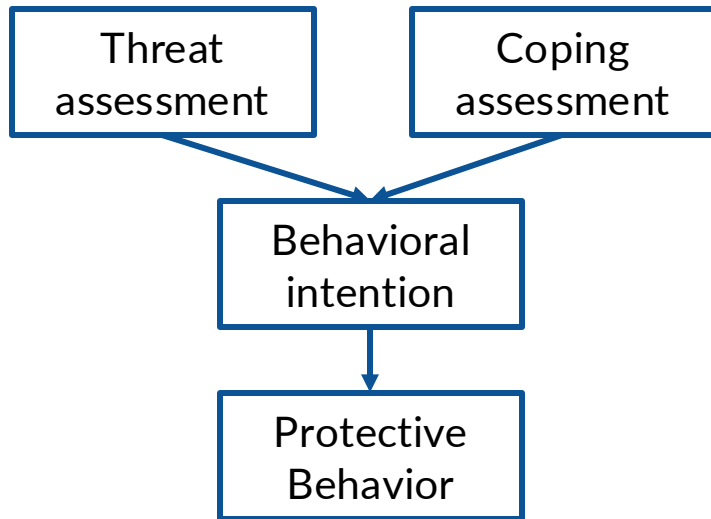


Protection Motivation Theory

Motivating Password Changes after Data Breaches Using the Protection Motivation Theory

Yixin Zou, Khue Le, Peter Mayer, Byron Lowens, Adam Aviv, Florian Schaub. Manuscript in preparation.

Ongoing work on improving breach notifications



Protection Motivation Theory

Highlight threats

	Yes	No
Yes	Change breached passwords	
No		

Highlight coping

Motivating Password Changes after Data Breaches Using the Protection Motivation Theory

Yixin Zou, Khue Le, Peter Mayer, Byron Lowens, Adam Aviv, Florian Schaub. Manuscript in preparation.

Promote changes through public policy

Shared policy recommendations w/
the US Federal Trade Commission.

**Issues with Data Breach Notifications and
Implications for Public Policy**
PrivacyCon, 2019

**Individuals' Awareness, Perception, and
Responses to Data Breaches that Affected Them**
PrivacyCon, 2021

**Consumers' Reactions to Data Breaches,
Deficiencies of Breach Notifications &
Opportunities for Public Policy**
FTC Internal Seminar, 2021



Summary: consumer reactions to data breaches



Intellectual contribution

Empirically show consumers' low awareness of data breaches, limited concern, and how awareness and concern motivate action using an innovative methodology



Broader impact

Inform the design of breach notifications and possible changes in data breach regulations (e.g., invited talks at the FTC)

Improving people's security and privacy behaviors



Understanding
consumer reactions
to data breaches



Designing
icons to convey
privacy controls

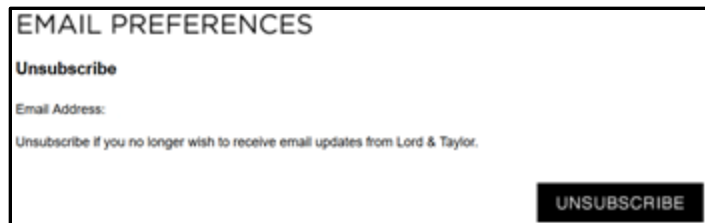


Supporting
survivors of tech-
enabled abuse

How to improve S&P behaviors through better design?

Example privacy controls

Marketing email opt-out



EMAIL PREFERENCES

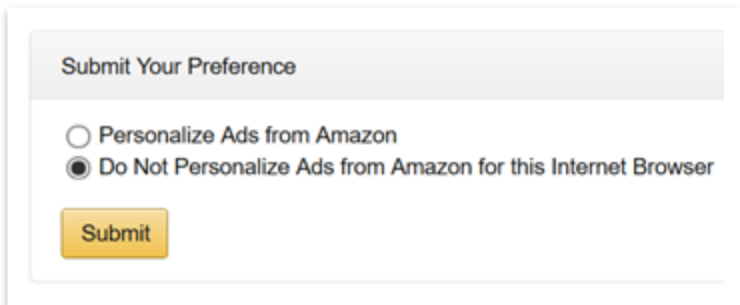
Unsubscribe

Email Address:

Unsubscribe if you no longer wish to receive email updates from Lord & Taylor.

UNSUBSCRIBE

Targeted advertising opt-out



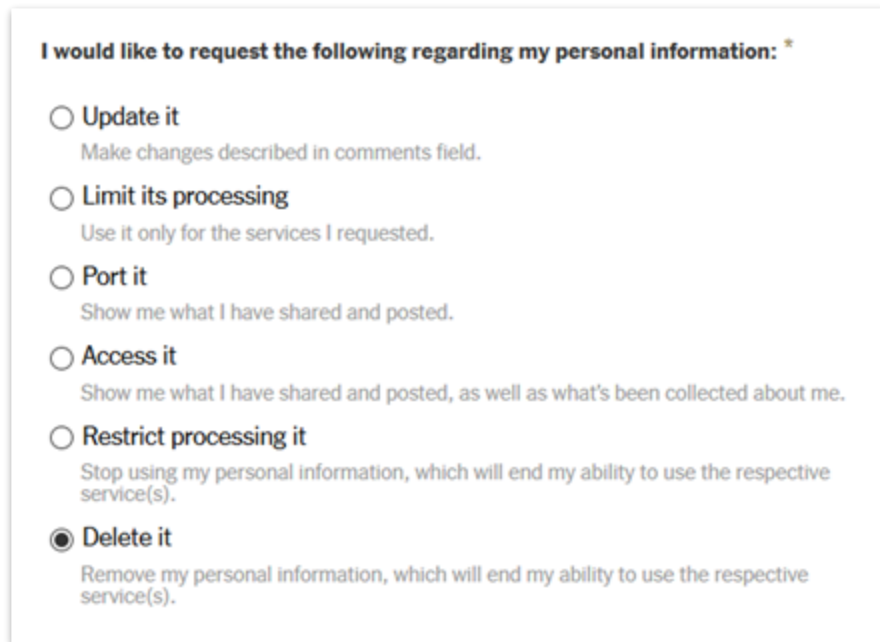
Submit Your Preference

☐ Personalize Ads from Amazon

☒ Do Not Personalize Ads from Amazon for this Internet Browser

Submit

Account deletion options



I would like to request the following regarding my personal information: *

☐ Update it
Make changes described in comments field.

☐ Limit its processing
Use it only for the services I requested.

☐ Port it
Show me what I have shared and posted.

☐ Access it
Show me what I have shared and posted, as well as what's been collected about me.

