ACM SIGCHI Outstanding Dissertation Award Talk | May 15, 2024

From Notifications to Icons: Empowering People in the Face of Privacy Risks

Yixin Zou

Human-Centered Privacy and Security

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

60% Password Reuse: Password Security Needs a Forced Reset

July 22, 2021 Brian Barr Account Takeover, Password Security

The New York Times

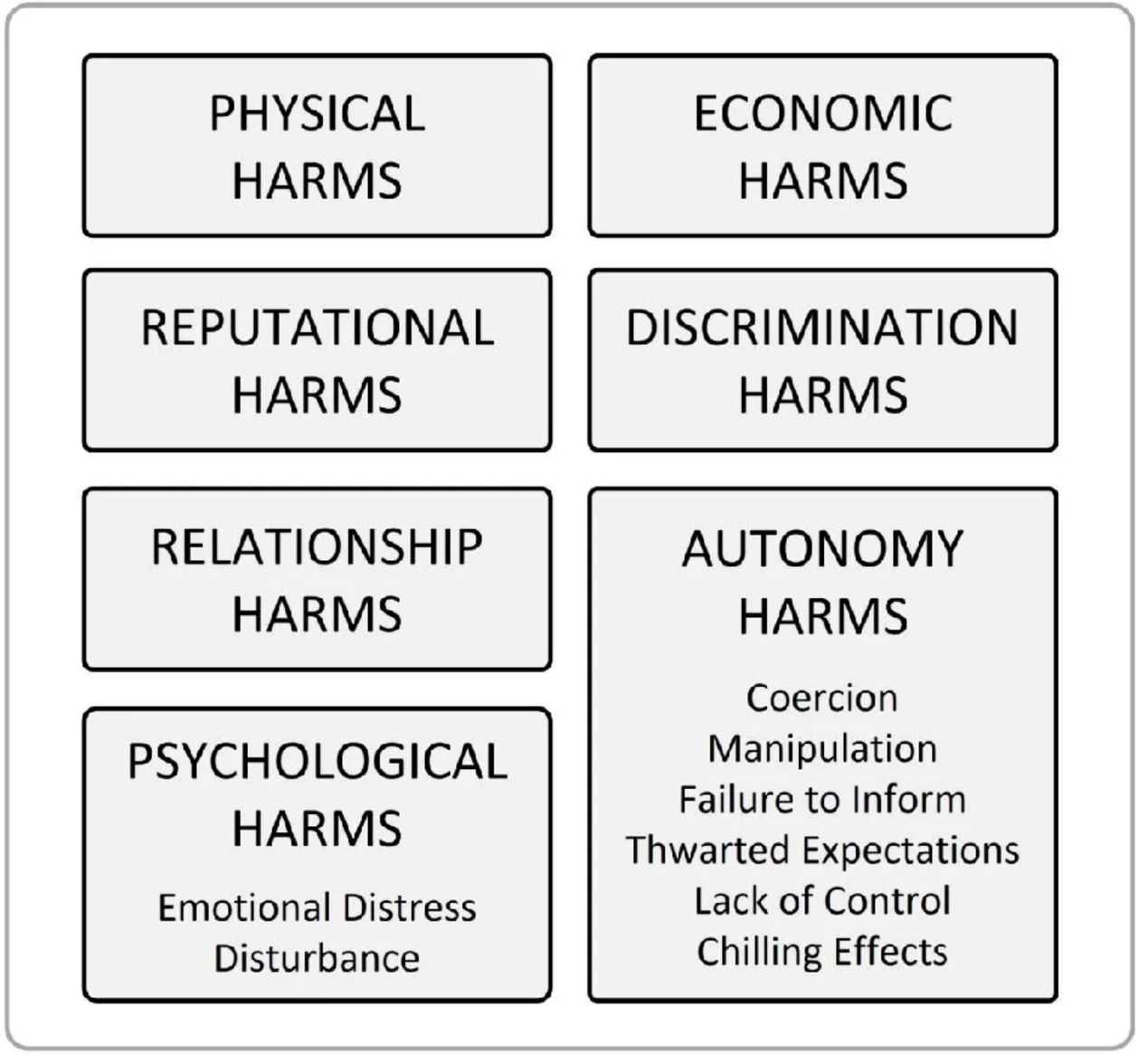
DealBook / Business & Policy

DEALBOOK NEWSLETTER

How Cookie Banners Backfired

An extensive digital privacy law aimed to give internet users more control over their data. Instead, experts say, it's created "almost a useless exercise."

TYPOLOGY OF PRIVACY HARMS



Privacy Harms
Danielle K. Citron and Daniel J. Solove
Boston University Law Review, 102(3), 793-864. 2022.

What prevents people from adopting privacy and security best practices?

How can we improve people's risk perceptions and behaviors?

