Privacy & Security

Overview Day

Olivia Figueira, Jessy Ayala,
Jiayu Yin, Katie Genuario

Agenda

1 What are Privacy & Security?

2 Introducing CHI Privacy & Security

3 Beyond CHI: USENIX, SOUPS, and others

4 Framing Papers

Privacy vs. Security

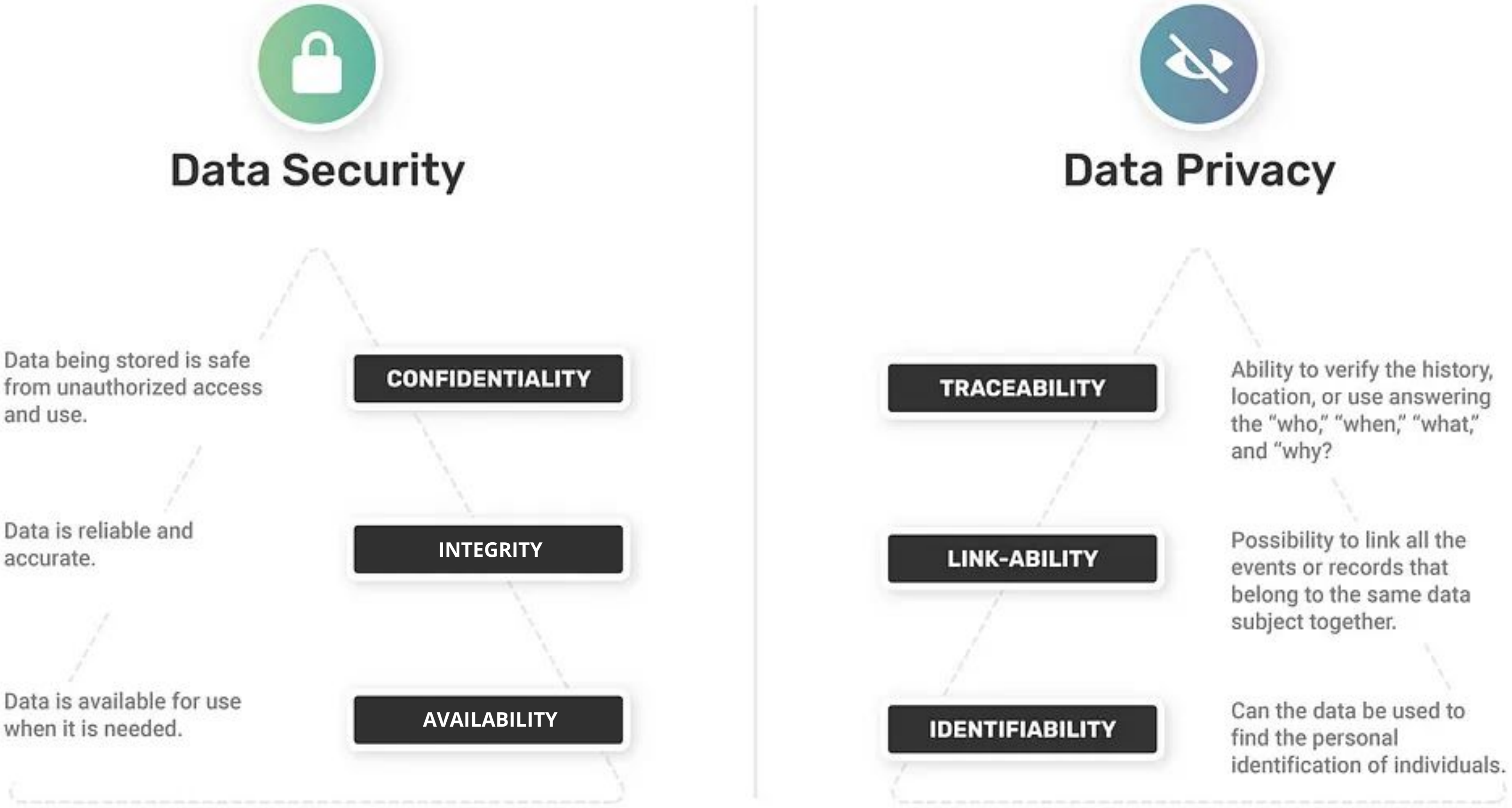
Privacy

- Focused on use and governance of personal data
- Refers to your right to control and manage your personal data and how that data is collected, stored, and used

Security

- Refers to the protection of this data from unauthorized access, attacks, and exploitation

Sources: https://iapp.org/about/what-is-privacy/, https://www.okta.com/identity-101/privacy-vs-security/



Data Security

CONFIDENTIALITY

Data being stored is safe from unauthorized access and use.

INTEGRITY

Data is reliable and accurate.

AVAILABILITY

Data is available for use when it is needed.

Data Privacy

TRACEABILITY

Ability to verify the history, location, or use answering the "who," "when," "what," and "why?

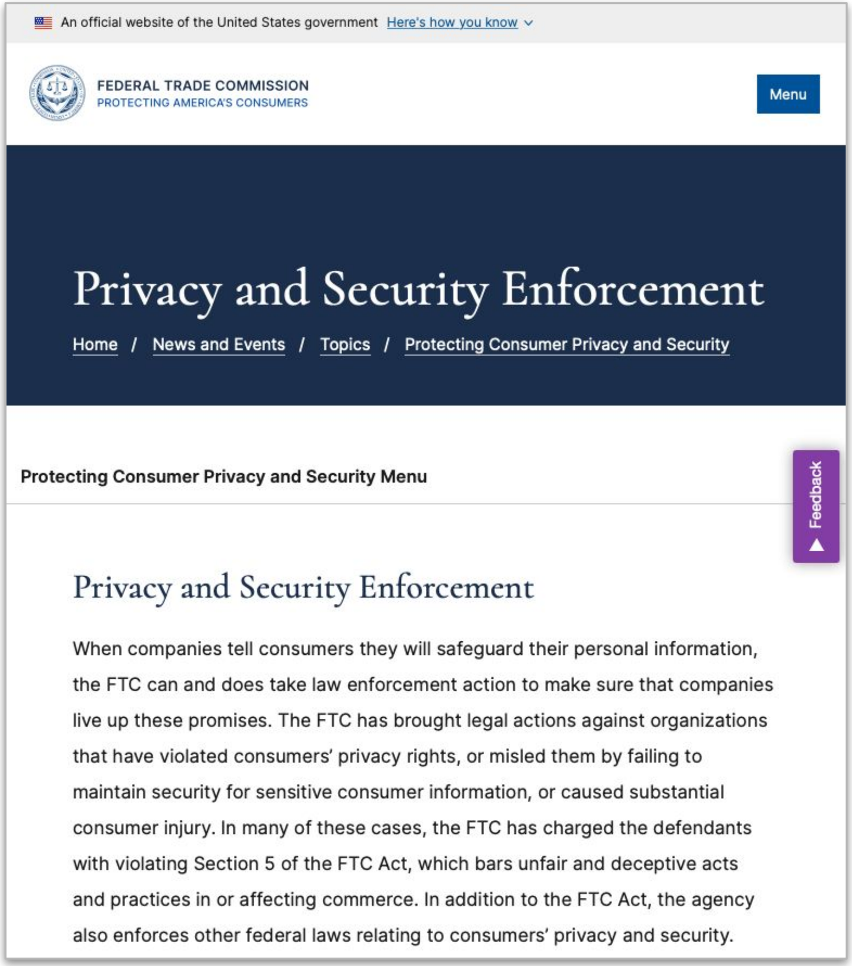
LINK-ABILITY

Possibility to link all the events or records that belong to the same data subject together.

IDENTIFIABILITY

Can the data be used to find the personal identification of individuals.

