Overview of Privacy & Security

INF 232 - Winter 2024
Ismat Jarin
Kenneth Pat
Kyuha Jung

Venues for Privacy and Security

Conference on Human Factors in Computing Systems (CHI): CHI is often considered to be the most prestigious conference in the field of human-computer interaction (HCI) and is part of ACM. It was founded in 1982 and has been held annually ever since.

USENIX Security: USENIX a nonprofit organization focusing on building communities in computing systems and is affiliated with the Computing Research Association. Just like CHI, it also hosts conferences and publishes academic journals.

Symposium on Usable Privacy and Security (SOUPS) is another conference that is held annually and hosted by USENIX. It focuses specifically on topics related to privacy and security, such as innovative security, evaluations, policies, ethical and psychological aspects of privacy and security.

History of the Privacy and Security Subcommittees

CHI

2013: "Privacy and security" first appeared in the description of the Specific Application Areas subcommittee, alongside education, health, home, sustainability, and creativity.

2018: "Privacy, Security and Visualization" subcommittee was created.

2020: Title changed to "Privacy, Security"

2021: Title changed to "Privacy and Security"

USENIX

1988: USENIX hold 1st Security Workshop

1989: Marking the inaugural standalone conference dedicated solely to security topics under the USENIX banner.

2000s: USENIX expands its focus on privacy and security, instead of ‘Security’ alone

2011: Summit on Gaming/Gamification Security

Core Research Areas/Scopes

CHI 2024
Surfing the World

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

SOUPS 2024
Symposium On Usable Privacy and Security

CHI (Privacy & Security)

- New techniques, systems, and technologies in P&S
- Evaluations of existing/new systems for P&S
- Lessons learned from real-world deployments
- Foundational P&S research identifying important theoretical and/or design insight for the community, etc.
- Contribution is judged two fold: P&S and their impact on HCI

USENIX (Application Security)

- Network and system security
- Security for protocols/analysis (formal methods)
- Computing P&S
  - i.e ML/data-driven P&S
- Privacy
  - i.e anonymity, privacy metrics
- Usable P&S
  - i.e user studies
- Social issues
  - i.e privacy policy

SOUPS (Usable Security)

- P&S functionality Design
- Usability evaluation of new/existing private/secure systems
- P&S testing of usability systems
- Privacy policy and law
- Foundation principle of P&S
- Ethical/psychological aspects of P&S

Scopes Within/Outside of HCI

CHI 2024
Surfing the World

Within HCI

- User-centric P&S
- Design/usability of privacy interfaces and privacy decisions of users
- P&S awareness and education for users
- Ethical/psychological aspects of P&S

Outside of HCI

- Computing
- User interface design and technical aspects
- Health

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Within HCI

- Computer system usability
- Privacy laws and its impact to community
- User studies related to applications

Outside of HCI

- Systems, networks, devices of P&S
- Data-driven P&S
- Security for protocols
- P&S using machine learning techniques

SOUPS
Symposium On Usable Privacy and Security
2024

Within HCI

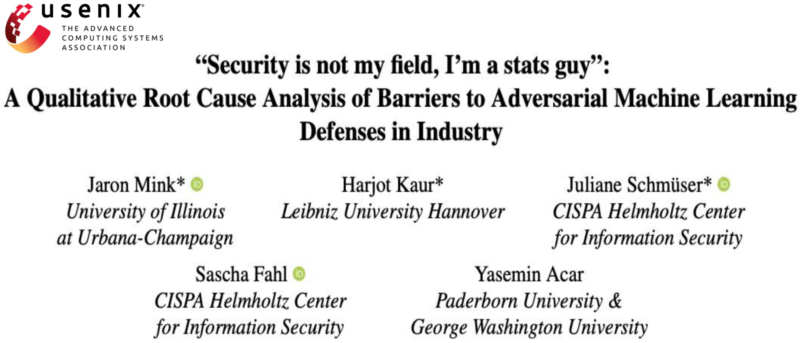
- Usability evaluation of new/existing private/secure systems
- P&S testing of usability systems
- Privacy policy and law
- Ethical/psychological aspects of P&S

Outside of HCI

- P&S functionality design
- P&S verification

Similarities/Differences between Conferences?