Dissertation overview

Understand Hurdles

Consumer reactions to data breaches [SOUPS'18, USENIXSec'21a]

Adoption and abandonment of P&S practices broadly [CHI'20]

Dissertation overview

Understand Hurdles

Consumer reactions to data breaches [SOUPS'18, USENIXSec'21a]

Adoption and abandonment of P&S practices broadly [CHI'20]

Develop Solutions

Data breach notifications that motivate consumers to take action [TOCHI]

Icons for communicating privacy controls [CHI'21]

Trauma-informed customer support for abuser survivors [USENIXSec'21b]

Dissertation overview

Understand Hurdles

Consumer reactions to data breaches [SOUPS'18, USENIXSec'21a]

Adoption and abandonment of P&S practices broadly [CHI'20]

Develop Solutions

Data breach notifications that motivate consumers to take action [TOCHI]

Icons for communicating privacy choices [CHI'21]

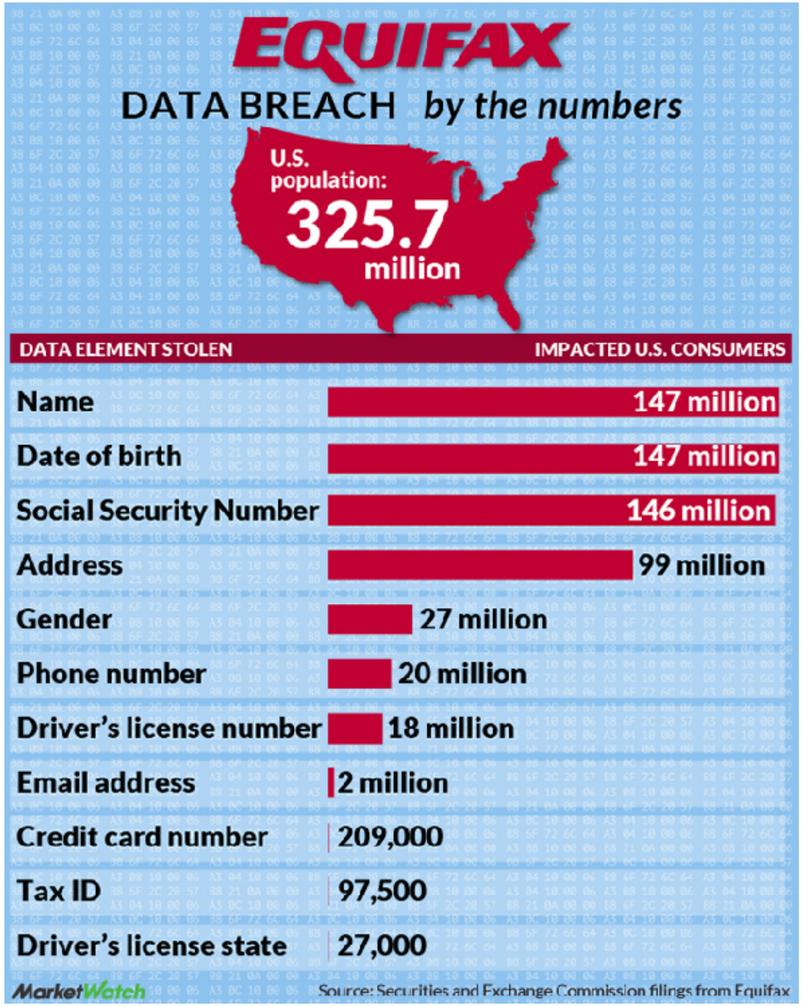
Trauma-informed customer support for abuser survivors [USENIXSec'21b]

Generate Impact

Reasons behind inaction

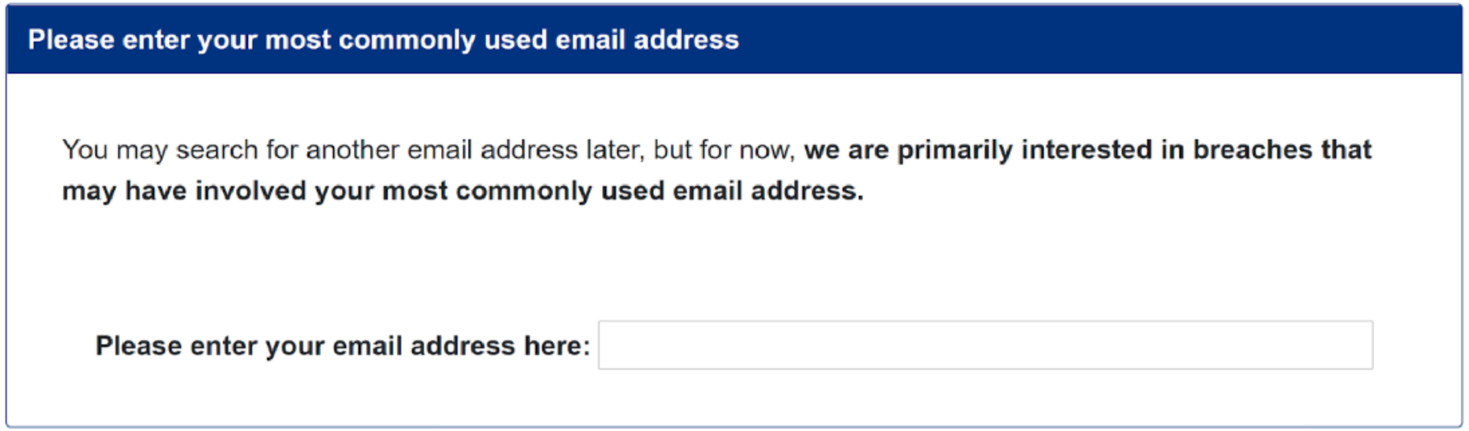
Semi-structured interviews (n=24)

- Optimism bias
- Reactive attitude toward risks
- Misconceptions about protective measures
- Financial costs