Source: https://becominghuman.ai/what-is-differential-privacy-1fd7bf507049


An official website of the United States government Here's how you know
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Menu
Feedback

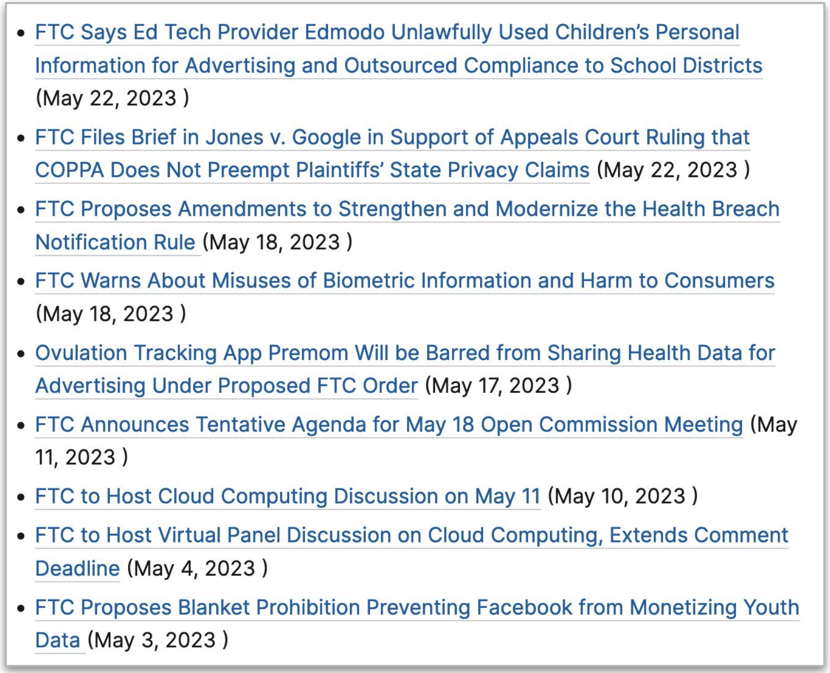
Privacy and Security Enforcement

Home / News and Events / Topics / Protecting Consumer Privacy and Security

Protecting Consumer Privacy and Security Menu

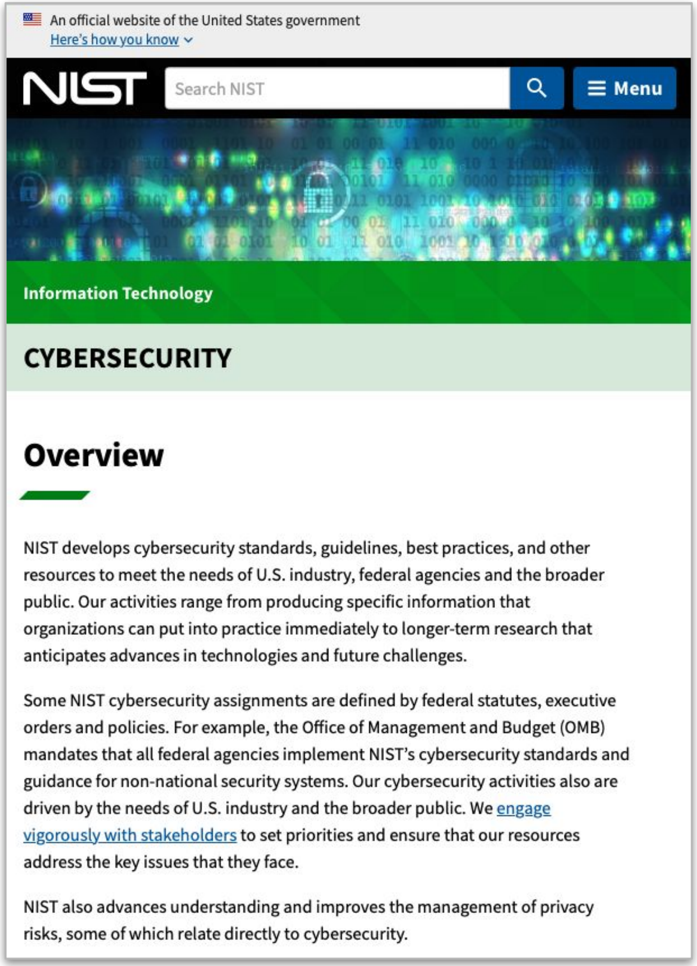
Privacy and Security Enforcement

When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.



- FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023)
- FTC Files Brief in Jones v. Google in Support of Appeals Court Ruling that COPPA Does Not Preempt Plaintiffs' State Privacy Claims (May 22, 2023)
- FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (May 18, 2023)
- FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023)
- Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023)
- FTC Announces Tentative Agenda for May 18 Open Commission Meeting (May 11, 2023)
- FTC to Host Cloud Computing Discussion on May 11 (May 10, 2023)
- FTC to Host Virtual Panel Discussion on Cloud Computing, Extends Comment Deadline (May 4, 2023)
- FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 3, 2023)

Source: https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement



CYBERSECURITY

Overview

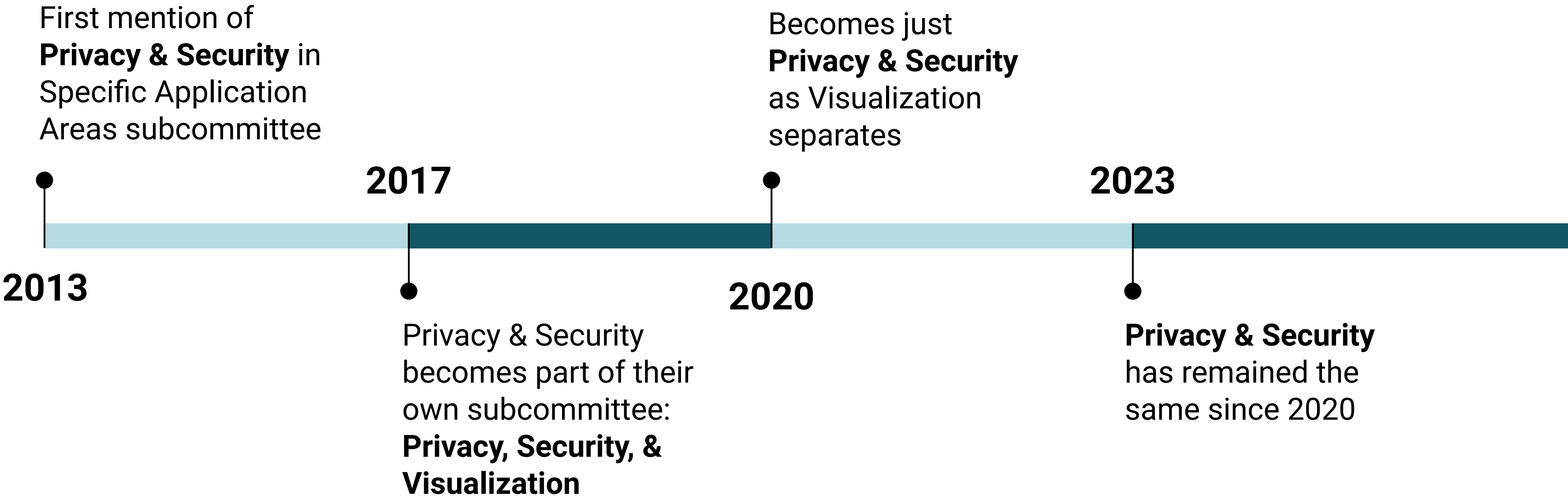
NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

Some NIST cybersecurity assignments are defined by federal statutes, executive orders and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems. Our cybersecurity activities also are driven by the needs of U.S. industry and the broader public. We engage vigorously with stakeholders to set priorities and ensure that our resources address the key issues that they face.

NIST also advances understanding and improves the management of privacy risks, some of which relate directly to cybersecurity.