Example Papers from Different Venues



"Security is not my field, I'm a stats guy": A Qualitative Root Cause Analysis of Barriers to Adversarial Machine Learning Defenses in Industry

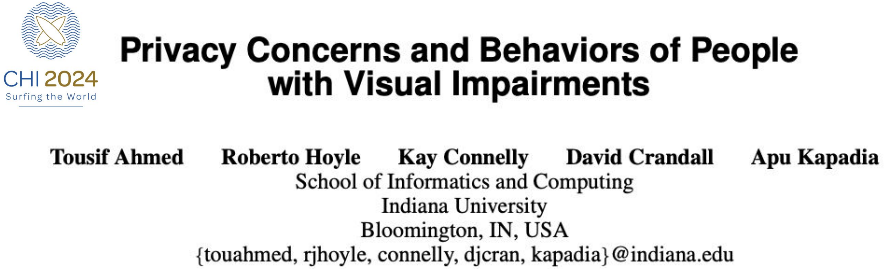
Jaron Mink*
University of Illinois at Urbana-Champaign

Harjot Kaur*
Leibniz University Hannover

Juliane Schmüser*
CISPA Helmholtz Center for Information Security

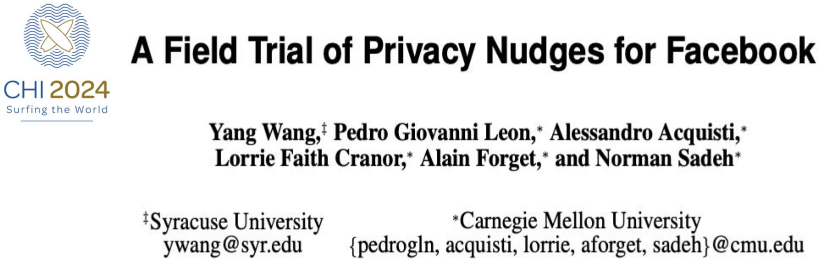
Sascha Fahl
CISPA Helmholtz Center for Information Security

Yasemin Acar
Paderborn University & George Washington University



Privacy Concerns and Behaviors of People with Visual Impairments

Tousif Ahmed **Roberto Hoyle** **Kay Connelly** **David Crandall** **Apu Kapadia**
School of Informatics and Computing
Indiana University
Bloomington, IN, USA
{touahmed, rjhoyle, connelly, djcran, kapadia}@indiana.edu

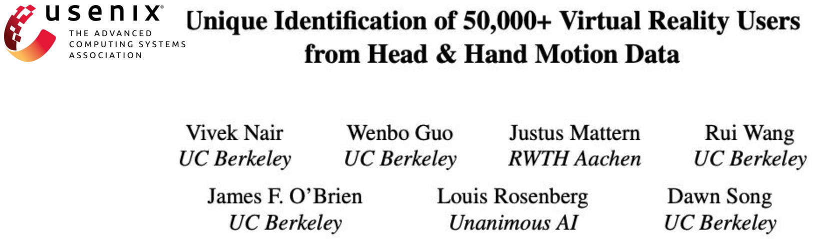


A Field Trial of Privacy Nudges for Facebook

Yang Wang,[‡] Pedro Giovanni Leon,[*] Alessandro Acquisti,[*] Lorrie Faith Cranor,[*] Alain Forget,[*] and Norman Sadeh[*]

[‡]Syracuse University
ywang@syr.edu

[*]Carnegie Mellon University
{pedrogln, acquisti, lorrie, aforget, sadeh}@cmu.edu



Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data

Vivek Nair
UC Berkeley

Wenbo Guo
UC Berkeley

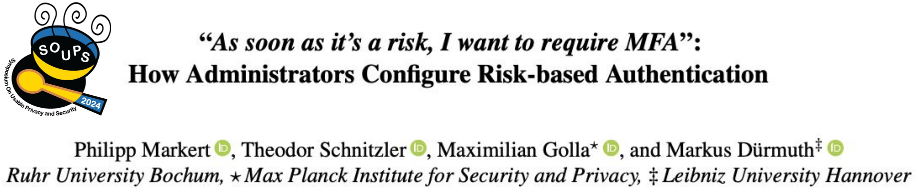
Justus Mattern
RWTH Aachen

Rui Wang
UC Berkeley

James F. O'Brien
UC Berkeley

Louis Rosenberg
Unanimous AI

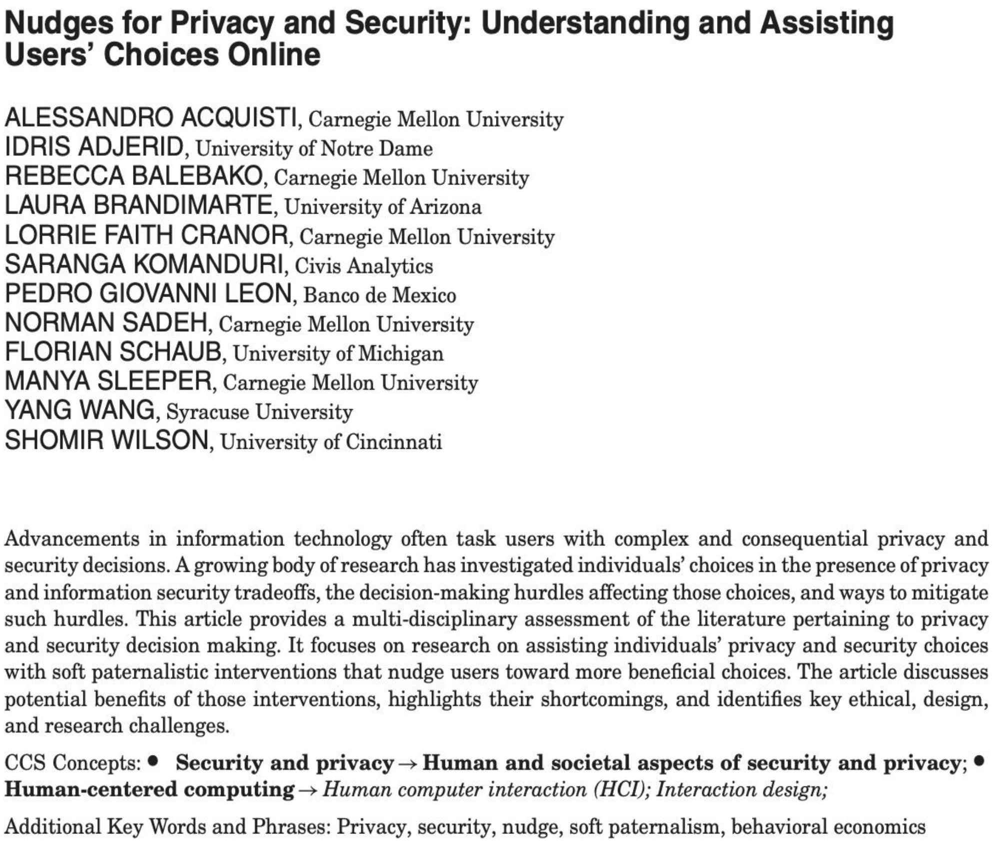
Dawn Song
UC Berkeley



"As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication

Philipp Markert, Theodor Schnitzler, Maximilian Golla[⋆], and Markus Dürmuth[‡]
Ruhr University Bochum, ⋆ Max Planck Institute for Security and Privacy, ‡ Leibniz University Hannover

Overview



Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online

ALESSANDRO ACQUISTI, Carnegie Mellon University
IDRIS ADJERID, University of Notre Dame
REBECCA BALEBAKO, Carnegie Mellon University
LAURA BRANDIMARTE, University of Arizona
LORRIE FAITH CRANOR, Carnegie Mellon University
SARANGA KOMANDURI, Civis Analytics
PEDRO GIOVANNI LEON, Banco de Mexico
NORMAN SADEH, Carnegie Mellon University
FLORIAN SCHAUB, University of Michigan
MANYA SLEEPER, Carnegie Mellon University
YANG WANG, Syracuse University
SHOMIR WILSON, University of Cincinnati