☐ Restrict processing it
Stop using my personal information, which will end my ability to use the respective service(s).

☒ Delete it
Remove my personal information, which will end my ability to use the respective service(s).

Usability issues with existing privacy controls

Users struggle with finding,
learning, using, & assessing
privacy controls

An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites

H.Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. Cranor, N. Sadeh, F. Schaub. SOUPS 2019.

"It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices

H. Habib, S. Pearman, J. Wang, Y. Zou, ... N. Sadeh, F. Schaub. CHI 2020. *[FPF Privacy Paper for Policymakers Honorable Mention]*

Data Breaches

Privacy Icons

Help Survivors

Future work

Usability issues with existing privacy controls

Users struggle with finding, learning, using, & assessing privacy controls

**Which one to click
for email opt-outs?**

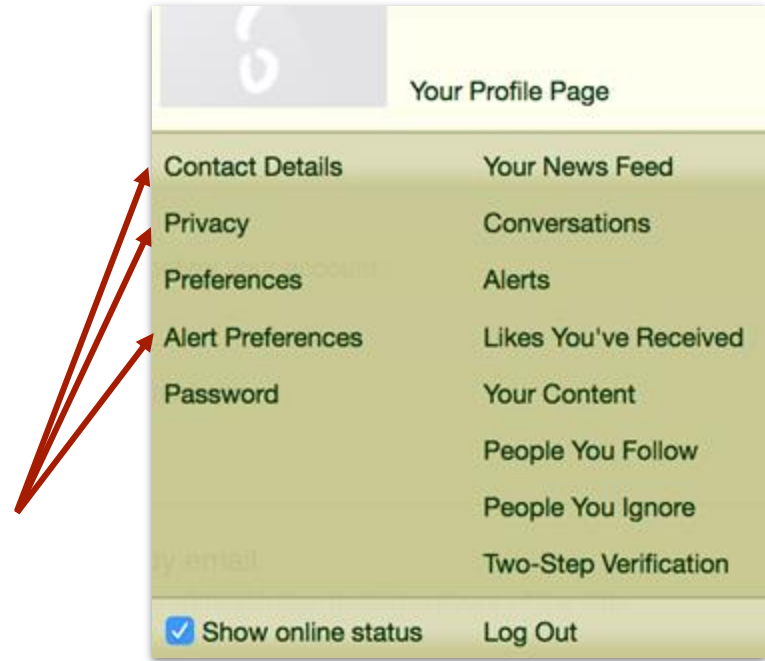


Image: screenshot of settings menu on majorgeeks.com

How to help users better find privacy controls?

→ A series of design workshops & experiments on **icons** that convey the presence of privacy controls

Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts
H. Habib*, Y. Zou*, Y. Yao, A. Acquisti, L. Cranor, J. Reidenberg, N. Sadeh, F. Schaub. CHI 2021. [** co-first authorship*]

Icons to the rescue!

Icons...

- guide attention
- communicate concepts concisely
- can be language & culture independent
- help with recognition