Source: https://www.nist.gov/cybersecurity

History of CHI Subcommittee



2013

First mention of **Privacy & Security** in Specific Application Areas subcommittee

2017

Privacy & Security becomes part of their own subcommittee: **Privacy, Security, & Visualization**

2020

Becomes just **Privacy & Security** as Visualization separates

2023

Privacy & Security has remained the same since 2020

2017-2019: Privacy, Security, & Visualization

“This subcommittee is suitable for papers across all areas of **usable privacy, security, data visualization and visual analytics**. This includes but is not limited to **new techniques/systems/technologies, evaluations of existing/new systems, ground work identifying important insights for the community, and lessons learned from real-world deployments.** Submissions will be judged based on the contribution they make to **privacy, security, visualization or a combination of those as well as their impact on HCI.** For example, papers that focus on technical contributions need to show how these relate to humans and user experience.”

2020-Present: Privacy & Security

“This subcommittee is suitable for papers relating to **privacy and security.** This includes but is not limited to: **new techniques/systems/technologies, evaluations of existing/new systems, lessons learned from real-world deployments, foundational research identifying important theoretical and/or design insight for the community,** etc. Submissions will be judged based on the **contribution they make to privacy and security as well as their impact on HCI.** For instance, papers that focus on technical contributions will need to show the relationship of the contribution to humans and user experience.”

Compare & Contrast

2017-2019: Privacy, Security, & Visualization

This subcommittee is suitable for papers across all areas of usable privacy, security, data visualization and visual analytics**.** This includes but is not limited to new techniques/systems/technologies, evaluations of existing/new systems, ground work identifying important insights for the community, and lessons learned from real-world deployments. Submissions will be judged based on the contribution they make to privacy, security, visualization or a combination of those as well as their impact on HCI. For example, papers that focus on technical contributions need to show how these relate to humans and user experience.

2020-Present: Privacy & Security

This subcommittee is suitable for papers relating to privacy and security. This includes but is not limited to: new techniques/systems/technologies, evaluations of existing/new systems, lessons learned from real-world deployments, **foundational research identifying important theoretical and/or design insight for the community**, etc. Submissions will be judged based on the contribution they make to privacy and security as well as their impact on HCI. For instance, papers that focus on technical contributions will need to show the relationship of the contribution to humans and user experience.

USENIX Security

“Refereed paper submissions are solicited in all areas relating to systems research in security and privacy. This topic list is not meant to be exhaustive; **USENIX Security is interested in all aspects of computing systems security and privacy**. **Papers without a clear application to security or privacy of computing systems, however, will be considered out of scope** and may be rejected without full review**.**”

Example Topics:

- System, network, wireless, and hardware security
- Security analysis
- Machine learning security and privacy
- Data-driven security and measurement studies
- Privacy (privacy metrics, attacks, web/mobile privacy)
- Usable security and privacy, including user studies and HCD
- Research on surveillance and censorship
- Social issues and security
- Applications of cryptography

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

SOUPS: Symposium on Usable Privacy and Security

“We invite authors to submit previously unpublished papers describing research or experience in **all areas of usable privacy and security**. We welcome a variety of research methods, including both **qualitative and quantitative approaches. Papers will be judged on their scientific quality, overall quality, and contribution to the field.**”

Example Topics:

- Innovative functionality and design
- Field studies of S&P technology
- Usability evaluations
- Security testing of usability features
- Longitudinal studies of deployed features
- Studies of administrators or developers and support for S&P
- Ethical, psychological, sociological, or anthropological aspects of usable S&P
- Usable S&P implications/solutions for specific domains (e.g., IoT, medicine)
- And more!

CHI Privacy & Security

“This subcommittee is suitable for papers relating to privacy and security. This includes but is not limited to: new techniques/systems/technologies, evaluations of existing/new systems, lessons learned from real-world deployments, foundational research identifying important theoretical and/or design insight for the community, etc. **Submissions will be judged based on the contribution they make to privacy and security as well as their impact on HCI.** For instance, **papers that focus on technical contributions will need to show the relationship of the contribution to humans and user experience**.”

Example Topics:

- New techniques/systems/technologies
- Evaluations of existing/new systems
- Lessons learned from real-world deployments
- Foundational research identifying important theoretical and/or design insight for the community

CHI23

Hamburg, Germany | Hybrid
April 23-28, 2023
reCHInnecting

CHI, USENIX, & SOUPS

Similarities

- All 3 include topics surrounding usable S&P:
  - Usable S&P, User Studies about S&P, HCD, Social Issues related to S&P
- Between CHI Privacy & Security and SOUPS:
  - Main target audiences: researchers and practitioners in human-computer interaction, security, and privacy

Differences

- USENIX also focuses on S&P related to systems, hardware, networks, ML, etc.
- SOUPS is more focused on aspects of S&P usability, whereas CHI focuses on contributions to humans and user experiences related to S&P

Core Research Questions & Topics

CHI Subcommittee

- Security and privacy areas related to humans or user experience
    - How to solve security and privacy issues from a human-centered perspective?
    - How are certain users groups impacted by security and privacy issues?

USENIX Security

- All aspects of computing systems security and privacy
    - What are novel techniques to discover security vulnerabilities and privacy invasions?
    - What are novel cybercrime ecosystems and privacy attacks/manipulations that are underexplored?
    - What are novel defense mechanisms for security and privacy attacks?

SOUPS

- Security and privacy usability
    - How usable are security and privacy tools, technologies, and features?

Other Privacy & Security Venues

PETS	Privacy Enhancing Technologies Symposium	applied and/or theoretical research into the design, analysis, experimentation, or fielding of privacy-enhancing technologies
CCS	ACM Computer and Communication Security	seeks submissions presenting novel contributions related to all real-world aspects of computer security and privacy
NDSS	Network and Distributed System Security Symposium	interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation
S&P	IEEE Symposium on Security and Privacy	advances in the theory, design, implementation, analysis, verification, or empirical evaluation and measurement of secure systems

Disciplines Beyond HCI

- **Data Privacy and Privacy-Enhancing Technologies**
  - Differential privacy, data anonymization and minimization, blocking ads/tracking online
- **Cybersecurity and Security-Enhancing Technologies**
  - Authentication (e.g., two/multi-factor, biometrics, passwords)
  - Cryptography and Encryption
  - Cyberattacks and Countermeasures (e.g, phishing, malware, firewalls, antivirus)
  - Security Testing (e.g., fuzzing, threat modeling, static analysis)
- **Computer Architecture and Networks**
  - Network traffic analysis, program analysis

Disciplines Beyond HCI

- **Machine Learning and Artificial Intelligence**
  - Adversarial ML, privacy-preserving ML, recommendation/personalization systems, NLP
- **Law and Regulations**
  - Privacy law, privacy policies, auditing systems and companies
- **Psychology**
  - Behavioral decision making, dark patterns, manipulative ads, social engineering, manipulative cyber attacks
- **Education**
  - Awareness of privacy/security issues and management, privacy/security nutrition labels
- **Business & Economics**
  - Advertising ecosystem, data monetization, “surveillance capitalism”

Title-Venue Matching: CHI, USENIX, or SOUPS?

Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels	**USENIX (2023)**
Evaluating the Usability of Privacy Choice Mechanism	**SOUPS (2022)**
Understanding People's Concerns and Attitudes Toward Smart Cities	**CHI (2023)**
GAP: Differentially Private Graph Neural Networks with Aggregation Perturbation	**USENIX (2023)**

Discussion Question

What are some areas of overlap or connections between HCI and security/privacy?

Or, what is an example that demonstrates an intersection between the two disciplines? This could be a:

- Research area
- Industry application
- Recent event

If you're unsure, feel free to take a guess. It's likely that there is some kind of security or privacy aspect to it :)

Let’s Share!

1. Have you ever been creeped out by an online advertisement? Have you ever felt like ads were following you around online?

2. What do you think about those cookie banner/pop-ups on all the websites nowadays?

3. Have you ever tried to read a Privacy Policy or Terms of Service document before accessing a service?

Framing Paper #1

Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. **Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online.** CSUR (2017).