Advancements in information technology often task users with complex and consequential privacy and security decisions. A growing body of research has investigated individuals' choices in the presence of privacy and information security tradeoffs, the decision-making hurdles affecting those choices, and ways to mitigate such hurdles. This article provides a multi-disciplinary assessment of the literature pertaining to privacy and security decision making. It focuses on research on assisting individuals' privacy and security choices with soft paternalistic interventions that nudge users toward more beneficial choices. The article discusses potential benefits of those interventions, highlights their shortcomings, and identifies key ethical, design, and research challenges.

CCS Concepts: • **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → *Human computer interaction (HCI); Interaction design;*

Additional Key Words and Phrases: Privacy, security, nudge, soft paternalism, behavioral economics

You are sharing everything! Your Location, Behavior, Sleeping Routine, Favorite Restaurants!

Importance of this Study

Gray Zone

- How users data is collected and which purpose the data is used?
- What are the trade-offs: sharing/not-sharing?

?

In which apps/medium are you comfortable with sharing your data? Why or why not?

Privacy Decisions: Hard Choice

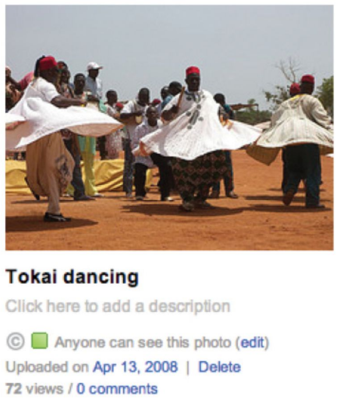
Decisions we make based on:

- Information-often incomplete (Result: Ended up with spam emails!)
- Heuristic/Bounded Rationality (Results: Can produce Meme)
- Cognitive/Behavioral Biases (Results: Provide SSN to ‘trusted’ company make them share this to unknown)
- Overconfident: Nothing is going to happen, not installing Security updates. (Results: Ended up having a malware)

What can be done to help the users?

Privacy Nudges!

- Nudges with Informations
- Nudges with Presentations
- Default Settings
- Reversibility of Error
- Timing



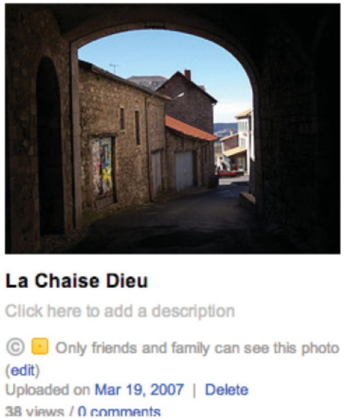
Tokai dancing

Click here to add a description

© 🟩 Anyone can see this photo (edit)

Uploaded on Apr 13, 2008 | Delete

72 views / 0 comments



La Chaise Dieu

Click here to add a description

© 🟨 Only friends and family can see this photo (edit)

Uploaded on Mar 19, 2007 | Delete

38 views / 0 comments

Research Contributions and Takeaways?

Q. Strengths of this work?
(content-wise, structure-wise, privacy/security-wise?)

Contributions

- Insights of cognitive/behavioral biases on online privacy/security decision making
- Help users make better decisions: users will regret less
- Introducing nudging research in the field of privacy/security

Framing the Paper

Research Contribution wrt HCI?