Icons in regulation

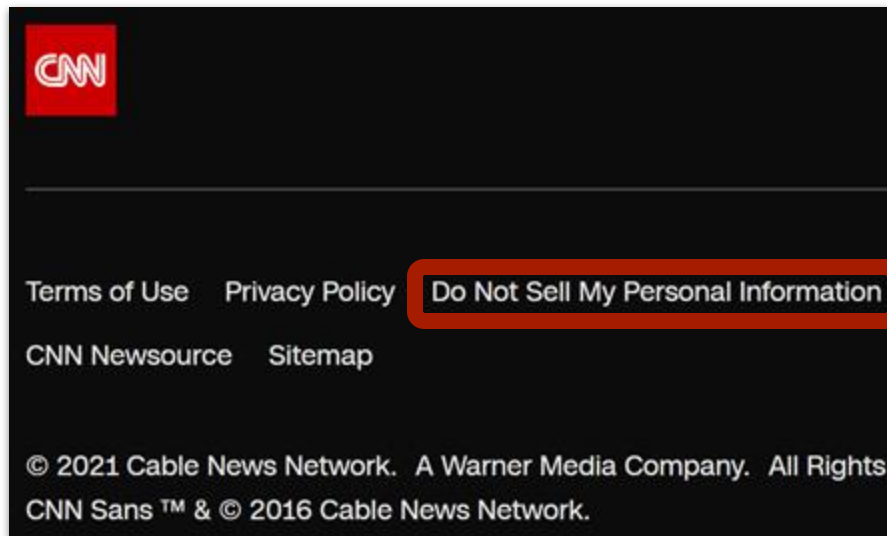


California
Consumer
Privacy
Act

Icons in regulation



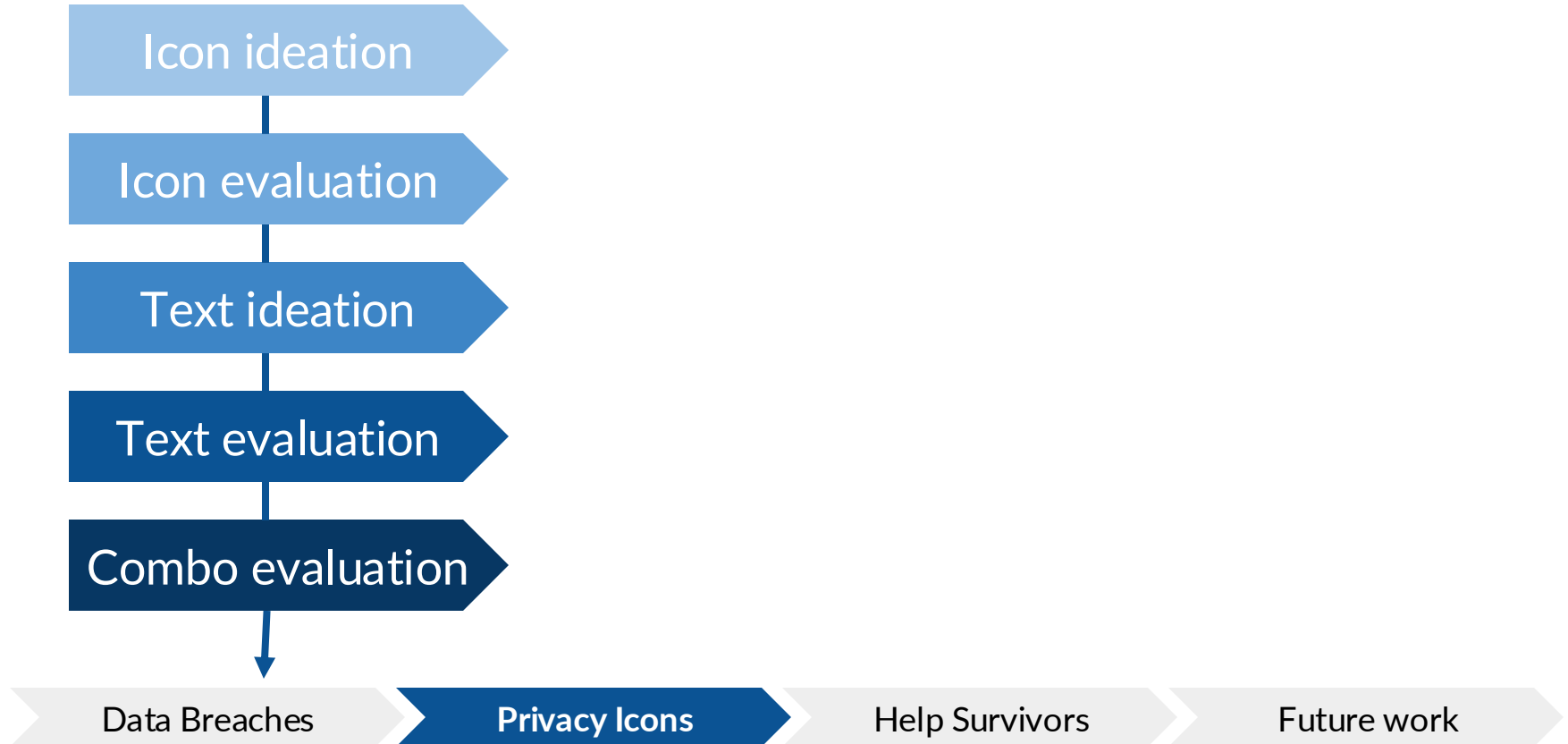
California Consumer Privacy Act



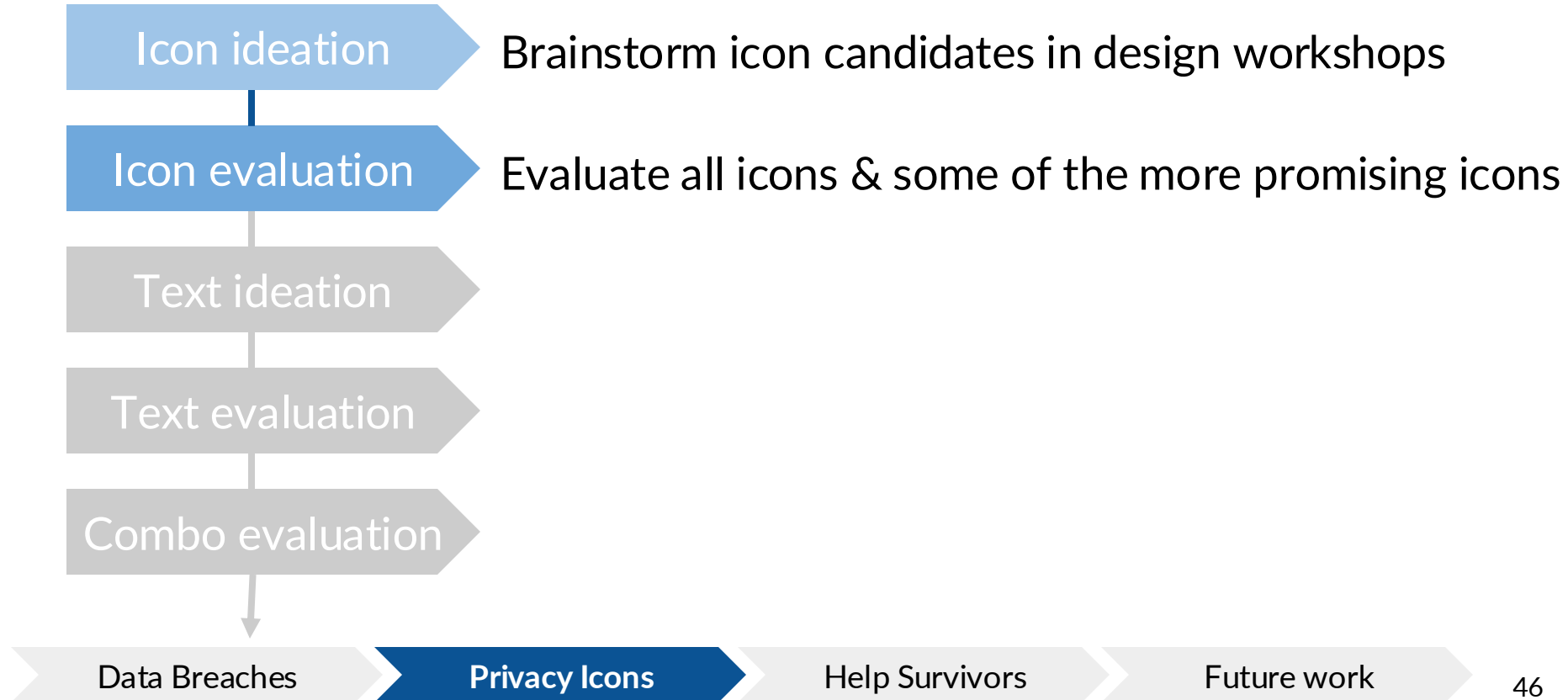
(e) Opt-Out Button or Logo

(1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]