ACM Computing Surveys: These comprehensive, readable surveys and tutorial papers give guided tours through the literature and explain topics to those who seek to learn the basics of areas outside their specialties in an accessible way. The carefully planned and presented introductions in Computing Surveys (CSUR) are also an excellent way for researchers and professionals to develop perspectives on, and identify trends in complex technologies. Contributions which bridge existing and emerging technologies (such as machine learning) with a variety of science and engineering domains in a novel and interesting way are also welcomed.Contributions are intended to be accessible to a broad audience, featuring clear exposition, a lively tutorial style, and pointers to the literature for further study.

Overview of Study

Every design decision potentially nudges users in one direction or another.

This article draws from results across this array of disciplines to **summarize the research aimed at understanding hurdles** (cognitive and behavioral biases) faced by individuals in online privacy and security decision making and **developing ways of effectively assisting individuals** (nudges) in their privacy and security decisions. Also goes over ethical questions and guidelines for designing nudges.

Fields: behavioral decision research, behavioral economics, experimental psychology, human factors, HCI, persuasive technologies, usability research

Some History & Terms

P&S decisions also involve complex tradeoffs, so scholars have tried to apply economic approaches to privacy since the late 1970s (human factors and usability research on interfaces affecting awareness) and to security in the late 1990s (behavioral economics research on biases and heuristics)

Theory of Rational Choice - models individuals as agents with stable preferences that guide their decision making: decision making is assumed to be rational, in that individuals aim to maximize their utility given their preferences and other constraints (or complexity) they may be subject to [Becker 1976]

Biases - systematic, and therefore predictable systematic errors in judgements and behaviors, deviations from rational choice theory

Heuristics - rules of thumb, are shortcuts in decision making that users lean on when evaluating the probability of adverse events

People have limited resources and rely on heuristics in decision making.

Heuristics and Cognitive Biases

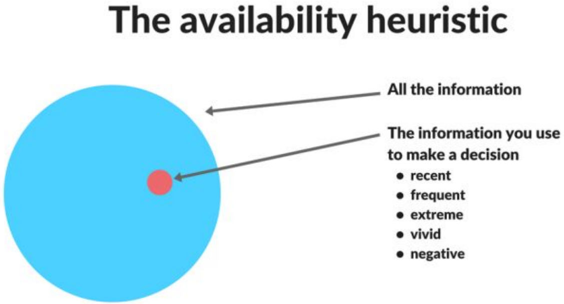
Incomplete (lack of information) **& Asymmetric information** (differential access to relevant information)

Bounded Rationality - human limitations prevents the exploration of all possible outcomes because they simplify choices using heuristics

Hyperbolic Discounting - an alternative model to discount utility theory (constant rate), accounts for observed patterns by considering a discount rate that is decreasing over time.

Optimism bias - underestimation of the chances that one might be subject to a negative event

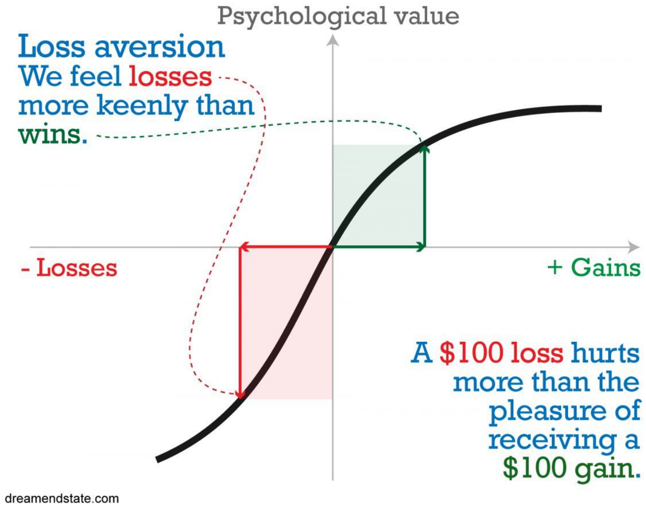
Overconfidence - overestimation of the accuracy of one's judgments


The availability heuristic

All the information

The information you use to make a decision
- recent
- frequent
- extreme
- vivid
- negative

Heuristics and Cognitive Bias



Post-completion Errors - errors resulting from multiple steps, where you succeed in achieving the primary goal but fail in the secondary goal

Status Quo bias - individuals' affinity for default choices.

Loss Aversion - people tend to be loss averse, one derives more disutility from loss over an the amount of utility from a gain

Anchoring - we often consider information that may or may not be relevant to the situation at hand. That information creates a reference point from which we make small adjustments to make a decision for the specific circumstance faced

Framing Effects - Wording of options available. Positive framing emphasizes the gain and thus moderates loss aversion, whereas negative framing makes losses salient.

Question

Think about a online decision that you make regularly (or have made in the past) related to P&S. Can you identify a heuristic or cognitive bias you use to make your decision? What are the tradeoffs of your decision?

Talk with a group for 3 minutes.

Approaches

Usable P&S research - aims to overcome decision complexity through the design of interfaces that offer users manageable and easy-to-understand options.

Paternalistic approaches - impose decisions on users that are believed to be beneficial for them

Libertarian approaches - freedom to choose what is in one's own self-interest, self-regulatory approaches. In system design this is a neutral design providing all available options without regard that some options are detrimental to users

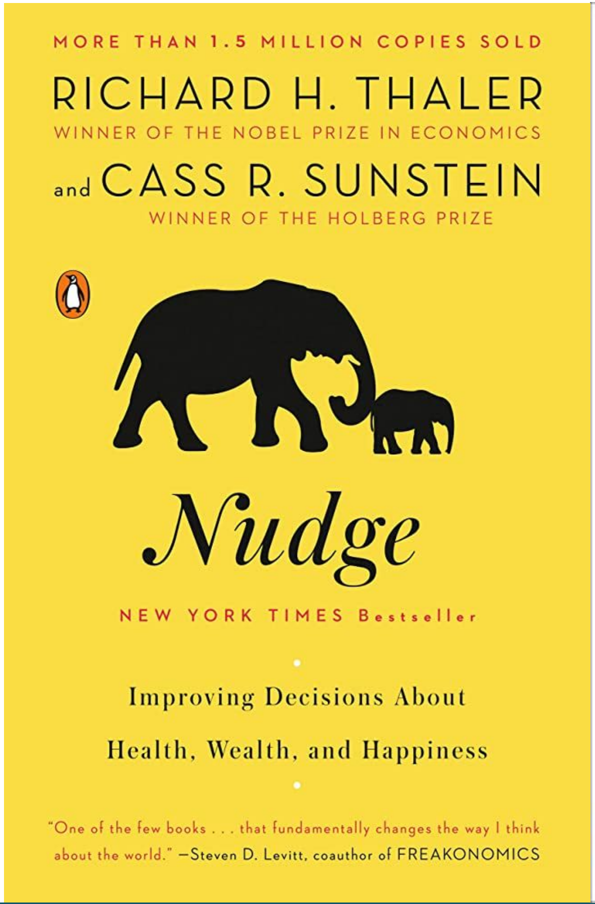
Soft paternalistic interventions - attempt to influence decision making to improve individual well-being, without actually limiting individual choices, but in fact preserving freedom of choice.

Nudges reframe the choices available to users to increase the likelihood that users will make decisions beneficial to them.

Debiasing - reduce the effect of an identified bias, or creating situations where biases don't emerge at all

Persuasive technologies - intentionally designed to change a person's attitude or behavior

Anyone read these classics?