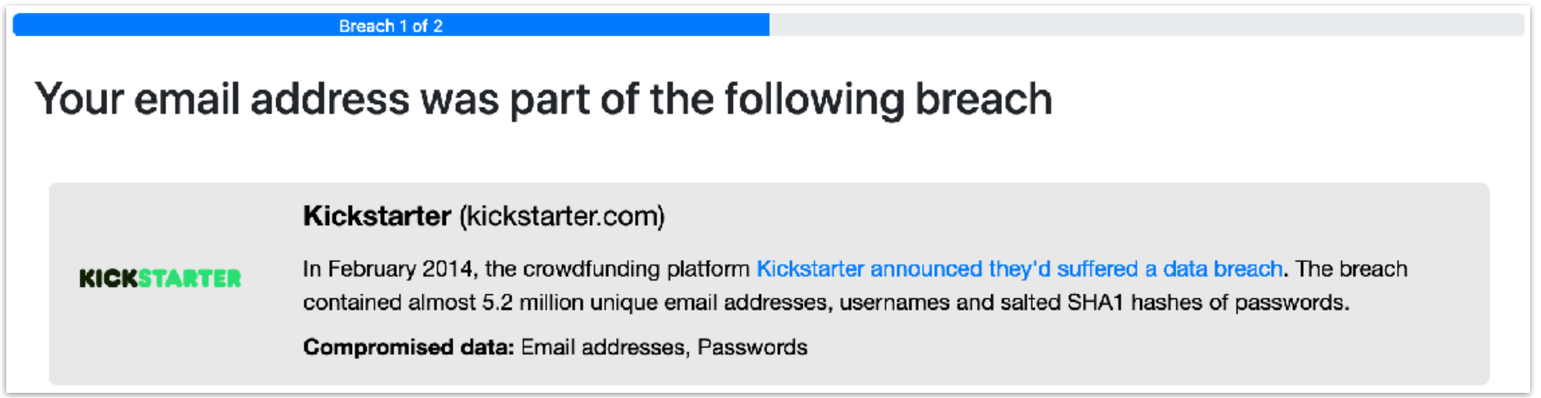
"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions After the Equifax Data Breach
Yixin Zou, Abraham H. Mhaidli, Austin McCall, Florian Schaub
SOUPS: Symposium on Usable Privacy and Security. 2018. *Distinguished Paper Award* 🏆

Study breach reactions at scale



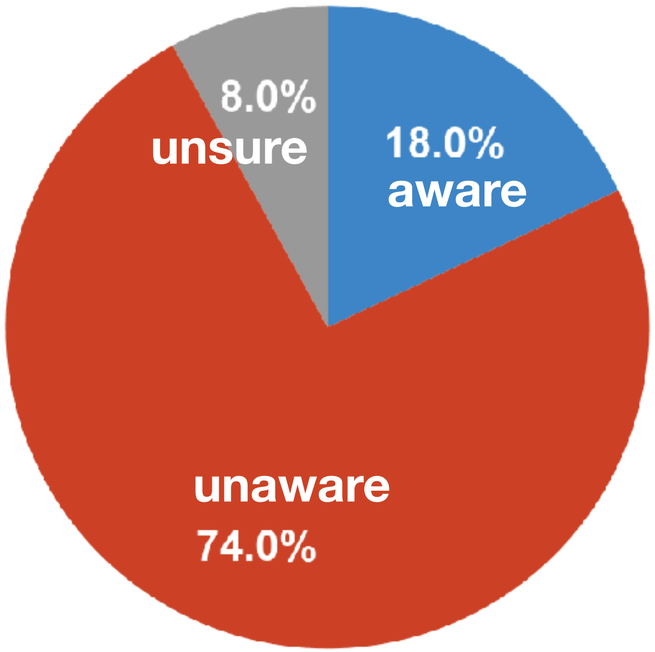
Online survey (n=413)