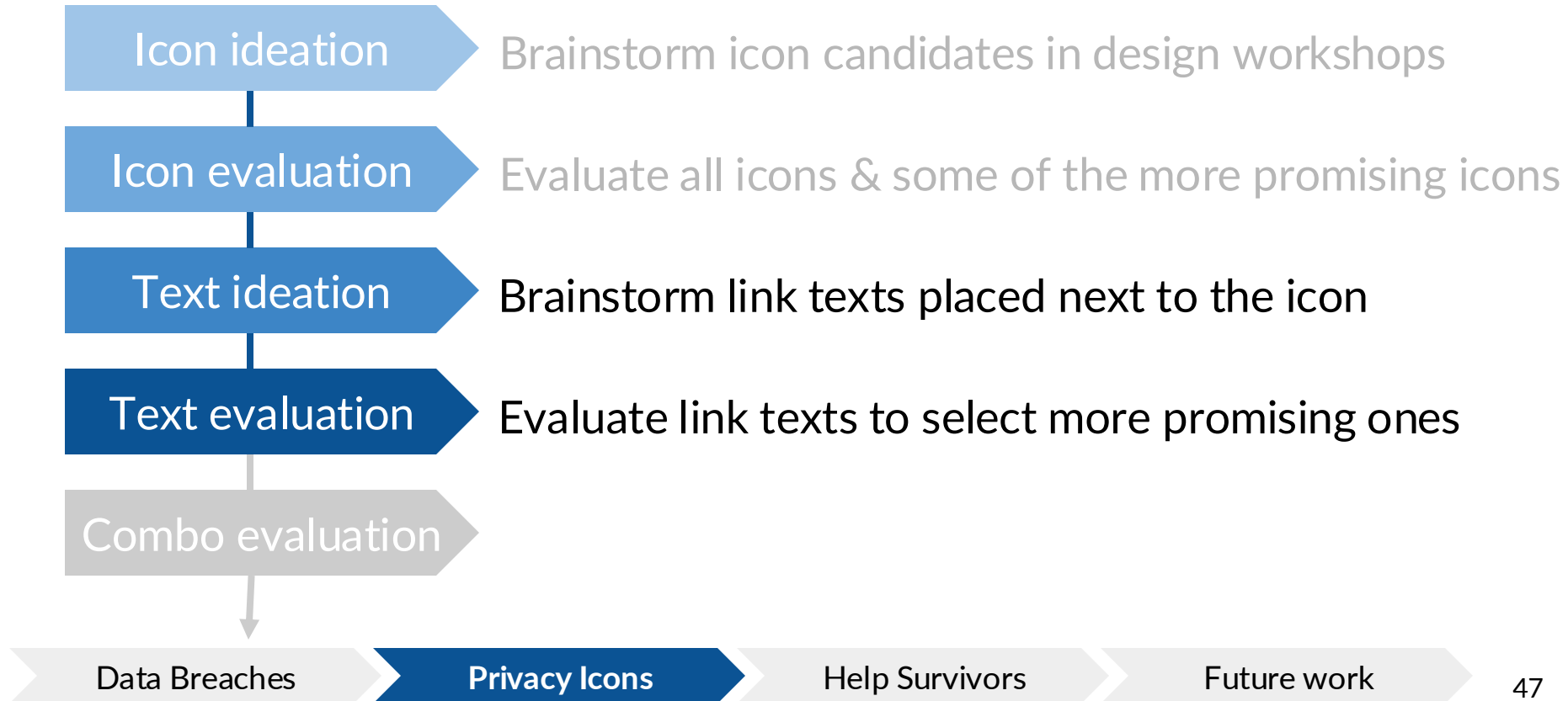
Iterative design and evaluation process



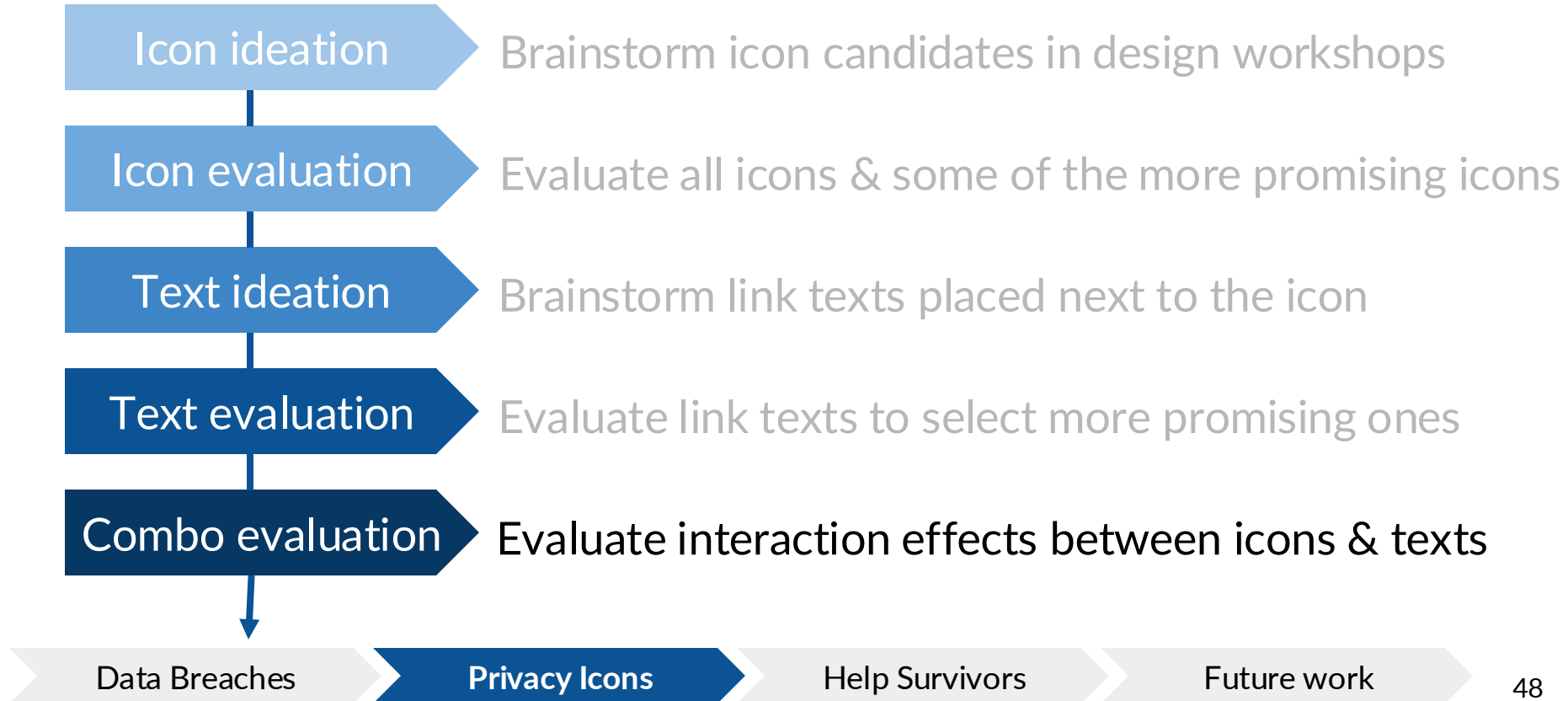
Iterative design and evaluation process



Iterative design and evaluation process



Iterative design and evaluation process



Icon ideation on three concepts

- choice / consent
- opting out
- do-not-sell



Icon candidates for evaluation

Choice/consent



Opting out



Do not sell (personal info)