MORE THAN 1.5 MILLION COPIES SOLD

RICHARD H. THALER
WINNER OF THE NOBEL PRIZE IN ECONOMICS

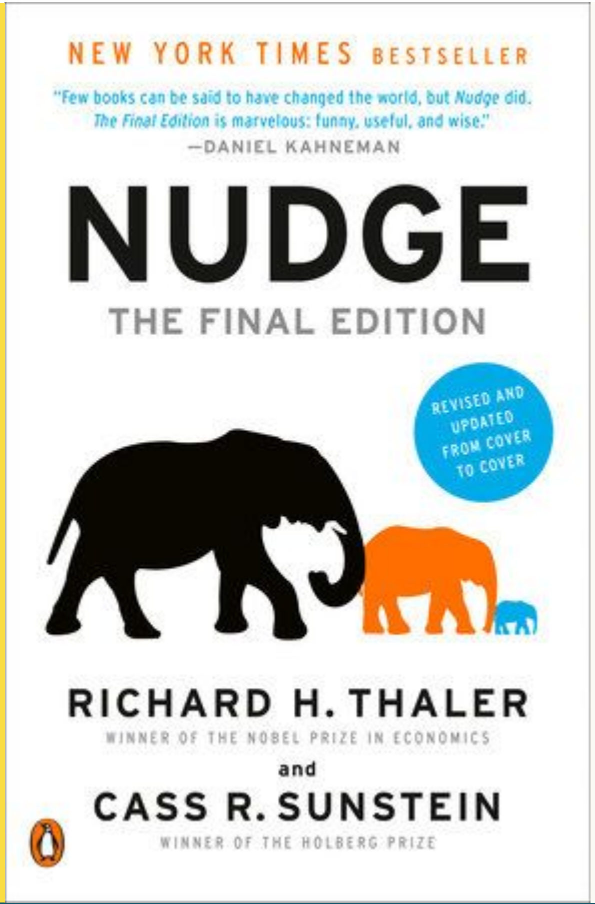
and CASS R. SUNSTEIN
WINNER OF THE HOLBERG PRIZE

Nudge

NEW YORK TIMES Bestseller

Improving Decisions About
Health, Wealth, and Happiness

"One of the few books . . . that fundamentally changes the way I think about the world." —Steven D. Levitt, coauthor of FREAKONOMICS



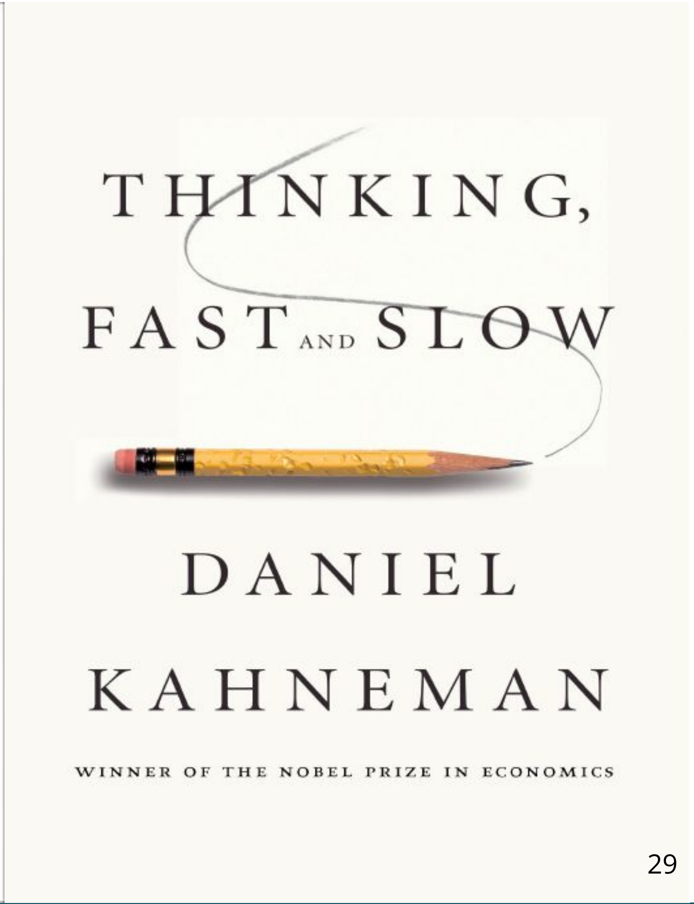
NEW YORK TIMES BESTSELLER

"Few books can be said to have changed the world, but *Nudge* did. *The Final Edition* is marvelous: funny, useful, and wise."
—DANIEL KAHNEMAN

NUDGE
THE FINAL EDITION

REVISED AND UPDATED FROM COVER TO COVER

RICHARD H. THALER
WINNER OF THE NOBEL PRIZE IN ECONOMICS
and
CASS R. SUNSTEIN
WINNER OF THE HOLBERG PRIZE



THINKING, FAST AND SLOW

DANIEL KAHNEMAN

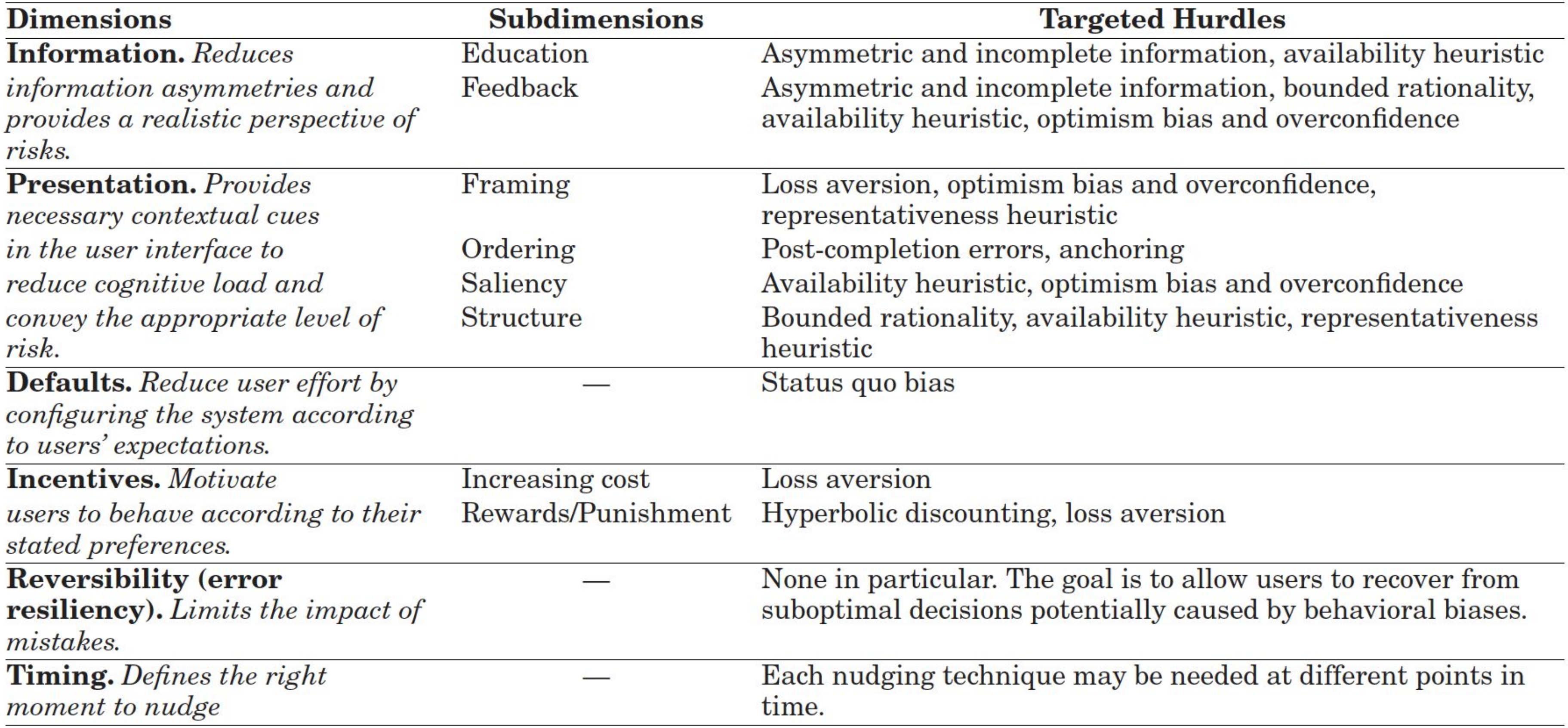
WINNER OF THE NOBEL PRIZE IN ECONOMICS

Question

Concerning design for P&S decisions or general UI design (ex. Social media), do you think design should use paternalistic, soft paternalistic, or libertarian approaches?