Real-world breaches affecting participants themselves

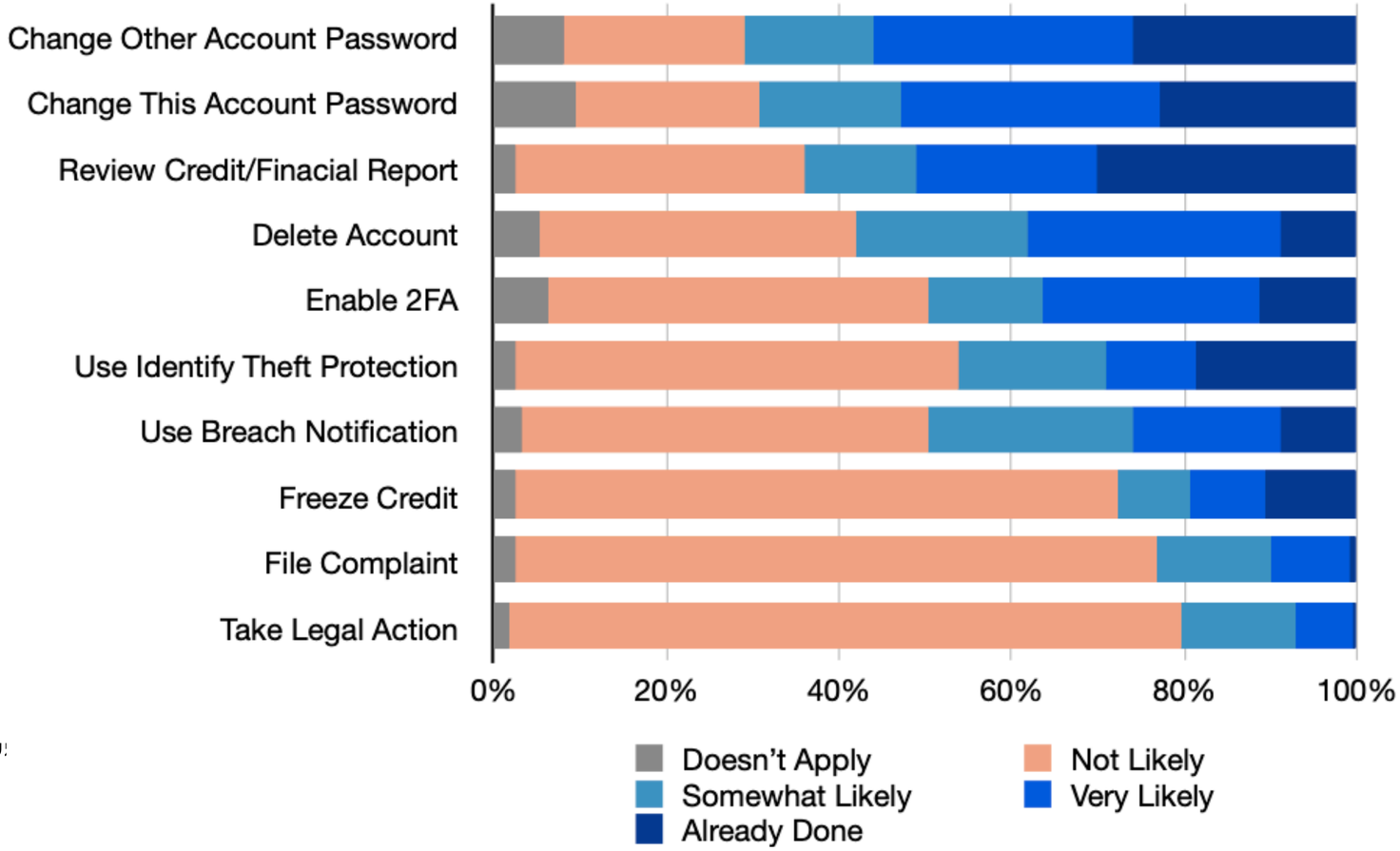


"Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches
Peter Mayer*, Yixin Zou*, Florian Schaub, Adam J. Aviv (*equal contributions)
USENIX Security Symposium. 2020.

Low awareness, limited action



"Prior to this study, were you aware that you are affected by this breach?"



"Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches
Peter Mayer*, Yixin Zou*, Florian Schaub, Adam J. Aviv (*equal contributions)
USENIX Security Symposium. 2020.

Issues with breach notifications

Dear <<First Name>> <<Last Name>>,

This letter is to provide you with information about a data security incident that may have affected your payment card information. The privacy and security of your personal information is extremely important to us as we very much appreciate your business and your confidence in us. We are sending this letter to notify you of the incident, to provide you with information about the nature of the incident, and the steps you can now take to protect your personal information.

What Happened. On October 15, 2021, <<Entity>> Warehouse, LLC ("<<Entity>> Warehouse") we became aware of a potential data security incident. We immediately began an internal investigation and engaged an independent computer forensics firm to determine whether any personal information was affected in the incident. The investigation has been extensive, requiring the analysis of a substantial amount of digital evidence. On November 6, 2021, the investigation determined that payment card information was obtained without authorization on October 1, 2021. On November 29, 2021, the investigation determined that your payment card information may have been affected during the incident.

What Information Was Involved. The incident may have involved payment card information, including your name, address, payment card number <<Last 4 Digits>> , expiration date, and payment card security code.