DAA Privacy Rights

Refined colored icons



Refined colored icons



Evaluating links texts as icon companions

Do Not Sell My Personal Information

Do Not Sell My Info

Don't Sell My Info

Do Not Sell

Don't Sell

Do-Not-Sell Choices

Do-Not-Sell Options

Do-Not-Sell Opt-Outs

Privacy Choices

Privacy Options

Privacy Opt-Outs

Personal Info Choices

Personal Info Options

Personal Info Opt-Outs

Do Not Sell My Info Choices

Do Not Sell My Info Options

Evaluating icon-link text combinations

3 icons + no icon



5 link texts + no link text

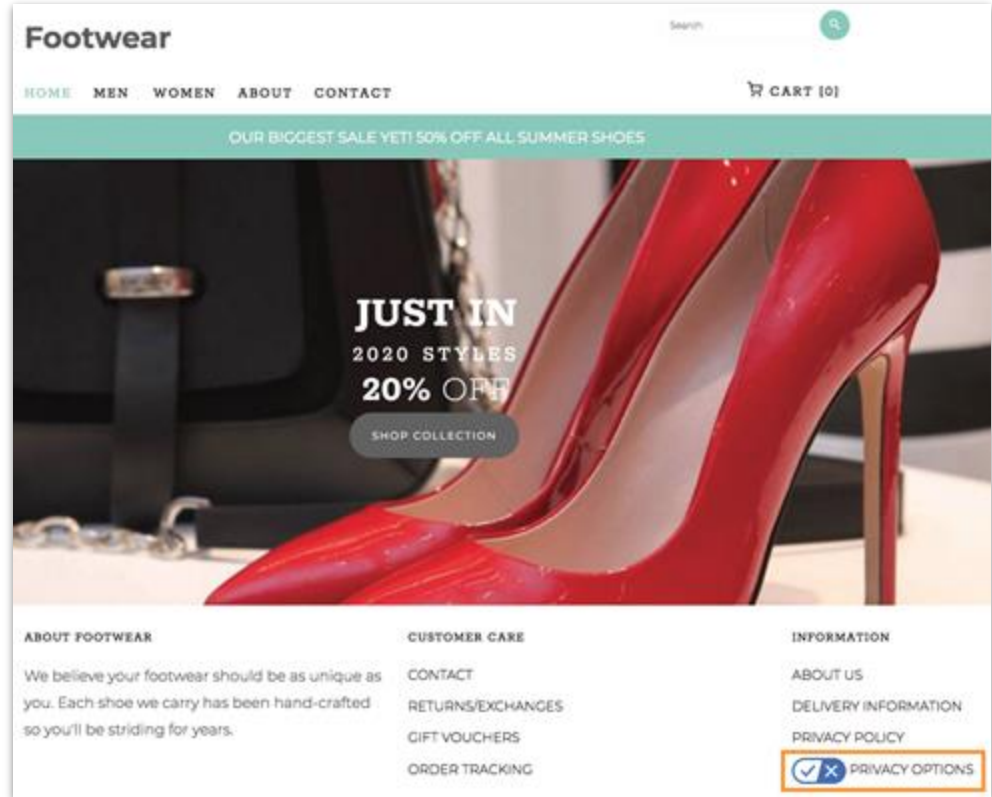
- Do not sell my personal information
- Do not sell my info
- Privacy choices
- Privacy options
- Personal info choices

23 combinations tested with 1,468 MTurk participants in a **between-subjects** design

Evaluating icon-link text combinations

“What do you think would happen if you clicked on the symbol / link?”


- Free-text response
- Rate scenario likelihood



Icon-link text combination findings

Misconceptions

“Personal info choices” --
shoe sizes, site settings, etc.


 payment options (e.g.,
secure payment)

None of the icons performed
well without a link text

Icon-link text combination findings


Misconceptions


“Personal info choices” --
shoe sizes, site settings, etc.

 payment options (e.g.,
secure payment)

None of the icons performed
well without a link text

Recommended combinations

 Privacy Options
...for choices about personal info

 Do Not Sell My
Personal Information
...for do-not-sell choices

Communicating findings with policymakers

Submitted recommendations to the California Office of Attorney General (OAG) in February 2020



Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA

L. Cranor, H. Habib, Y. Zou, A. Acquisti, J. Reidenberg, N. Sadeh, F. Schaub. Technical Report.

Data Breaches

Privacy Icons

Help Survivors

Future work

Our recommended icon



OAG's revised proposed regulations

(1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.



(2) When the opt-out button is used, it shall appear to the left of the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link, as demonstrated below, and shall be approximately the same size as other buttons on the business’s webpage. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]



Do Not Sell My Personal Information



Do Not Sell My Info

Our
recommended
icon



iOS toggle
switch



OAG's revised proposed regulations

- (1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.



- (2) When the opt-out button is used, it shall appear to the left of the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link, as demonstrated below, and shall be approximately the same size as other buttons on the business’s webpage.
[BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]





Alex Stamos  @alexstamos · 14h

Quick, tell me what that button indicates in its current state. Are you opted into your data being used or out? Red X next to "Do Not", so does that cancel out the not?

The California AG's office is now mandating really bad interaction design. Great job, everybody.



Aaron Alva @aalvatar · 2h

This is terribly confusing. Was this disclosure user tested to make sure users' expectations align with what you're trying to convey? (Likely not)

We expect companies to do user testing; we should expect governments to do same.

one resource: ftc.gov/news-events/ev... #CCPA

Follow-up evaluation on OAG's icon

stylized-toggle



CalAG toggle



CalAG-X toggle



+ swapped colors

Follow-up evaluation on OAG's icon

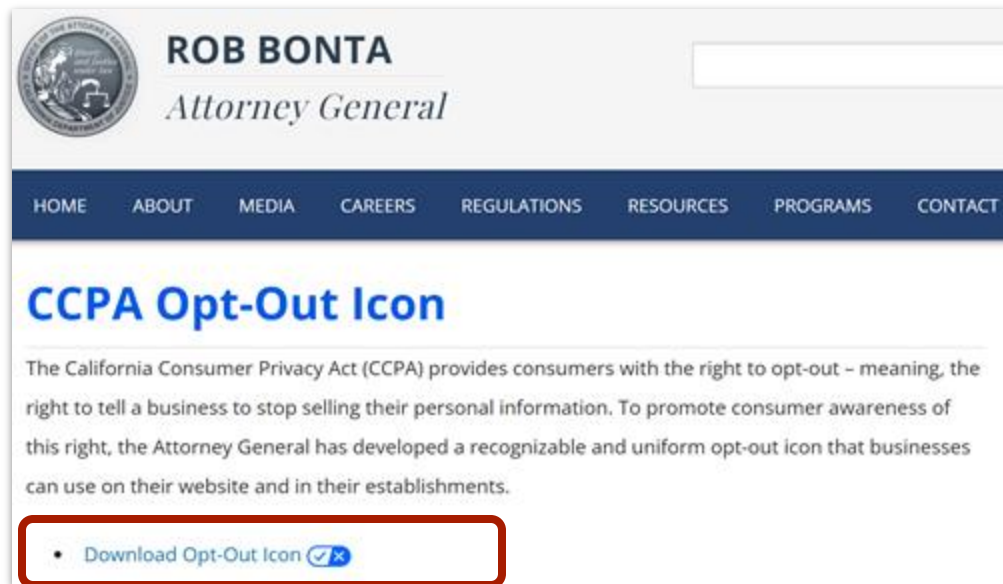


- Insignificant difference between big vs. small “X” or red vs. blue
- Big differences between the CalAG icon and our stylized toggle: CalAG icon more likely to be **misinterpreted** as an **actual toggle**