When do you think design should take on these approaches (users, contexts) and when do you think they are not appropriate?

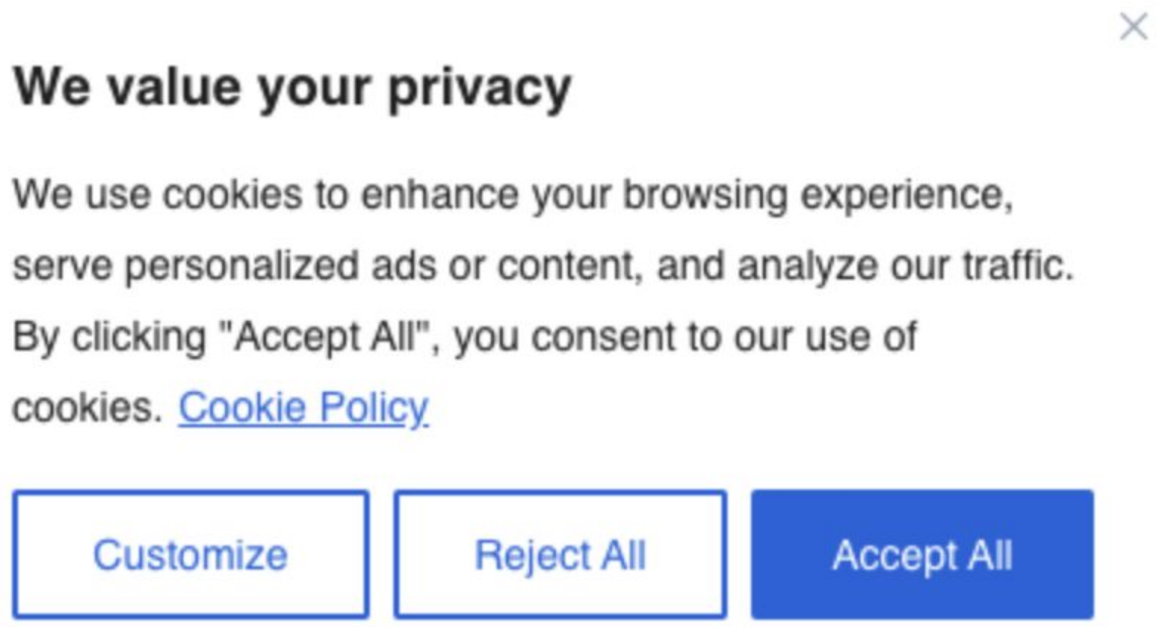
Table I. Overview of Nudging Dimensions and the Relevant Hurdles that They Mitigate or Exploit. Dimensions Are not Necessarily Mutually Exclusive



Dimensions	Subdimensions	Targeted Hurdles
Information. *Reduces information asymmetries and provides a realistic perspective of risks.*	Education	Asymmetric and incomplete information, availability heuristic
	Feedback	Asymmetric and incomplete information, bounded rationality, availability heuristic, optimism bias and overconfidence
Presentation. *Provides necessary contextual cues in the user interface to reduce cognitive load and convey the appropriate level of risk.*	Framing	Loss aversion, optimism bias and overconfidence, representativeness heuristic
	Ordering	Post-completion errors, anchoring
	Saliency	Availability heuristic, optimism bias and overconfidence
	Structure	Bounded rationality, availability heuristic, representativeness heuristic
Defaults. *Reduce user effort by configuring the system according to users' expectations.*	—	Status quo bias
Incentives. *Motivate users to behave according to their stated preferences.*	Increasing cost	Loss aversion
	Rewards/Punishment	Hyperbolic discounting, loss aversion
Reversibility (error resiliency). *Limits the impact of mistakes.*	—	None in particular. The goal is to allow users to recover from suboptimal decisions potentially caused by behavioral biases.
Timing. *Defines the right moment to nudge*	—	Each nudging technique may be needed at different points in time.

Question

What nudging dimensions are shown here?



We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Cookie Policy

Education & Feedback - privacy policies (p.14-17)

Information dimension - Reduces information asymmetries and provides a realistic perspective of risks.

Privacy policy documents, such as those provided by websites, are examples of notices that might overwhelm the reader. Education and information can be achieved through better design [Schaub et al. 2015]. For example, **policies can be formatted in a readable and concise manner, such as the “nutrition labels format suggested by Kelley et al. [2010], who found that standardized privacy labels can have a significant impact on users’ understanding of privacy policies.** Participants were more accurate and faster in reading the standardized notices, and could better compare different policies.

Usable and in-time privacy notices **make websites data practices more salient** and can nudge Internet users to use websites with more privacy-respectful data practices. **Privacy Bird was built with the idea of warning users** whenever a website engages in practices that do not align with users’ expectations [Cranor et al. 2006]

Framing - paying for privacy (p.19)

Presentation dimension - Provides necessary contextual cues in the user interface to reduce cognitive load and convey the appropriate level of risk

The way that choices are framed and structured also impacts how people balance costs and privacy concerns. Egelman et al. [2013] found that **people were willing to pay more for Android apps that requested fewer permissions when they had several options for price and permissions. However, when only given one choice, participants were not as willing to pay for privacy.** Therefore, applications that only give users the option of installation with a fixed set of permissions may be nudging users away from privacy, indicating the need for more structured choices, such as systems that provide users with selective permission controls [Almuhimedi et al. 2015].

Status Quo - browser history tracking (p.21)

Default dimension - reduce user effort by configuring the system according to user expectations.

In 2012, Microsoft announced that it would turn on the **“Do Not Track” option by default in the release of its browser Internet Explorer 10.** All users who did not change the default setting would send a flag to online advertisers that they did not want their browsing history to be tracked. The ensuing debate showed **how crucial the default setting is, as advertisers balked** and stated that such a default setting could not be honored [Angwin 2012], as it may not reflect the user’s actual preference.

Loss aversion - what’s your price? (p. 23)

Incentives dimension - motivate users to behave according to their stated preferences.

Grossklags and Acquisti [2007] found that users will set different prices on privacy depending on whether they are asked to pay for protection or are offered payment for the same information. They found that **the “willingness-to-accept” price at which individuals are willing to sell information, is substantially higher than the average “willingness-to-protect” price,** which individuals would be willing to pay to protect their information.

In one study, Christin et al. [2012] paid participants a small amount to download an unknown executable onto their computer. They increased the financial incentive each week, to determine how that impacted participants’ security decisions. **At the maximum payment of $1.00, 43% of participants were willing to download and execute the file.**

Reversible photo tagging (p. 24)

Reversibility (error resiliency) dimension - limits the impact of mistakes.

Besmer and Lipford [2010] studied how people respond to Facebook photo tags. They found that individuals may not want their photos shared on the social network by others. A photo tagging tool built by the researchers allowed users to request that their friends remove tags from photos. **They found that users actually preferred an undo tag over negotiating with their friends to remove tags.**

Note: I think photo tagging now it comes through as a request for certain privacy settings?

Timing the privacy notice (p. 24)

Timing dimension - defines the right moment to nudge.

Other nudges, such as privacy indicators, may have a greater impact based on when they are seen. Egelman et al. [2009] investigated whether participants in a lab study were more likely to pay a premium for websites with good privacy practices. **They found that the timing of the privacy notice was important; viewing privacy indicators before visiting the website had a greater impact than seeing the indicators once the users already arrived at the website.** Balebako et al. [2015] found that individuals pay more attention to privacy notices shown in the context of a mobile app compared to in the app store.