image source: Maryland Attorney General

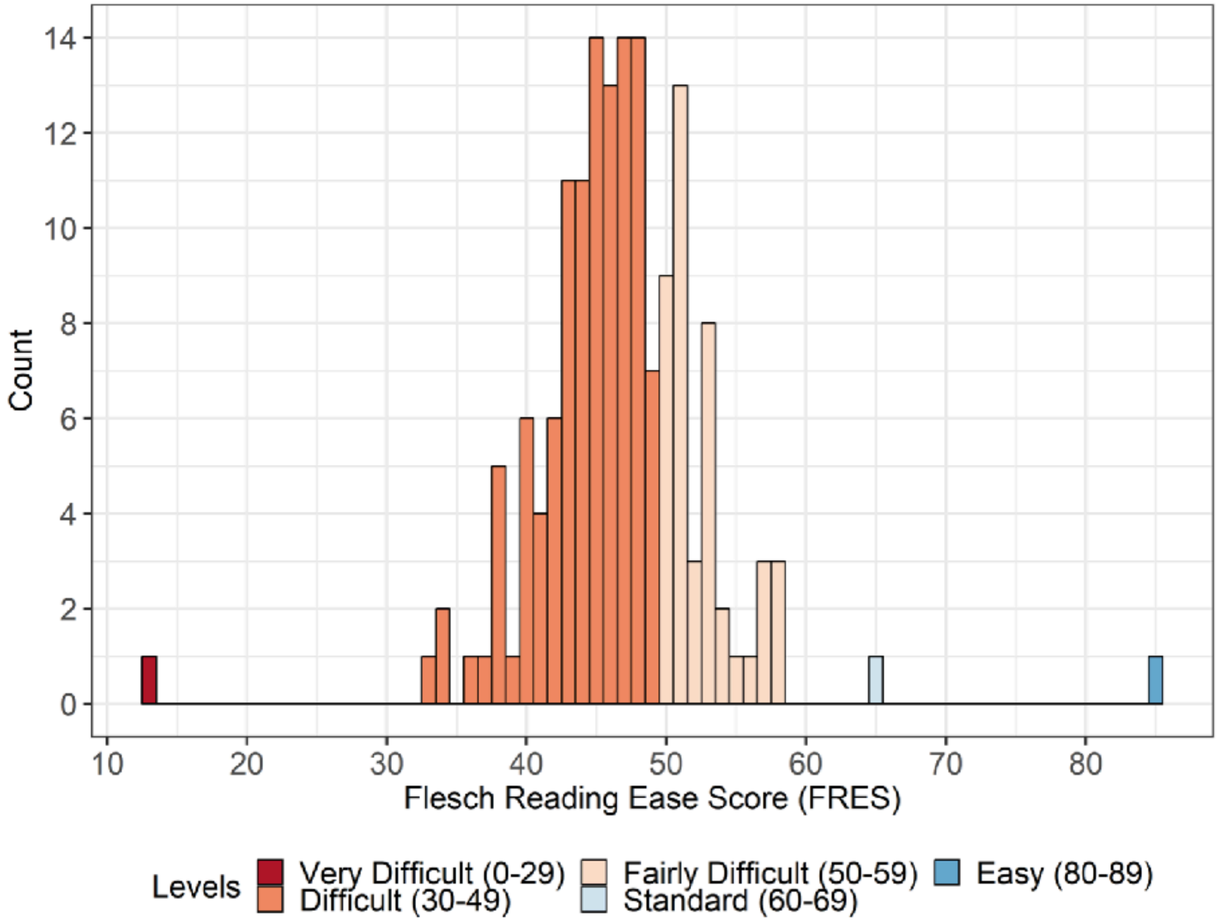
Issues with breach notifications

Content analysis (n=161)

Poor readability

Using hedging terms

Suggesting many
actions with no priority



You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications
Yixin Zou, Shawn Danino, Kaiwen Sun, Florian Schaub
CHI: ACM Conference on Human Factors in Computing Systems. 2019.

Issues with breach notifications

Content analysis (n=161)

Poor readability

Using hedging terms

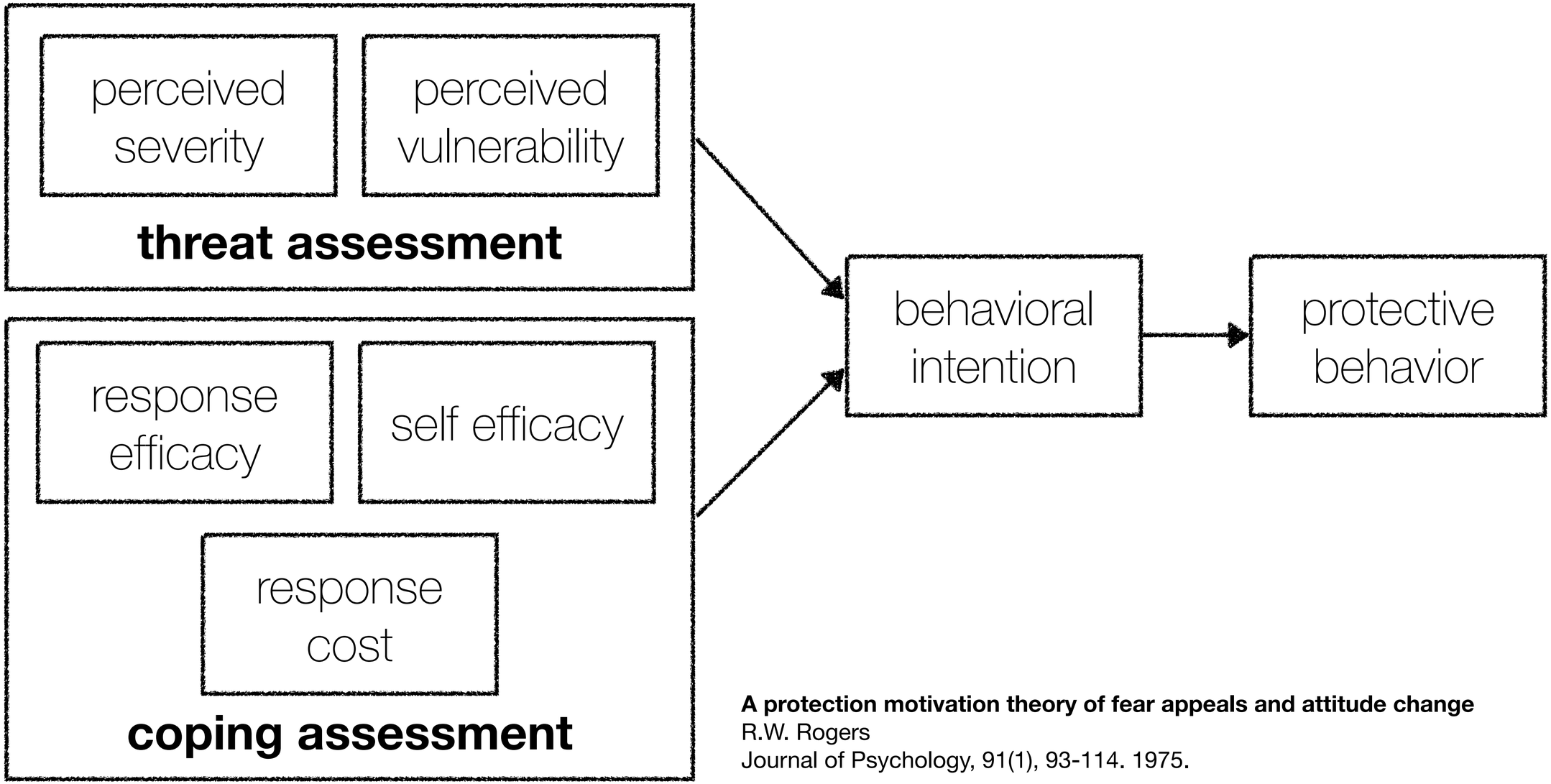
Suggesting many
actions with no priority

We need stronger data breach notification laws!

cfpb Consumer Financial Protection Bureau

You ‘Might’ Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications
Yixin Zou, Shawn Danino, Kaiwen Sun, Florian Schaub
CHI: ACM Conference on Human Factors in Computing Systems. 2019.