Direct impact on California privacy regulations

OAG removed the problematic icon from draft regulations

Amended CCPA regulations
in March 2021 →



<https://oag.ca.gov/privacy/ccpa/icons-download>

Summary: privacy icons design & evaluation



Intellectual contribution

Novel designs of privacy icons that convey the presence of privacy controls with few misconceptions, supported by user testing



Broader impact

Direct influence on the California Consumer Privacy Act (CCPA) — an exemplar of informing public policy with evidence from research

Improving people's security and privacy behaviors



Understanding
consumer reactions
to data breaches



Designing
icons to convey
privacy controls



Supporting
survivors of tech-
enabled abuse

How to consider users' needs in developing solutions?

Survivors of intimate partner violence (IPV)

- Physical control of accounts or devices by the abuser



Survivors of intimate partner violence (IPV)

- Physical control of accounts or devices by the abuser
- Remote surveillance / harassment enabled by tech



Survivors of intimate partner violence (IPV)

- Physical control of accounts or devices by the abuser
- Remote surveillance / harassment enabled by tech
- Routine behaviors could escalate the violence



Reset password



Location setting

How to help IPV survivors stay safe with care and caution?

→ A qualitative study to explore how **computer security customer support** can help IPV survivors

The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence

Y. Zou, A. McDonald, J. Narakornpichit, N. Dell, T. Ristenpart, K. Roundy, F. Schaub, A. Tamersoy. USENIX Security 2021.

Data Breaches

Privacy Icons

Help Survivors

Future work

Computer security customer support can help

- Complement limited tech expertise of IPV professionals
- Support at scale (esp. for large companies)



Computer security customer support can help

- Complement limited tech expertise of IPV professionals
- Support at scale (esp. for large companies)



Such help must be provided **carefully** to avoid inadvertent harm



Research process

1

Qualitative analysis
of chat records



2

Focus groups w/
IPV professionals



3

Focus groups w/
support practitioners



Tech abuse cases exist; agents not prepared



My ex-husband keeps getting my account passwords. I have changed phones so many times and got a restraining order on him, but he still managed to do this. Help me please.



Please do not worry about these problems if you have [product] installed. We will do everything we can to help you further.

Acknowledge the limits of security software

Data Breaches

Privacy Icons

Help Survivors

Future work

Acknowledge the limits of security software



Please do not worry about these problems if you have [product] installed. We will do everything we can to help you further.

- “ The goal should be to **hear** and **be honest** about the limitations of what [product] can or cannot do. (*P11, attorney*) ”
- “ Acknowledge that ‘this is scary’ and that ‘it sounds like you’re having a really hard time.’ (*P2, counselor*) ”

Advise with caution and boundaries



Have a safety check-in

“Do you worry that someone might be listening to or recording our conversation?”

→ If not, offer to reconnect on a safe line. Let them decide.

Advise with caution and boundaries



Have a safety check-in

“Do you worry that someone might be listening to or recording our conversation?”

→ If not, offer to reconnect on a safe line. Let them decide.



Avoid untrained areas

Example out-of-scope advice: comprehensive IPV-related counseling, safety planning, legal advice, etc.

Make external referrals



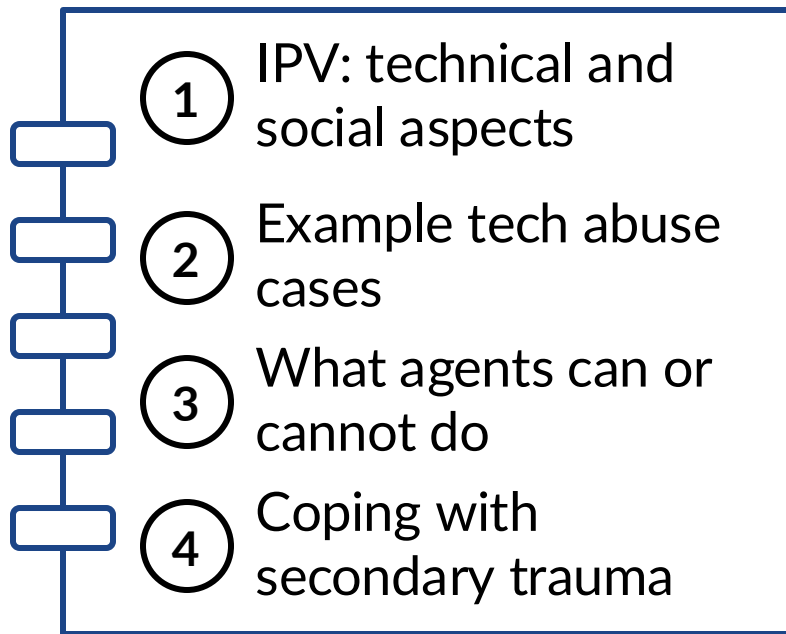
Make external referrals



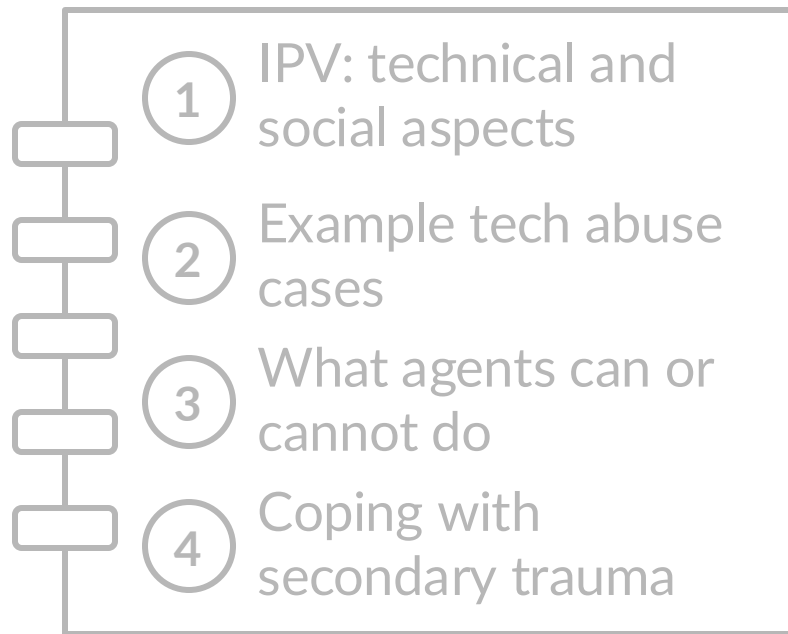
Use trauma-informed language;
avoid potentially harmful labeling