Question

Would you pay more for privacy and security features? For example, would you pay for a tool that prevented websites/companies from re-selling your data to third parties without your approval?

Rather than using a free version, would you pay for a "premium" version of a service so that it does *not* sell your data to third parties?

Guidelines for Ethical Nudge Design

1. Are the normative judgments expressed through the nudge appropriate for the privacy and security concerns of the user population?
2. How likely are unintended adverse consequences?
3. Does nudging transfer responsibility in an inappropriate way?
4. **Could the nudge appear to present a conflict of interest, and does the nudging party have an appropriate responsibility to nudge? Glaeser [2005]**
5. The direction, salience, and firmness of a nudge should be proportional to the user's benefit from the suggested course of action.
6. The user's choices should be respected.
7. Nudging techniques should respect ethical norms applicable to persuasion.
8. Users' expectations for truthful information should be respected

Author suggestions:

1. **Minimizing regret,** instances in which disclosures by individuals are likely to be regretted in the future are nudge-worthy
2. **Aligning behavior with stated preferences** is nudge worthy.

Ethical Questions about Design

Whenever a designer creates a system, every design choice inescapably influences the user in some way (good or bad).

Should we nudge at all (Section 5.1)? If yes, then toward what **outcomes** (Section 5.2)? And **who** should implement those nudges (Section 5.3)?

End users self-commitment? Regulators? Market forces? Third parties?

Do system designers know what’s best for users? Who should be involved in designing and evaluating nudges? Do you feel that you have power to advocate for more ethical design in your (past/current/future) workplace?

Framing Paper #2

Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Woelfer, Martin Shelton, Cori Mathorne, Elizabeth F. Churchill, and Sunny Consolvo. **Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse.** CHI (2017).

Research fields: Privacy; security; user study; Information interfaces and presentation; intimate partner abuse; domestic violence;

Study Focus:

- To understand the experiences of IPA survivors, particularly on their use of technology in the context of privacy and security.
- Explores the types of digital attacks experienced by survivors
- The precautionary behaviors they adopt to protect their privacy and security.

Survivors of IPA:

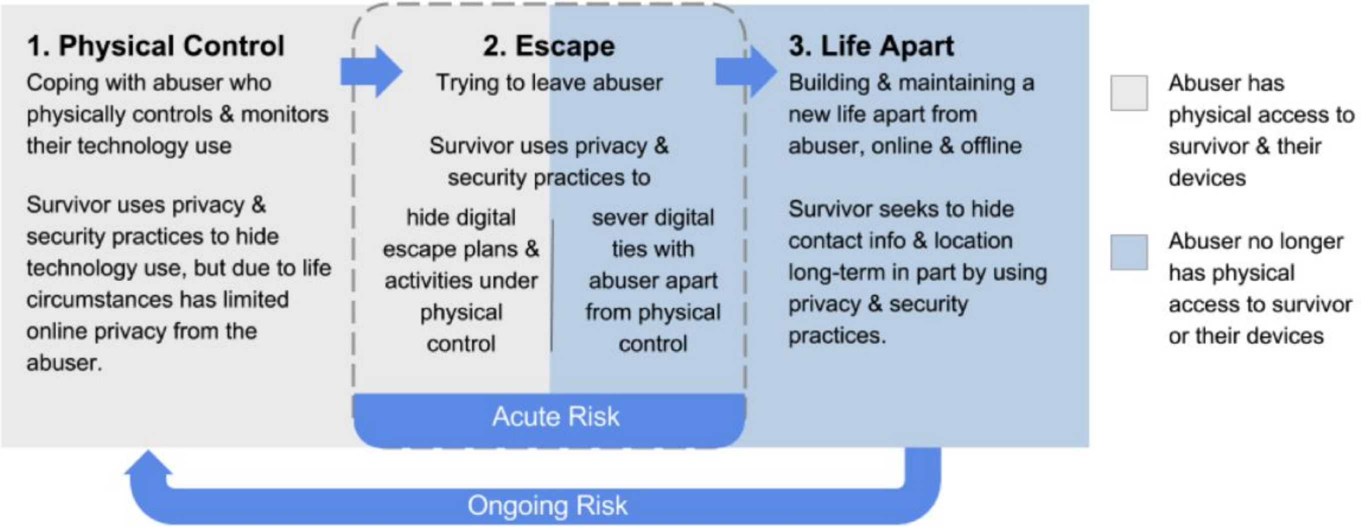
- People who are broadly targeted by an intimate partner, typically a current or former significant partner.
- They may experience threats or abuse from their abuser, like stalking; and be controlled financially or spiritually.

Problem: Survivors of IPA have a persistent attacker, who has intimate knowledge of their lives. These attackers may use technology to further their abuse.

- Installing spyware on their phones to monitor the survivors
- Hijacking their social accounts.
- Harassing them online.

Method: Semi-structured interviews with 15 survivors of IPA who were receiving services at non-profit organizations in the U.S.

Key Findings: Three stages of IPA that affected technology use



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

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.

□ Abuser has physical access to survivor & their devices

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

Acute Risk

Ongoing Risk

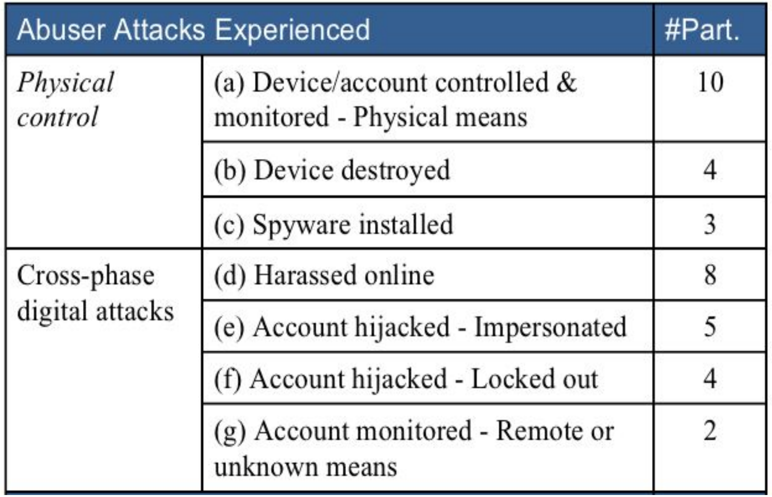
Figure 1. Three phases of IPA that affected technology use, focusing on privacy & security practices.

Discussion for High-Risk Privacy Research

- **What precautions were taken when conducting this study to maintain the safety of the participants?**
- **How were trust and rapport built?**
- **How was privacy maintained within the research study? (Perusall)**

- Met in-person where they felt safe.
- Plans were made with the agencies to address any problematic situations
- collaborating with agency staff to co-create a safe and comfortable environment for them.
- Less demographic info collected
- Informed consent
- Consulted with privacy experts and developed an anonymization guide to ensure the removal of any identifying information
- Specifics were replaced with more general phrases, Participant stories were carefully chosen to without revealing unique details.
- The anonymization process was reviewed by privacy experts

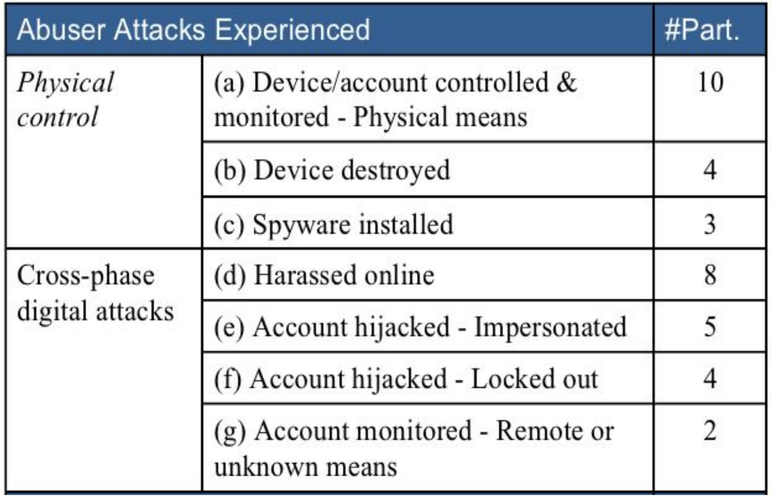
Key Findings: Attacks from abusers



Abuser Attacks Experienced		#Part.
Physical control	(a) Device/account controlled & monitored - Physical means	10
	(b) Device destroyed	4
	(c) Spyware installed	3
Cross-phase digital attacks	(d) Harassed online	8
	(e) Account hijacked - Impersonated	5
	(f) Account hijacked - Locked out	4
	(g) Account monitored - Remote or unknown means	2