Protection Motivation Theory

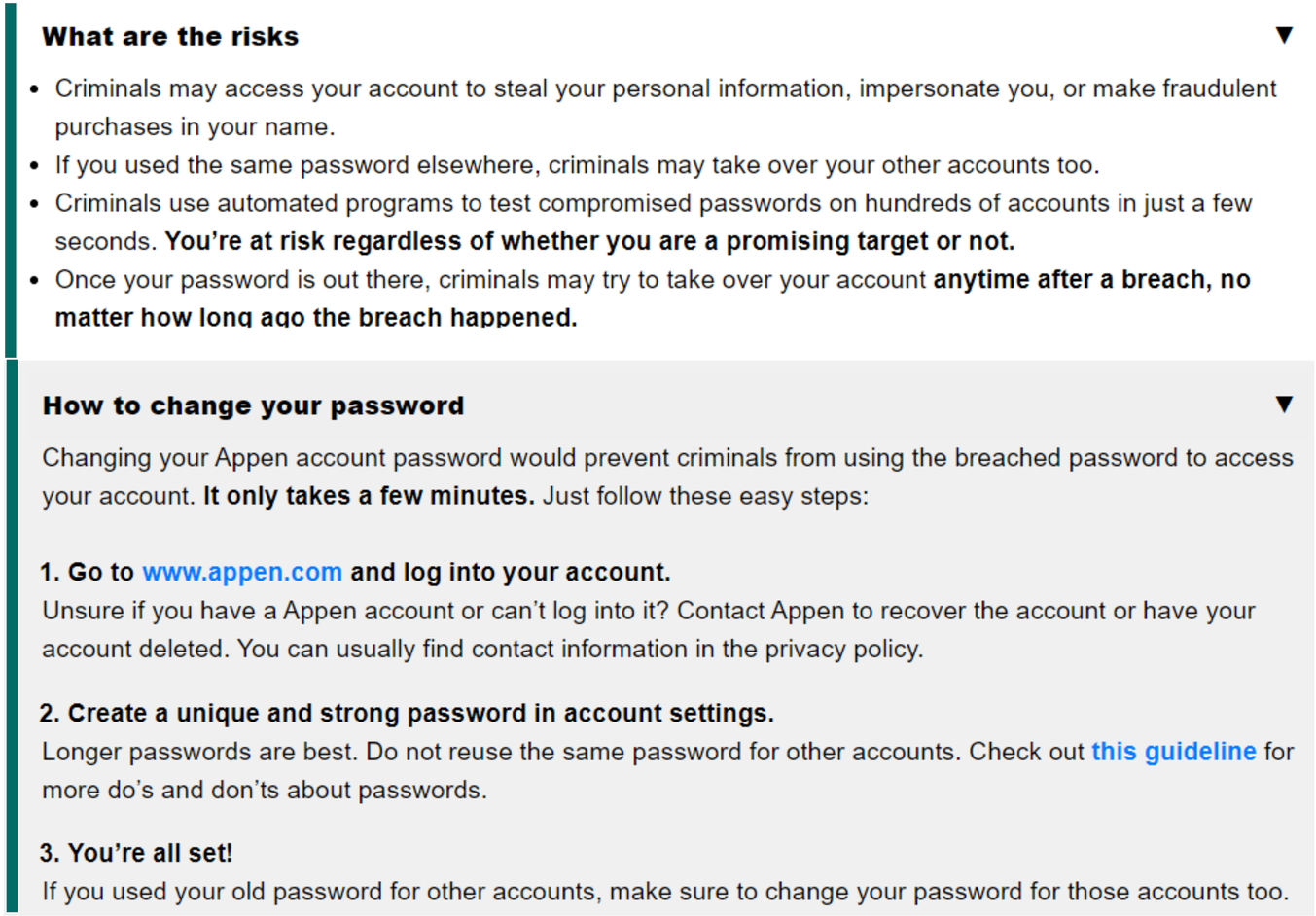


A protection motivation theory of fear appeals and attitude change
R.W. Rogers
Journal of Psychology, 91(1), 93-114. 1975.

Design better breach notifications

threat nudge

coping nudge



Nudging Users to Change Breached Passwords Using the Protection Motivation Theory
Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J. Aviv, Florian Schaub
TOCHI: ACM Transactions on Computer-Human Interaction. Accept with minor revision.