“ I’m not going to say ‘you are a survivor of domestic violence’ [...] Give them the opportunity to **call it in whatever ways they want.** (P14, counselor) ”

Incorporate recommendations into training



Incorporate recommendations into training



“ Regular support agents have **no dedicated training** on this. (S10, director) ”

“ Emphatic language could be done regardless of whether I’m interacting with someone [with] IPV. (S6, director) ”

Summary: helping tech abuse survivors



Intellectual contribution

Showcase the care needed in helping tech abuse survivors through computer security customer support as a novel avenue






Broader impact



Develop training materials for support agents to better handle tech abuse cases

Improving people's security and privacy behaviors

Data breaches

[SOUPS'18] 
[CHI'19a] 
[IEEE&PMag.'19]
[USENIXSec'21a] 



Privacy controls

[SOUPS'19a]
[CHI'20a]  
[PoPETs'20]
[CHI'21]


At-risk populations

[CSCW'21]
[USENIXSec'21b]
[CHI'22]

Abandonment

[CHI'20b]  

Phishing warning

[CHI'19b] 

Developer privacy

[SOUPS'19b]



Distinguished Paper



Best Paper Honorable Mention



Award

Presented at FTC PrivacyCon



FPF Privacy Papers for Policymakers Honorable Mention

Security & Privacy

Trauma-informed

Cross-cultural

Longitudinal

Future Work

Data Breaches

Privacy Icons

Help Survivors

Future work

Trauma-informed computing

Safety

Trust

Peer support

Collaboration

Enablement

Intersectionality

User Research
& DesignArtificial
Intelligence &
Machine Learning**Trauma-Informed Computing: Towards Safer Technology Experiences for All**

J. Chen*, A. McDonald*, Y. Zou*, E. Tseng, K. Roundy, A. Tamersoy, F. Schaub, T. Ristenpart, N. Dell. CHI 2022. [* co-first authorship]

Data Breaches

Privacy Icons

Help Survivors

Future work

Trauma-informed security & privacy solutions

How to inform users of risks & actions while avoiding (re)traumatization?

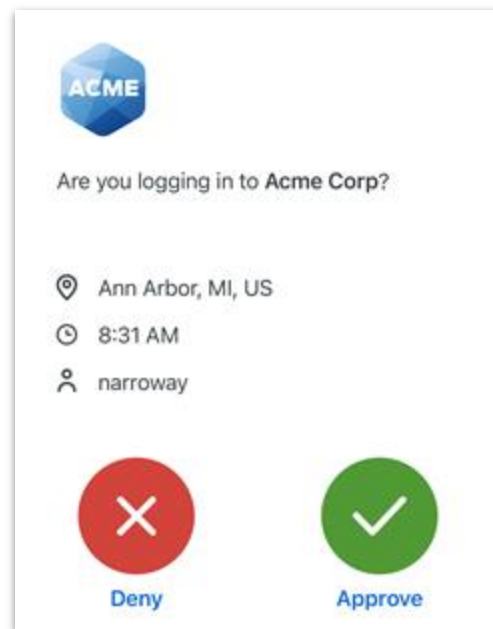
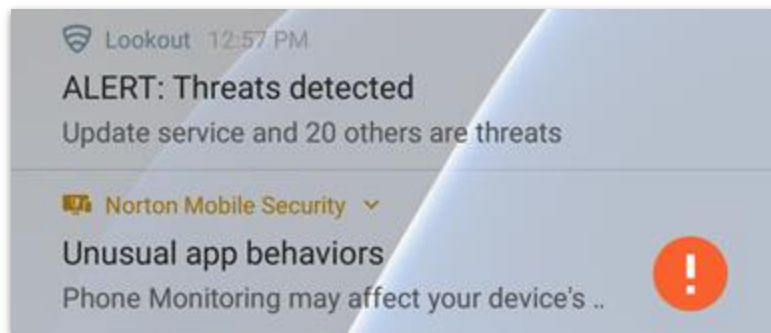


Image: Norton Mobile Security (left); Duo Security (right)

Privacy concerns of Muslim-American women

- Being Muslim-American
- Being Muslim-American women
- Individual religiosity



Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women

T. Afnan, Y. Zou, M. Naseem, M. Mustafa, F. Schaub. Under Review.

A cross-cultural lens of security & privacy

Cross-country studies of people's S&P attitudes and behaviors

How does it inform **tech design** and **regulations**?

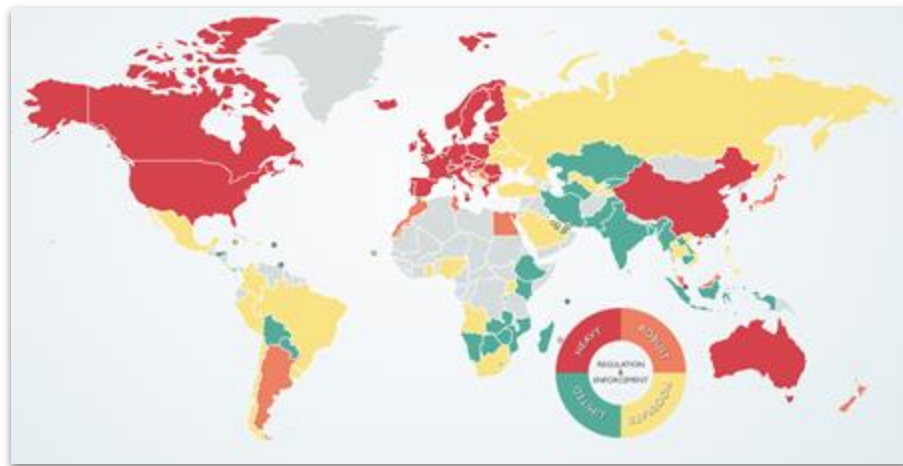
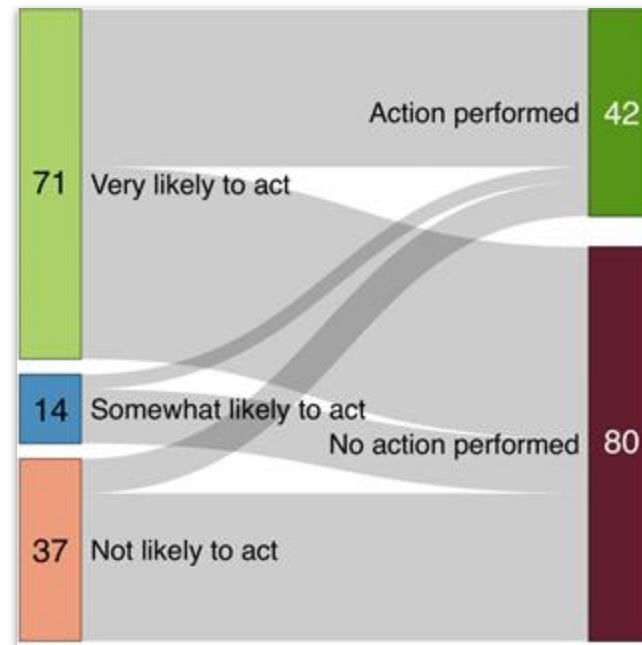