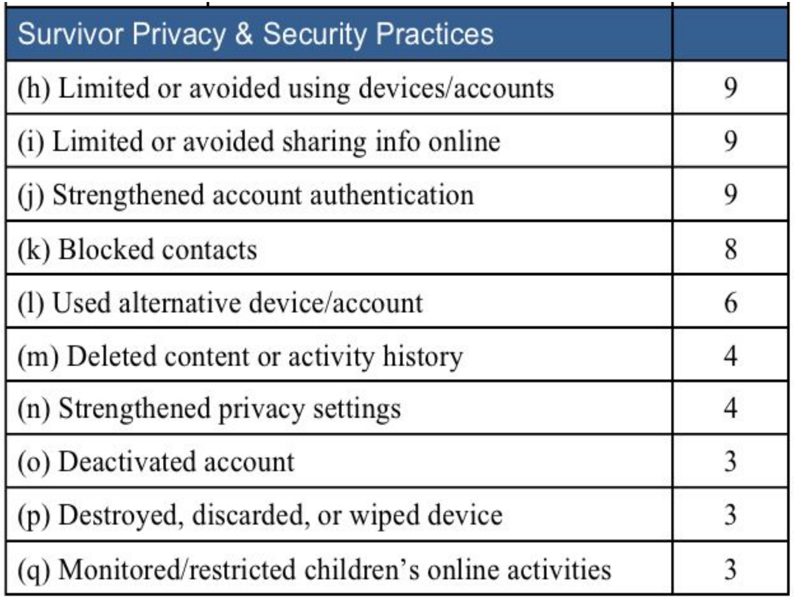
1. Physical control phase:
    a. Physically controlled and monitored survivors device or account use.
    b. Installed spyware on their devices to monitor their activity.
2. Digital attacks during all phases:
    a. **Account hijacking:** Abusers impersonated the survivors to damage their reputations or gather information about them.
    b. **Online harassment**: Abusers tried to intimidate them to stay or return by harassing them online with repeated, threatening messages.

Key Findings:
Attacks from abusers



Abuser Attacks Experienced		#Part.
Physical control	(a) Device/account controlled & monitored - Physical means	10
	(b) Device destroyed	4
	(c) Spyware installed	3
Cross-phase digital attacks	(d) Harassed online	8
	(e) Account hijacked - Impersonated	5
	(f) Account hijacked - Locked out	4
	(g) Account monitored - Remote or unknown means	2

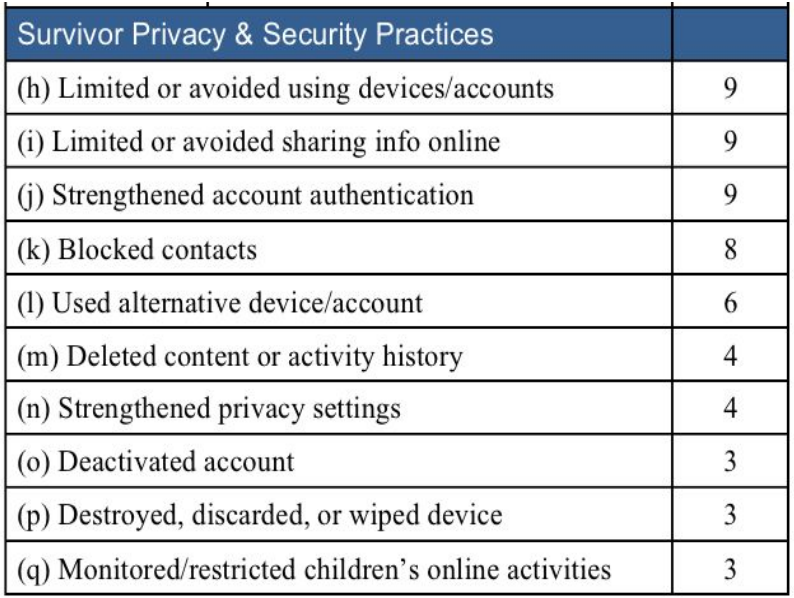
Key Findings:
Practices survivors deployed



Survivor Privacy & Security Practices	
(h) Limited or avoided using devices/accounts	9
(i) Limited or avoided sharing info online	9
(j) Strengthened account authentication	9
(k) Blocked contacts	8
(l) Used alternative device/account	6
(m) Deleted content or activity history	4
(n) Strengthened privacy settings	4
(o) Deactivated account	3
(p) Destroyed, discarded, or wiped device	3
(q) Monitored/restricted children's online activities	3

Key Findings:
Practices survivors deployed

1. Physical Control Phase:
    a. Limited or avoided using devices and/or accounts the abuser could access.
    b. Use alternate devices or delete content or activity histories.
2. Life Apart Phase:
    a. Deactivated their accounts as a way to hide their escape location
    b. Strengthen account authentication.
    c. Limit or avoid sharing information online
3. Long-term Practice:
    a. Limiting Technology Use to avoid information sharing
    b. Monitoring & Restricting Kids & Networks to prevent the abuser know their information from children's social media



Survivor Privacy & Security Practices	
(h) Limited or avoided using devices/accounts	9
(i) Limited or avoided sharing info online	9
(j) Strengthened account authentication	9
(k) Blocked contacts	8
(l) Used alternative device/account	6
(m) Deleted content or activity history	4
(n) Strengthened privacy settings	4
(o) Deactivated account	3
(p) Destroyed, discarded, or wiped device	3
(q) Monitored/restricted children's online activities	3

Discussion for Design Implication

We observed that participants made mistakes when deleting or clearing information. Designers should therefore consider both the general usability of privacy and security features, and their use during high-stress, high-risk situations.

What features can be considered by designers for users to delete or clear information, especially in high-stress, high-risk situations?

Thoughts:

- Notifying users if the content they delete will still have a backup (like in the Trash or Recently Deleted) or if it will be deleted completely.
- Navigate users to the right place if they want to completely delete that content.

Discussion for Design Implication

This study noted some types of privacy and security options that were particularly useful to survivors that enabled them to safely and privately use alternate devices (e.g., using private browsing on someone else’s device) and effectively control their digital traces (e.g., delete content)

What are the pros/cons of using private browsing on their own device or someone else’s device in such cases?

Thoughts:

- Pros: ensure the privacy and confidentiality of their activities, such as when making escape plans.
- Cons: It is hard to mark down the information they need, especially when the plan cannot be finished in one session, such as searching and planning to find a new location…

Discussion for Design Implication

For online harassment, designers can help by providing controls to block other users and report threatening content. **However, designers should consider methods for giving survivors the option to choose to use these types of controls as appropriate in context**. For example, digital channels can provide an outlet for an abuser's desire to exert control, and **blocking an abuser online could lead the abuser to seek physical contact instead.**

For designers, how do we balance this tradeoff? What options can be designed for survivors in these situations?

Thoughts:

- Blocking but not notifying the abuser that they were blocked: survivors don't need to see those threatening words anymore while still leaving an outlet for abusers that won't enrage them…

Thank you!

Get ready to talk about Dark Patterns and Contextual Integrity next class!