Design better breach notifications

Online experiment (n=1,386)

58-67% showed intention

22-31% changed the password

Conditions	% w/ intention	OR	p-value
Threat only vs. Control	67.3% vs. 58.2%	1.48	.02
Coping only vs. Control	62.9% vs. 58.2%	1.22	.23
Combined vs. Control	62.3% vs. 58.2%	1.19	.30

Conditions	% w/ action	OR	p-value
Threat only vs. Control	28.0% vs. 22.7%	1.32	.14
Coping only vs. Control	27.0% vs. 22.7%	1.26	.23
Combined vs. Control	31.1% vs. 22.7%	1.54	.02

Nudging Users to Change Breached Passwords Using the Protection Motivation Theory
Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J. Aviv, Florian Schaub
TOCHI: ACM Transactions on Computer-Human Interaction. To appear.

Protective behaviors beyond data breaches

Online survey (n=902)

Partial adoption and abandonment of protective behaviors are common

Expert-recommended best practices were perceived “impractical” “not needed”

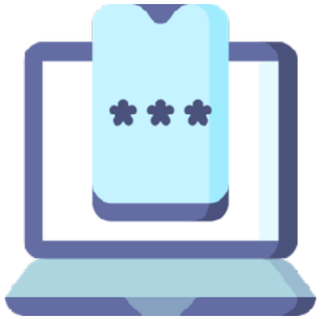


image source: flaticon

Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices
Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, Florian Schaub
CHI: ACM Conference on Human Factors in Computing Systems. 2020. *Best Paper Honorable Mention*

Design better privacy icons

California Consumer Privacy Act

§ 999.315. Requests to Opt-Out

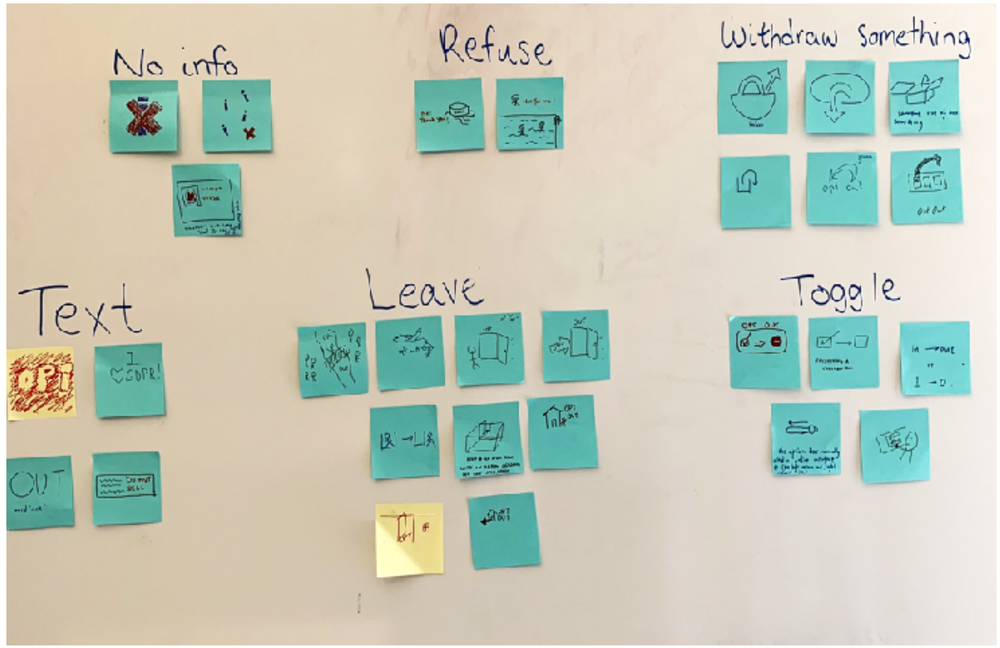
(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's

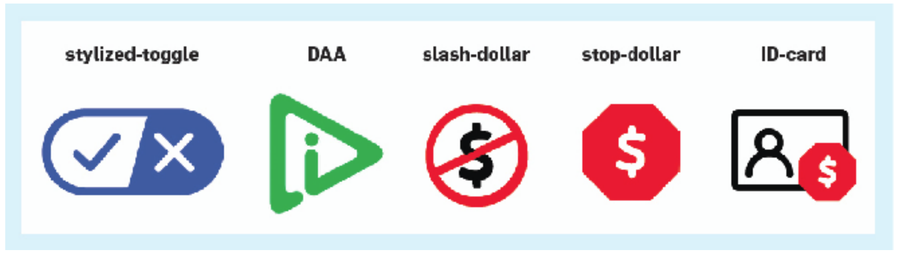
(e) Opt-Out Button or Logo

(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.]

Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts
Hana Habib*, Yixin Zou*, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Joel Reidenberg, Norman Sadeh, Florian Schaub (*equal contributions)
CHI: ACM Conference on Human Factors in Computing Systems. 2021.

Design better privacy icons





Privacy Options

Do Not Sell My Personal Information

Base icons on simple and familiar concepts

Text required next to the icon to avoid misconception (at least for initial adoption)

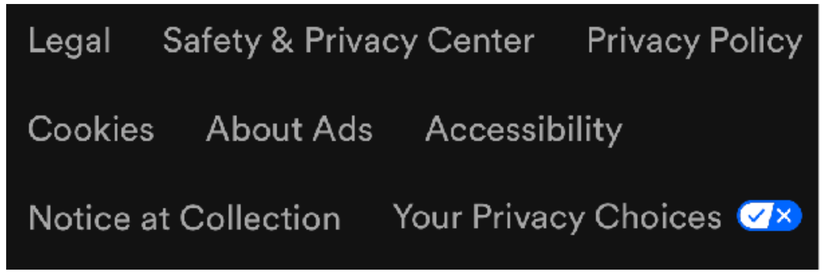
Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts
Hana Habib*, Yixin Zou*, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Joel Reidenberg, Norman Sadeh, Florian Schaub (*equal contributions)
CHI: ACM Conference on Human Factors in Computing Systems. 2021.