Image: Data Privacy Laws in 2022 by WireWheel

Intention-behavior gap in reacting to data breaches

Less than half who said “very likely to act” actually changed the breached password six months later



The Intention-Behavior Gap in Individuals' Responses to Data Breaches that Affected Them

P. Mayer, [Y. Zou](#), B. Lowens, H. Dyer, K. Le, F. Schaub, A. Aviv. Manuscript in preparation.

Longitudinal security & privacy risks and harms

How do **risks** of being affected by a data breach **materialize** as concrete security incidents?



identity theft



phishing attack

→ Use empirical data to improve expert advice by highlighting which actions to **prioritize**



account compromise

Acknowledgements



Florian
Schaub



Alessandro
Acquisti



Tanisha
Afnan



Adam
Aviv



Janet
Chen



Lorrie
Cranor



Nicola
Dell



Hana
Habib



Byron
Lowens



Peter
Mayer



Allison
McDonald



Abraham
Mhaidli



Justin
Petelka



Thomas
Ristenpart



Kevin
Roundy



Norman
Sadeh



Kaiwen
Sun



Acar
Tamersoy



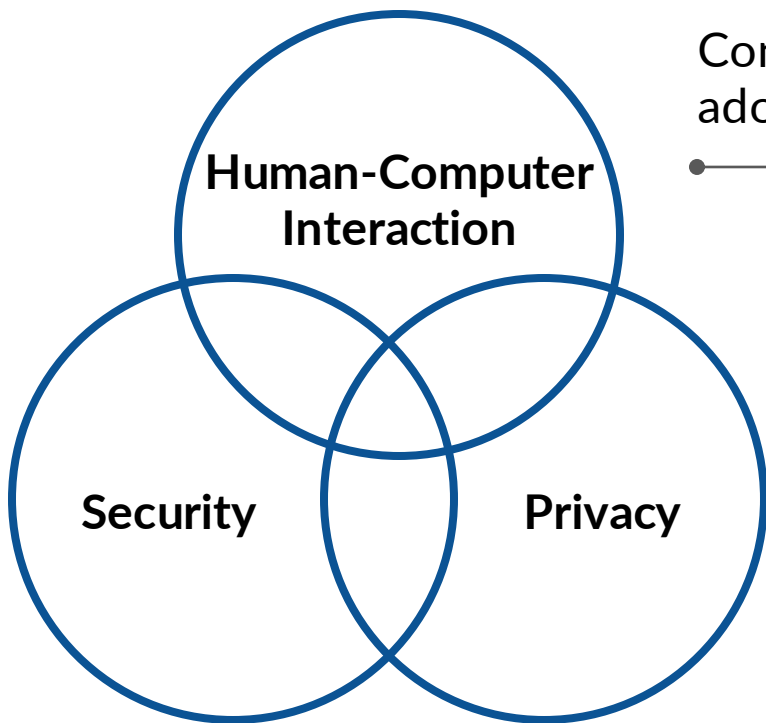
Emily
Tseng



Yaxing
Yao



Improving people's security and privacy behaviors



Contribute novel empirical evidence of hurdles for adopting security and privacy behaviors

Improve people's S&P behaviors with a multi-pronged approach (tech, policy, education)

Policy discussions with stakeholders (e.g., FTC, California OAG) resulting in real-world changes

Future work: trauma-informed, cross-cultural, longitudinal security & privacy

Improving people's security and privacy behaviors

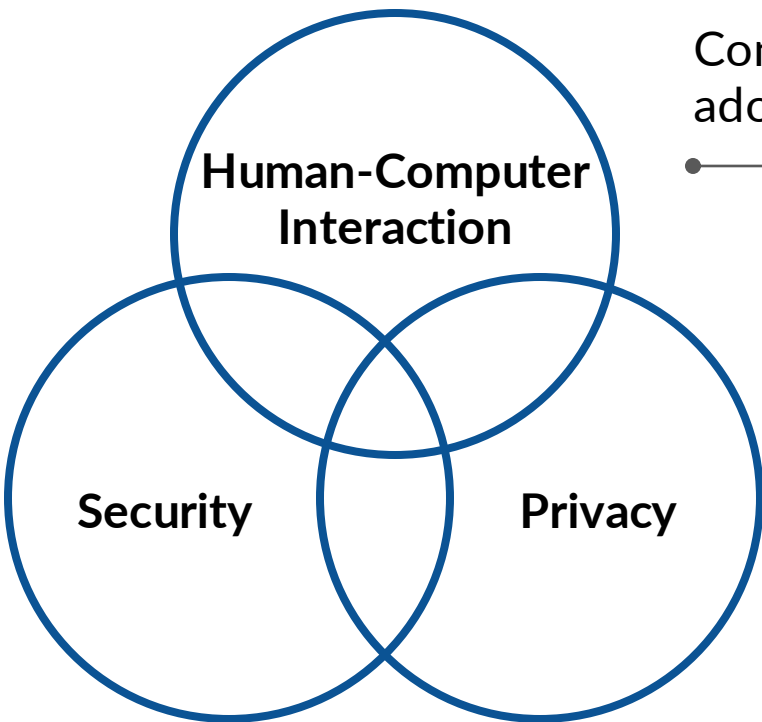
Yixin Zou



yixinz@umich.edu



yixinzou.github.io



Contribute novel empirical evidence of hurdles for adopting security and privacy behaviors

Improve people's S&P behaviors with a multi-pronged approach (tech, policy, education)

Policy discussions with stakeholders (e.g., FTC, California OAG) resulting in real-world changes

Future work: trauma-informed, cross-cultural, longitudinal security & privacy