‘Theoretical’

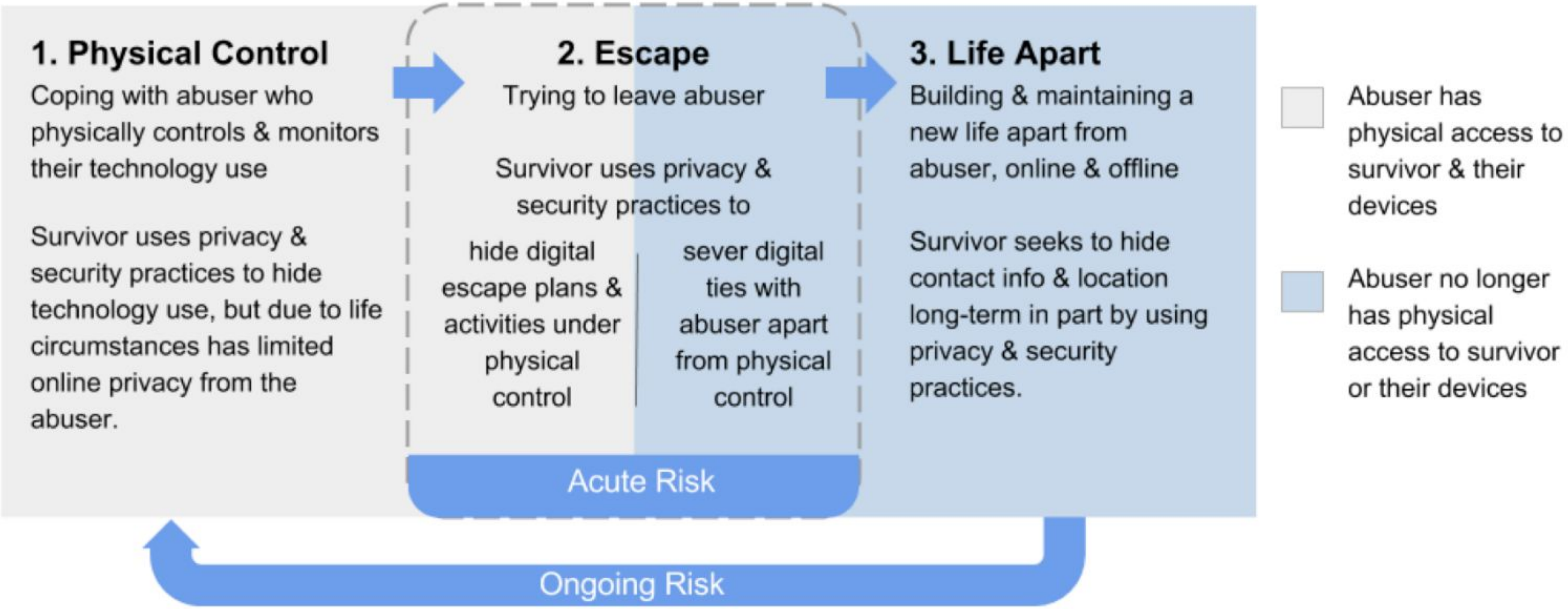
Research Scope of this Paper?

- Foundational privacy/security research identifying important theoretical and/or design insights for the community
- Privacy/security awareness and education for users
- Phycological, behavioral & decision studies

Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse

Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne*, Elizabeth F. Churchill, Sunny Consolvo
Google, Mountain View, CA, USA,
taramatthews@google.com, katieole@gmail.com, {annaturn, manya, jillwoelfer, martinshelton}@google.com, churchill@acm.org, sconsolvo@google.com
*Community Overcoming Relationship Abuse, San Mateo, CA, USA
corim@corasupport.org

Three Phases of IPA (intimate partner abuse)



1. Physical Control

Coping with abuser who physically controls & monitors their technology use

Survivor uses privacy & security practices to hide technology use, but due to life circumstances has limited online privacy from the abuser.

2. Escape

Trying to leave abuser

Survivor uses privacy & security practices to

hide digital escape plans & activities under physical control

sever digital ties with abuser apart from physical control

Acute Risk

3. Life Apart

Building & maintaining a new life apart from abuser, online & offline

Survivor seeks to hide contact info & location long-term in part by using privacy & security practices.

Ongoing Risk

⬜ Abuser has physical access to survivor & their devices

🟦 Abuser no longer has physical access to survivor or their devices

Figure 1. Three phases of IPA that affected technology use, focusing on privacy & security practices.

Q. Strengths of this work?
(content-wise, structure-wise, privacy/security-wise?)

Q. Researchers’ roles & ethical practices in reporting such privacy/security sensitive information?