Icon recommendations adopted by CCPA

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices," or, "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

Zoom



Spotify

Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts
Hana Habib*, Yixin Zou*, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Joel Reidenberg, Norman Sadeh, Florian Schaub (*equal contributions)
CHI: ACM Conference on Human Factors in Computing Systems. 2021.

Going beyond “the average user”

Survivors of intimate partner violence

Physical control of accounts/devices

Remote surveillance and harassment

Routine protective-behaviors can escalate violence

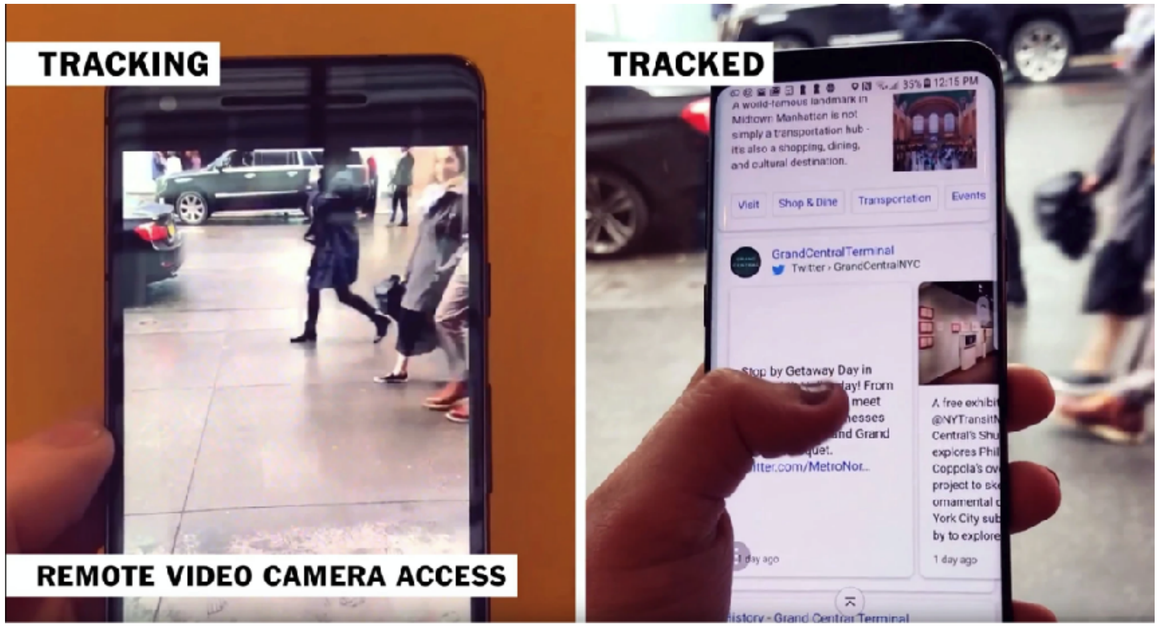


image source: The New York Times

The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence
Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Tom Ristenpart, Kevin Roundy, Florian Schaub, Acar Tamersoy
USENIX Security Symposium. 2021.

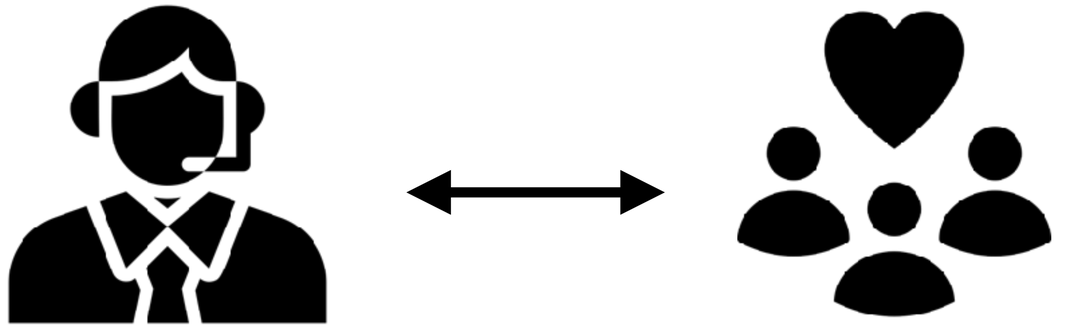
Trauma-informed customer support

Focus groups with IPV and customer support professionals

Use trauma-informed language

Advise with caution and boundaries

Refer to external resources



Computer Security Customer Support

Existing Support Ecosystem

NortonLifeLock™

Coalition Against Stalkerware

The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence
Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Tom Ristenpart, Kevin Roundy, Florian Schaub, Acar Tamersoy
USENIX Security Symposium. 2021.

Understand Hurdles

Consumer reactions to data breaches [SOUPS'18, USENIXSec'21a]

Adoption and abandonment of P&S practices broadly [CHI'20]

Develop Solutions

Data breach notifications that motivate consumers to take action [TOCHI]

Icons for communicating privacy controls [CHI'21]

Trauma-informed customer support for abuser survivors [USENIXSec'21b]

Generate Impact

Drive changes in product design and discussions with regulators

Inform California privacy regulations with research

Yixin Zou
Tenure-Track Faculty, MPI-SP

yixin.zou@mpi-sp.org

yixinzou.github.io