

# Privacy & Security

## Discussion Day

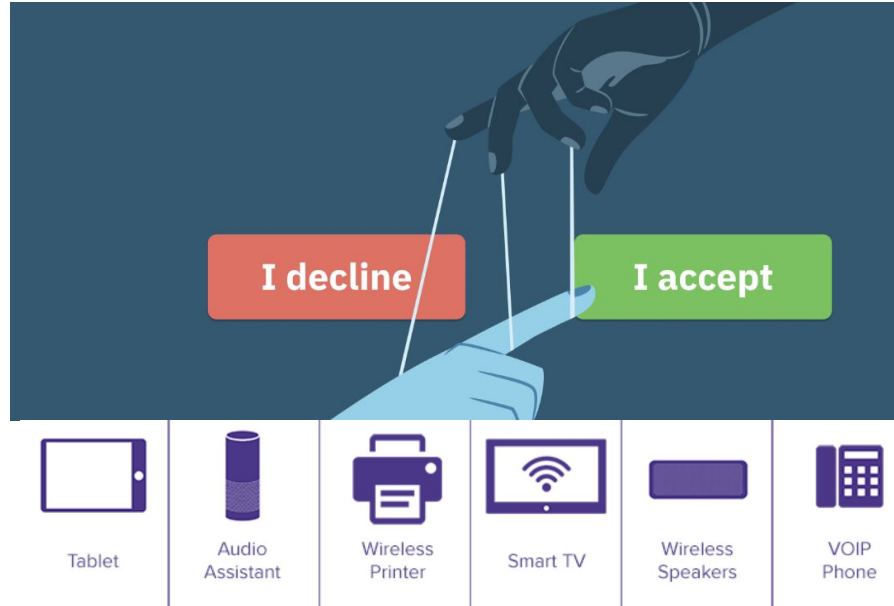
Olivia Figueira, Jessy Ayala,  
Jiayu Yin, Katie Genuario

# Agenda

- 1 Understanding Dark Patterns in Home IoT Devices
  - 2 Online Proctoring: Privacy Invasion or Study Alleviation?: Discovering Acceptability Using Contextual Integrity
-

# Discussion Paper #1

Monica Kowalczyk, Johanna T. Gunawan, David Choffnes, Daniel J Dubois, Woodrow Hartzog, and Christo Wilson. **Understanding Dark Patterns in Home IoT Devices**. CHI (2023).



## Quick Question

Q

Think about any smart devices you may have (e.g., watch). What are some security or privacy concerns you may have thought of before?

Take a moment to think and we'll ask for you to share :)

# Overview of Study

Systematic study of IoT device dark patterns attempting to uncover as many possible features, settings, and categories. Method used builds upon existing taxonomies, and evaluates multimodality. 12 new dark patterns found.

- 57 multiple devices
- 9 categories
- 3 interaction methods
- 6 manufacturers

Device Type	Device Name	Ecosystem	App Name (If Used)	App Dependency	Video Duration
Home Automation	Amazon Smart Plug	Amazon	Amazon Alexa	All interactions	0:11:13
	Jinwoo Smart Bulb		Jinwoo Smart	All interactions	0:19:22
	Gosund Smart Light Bulb		Gosund	All interactions	0:12:30
	Govee LED Light Bulb		Govee Home	All interactions	0:15:41
	Magichome Strip	Google	Magic Home Pro	All interactions	0:09:24
	Meross Door Opener		meross	All interactions	0:12:17
	Nest Thermostat*		Nest	All interactions	0:26:27
	Ring Chime		Ring	All interactions	0:19:50
	Smartlife LED Bulb	Amazon	Smart Life	All interactions	0:18:27
	WeMo Plug		Wemo	All interactions	0:13:14
	Thermopro TP90		ThermoPro Home	Smart interactions	0:06:59
	TP-Link Bulb		Kasa Smart	All interactions	0:14:03
	TP-Link Plug	Kasa	Kasa Smart	All interactions	0:14:23

Context Category	Dark Pattern Description	Mapping to Prior Taxonomies	Potential Harms
Registration	Account required to use service Account required to set up device	Forced Registration [19], Forced Action [26, 39] Forced Registration [19], Forced Action [26, 39]	Privacy [68] Privacy [68]

# How does this paper argue that its topic is worthy of study?

“Internet-of-Things (IoT) devices are ubiquitous, but little attention has been paid to how they may incorporate dark patterns despite consumer protections and privacy concerns arising from their **unique access to intimate spaces and always-on capabilities.**”

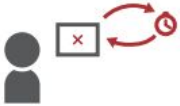




“With access to sensitive information (e.g., health data, video feeds, sensor data), always-on capabilities, and experiences that span hardware and software, IoT device experiences may **exacerbate harms or include previously undocumented dark pattern** instances.”

# The Dark (Patterns) Side of UX Design - Gray et al. [42]

Type of Dark Pattern	Description
Bait and Switch	You set out to do one thing, but a different, undesirable thing happens instead.
Disguised Ad	Adverts that are disguised as other kinds of content or navigation, in order to get you to click on them.
Forced Continuity	When your free trial with a service comes to an end and your credit card silently starts getting charged without any warning. In some cases this is made even worse by making it difficult to cancel the membership.
Friend Spam	The product asks for your email or social media permissions under the pretence it will be used for a desirable outcome (e.g. finding friends), but then spams all your contacts in a message that claims to be from you.
Hidden Costs	You get to the last step of the checkout process, only to discover some unexpected charges have appeared, e.g. delivery charges, tax, etc.
Misdirection	The design purposefully focuses your attention on one thing in order to distract your attention from another.
Price Comparison Prevention	The retailer makes it hard for you to compare the price of an item with another item, so you cannot make an informed decision.
Privacy Zuckering	You are tricked into publicly sharing more information about yourself than you really intended to. Named after Facebook CEO Mark Zuckerberg.
Roach Motel	The design makes it very easy for you to get into a certain situation, but then makes it hard for you to get out of it (e.g. a subscription).
Sneak into Basket	You attempt to purchase something, but somewhere in the purchasing journey the site sneaks an additional item into your basket, often through the use of an opt-out radio button or checkbox on a prior page.
Trick Questions	You respond to a question, which, when glanced upon quickly appears to ask one thing, but if read carefully, asks another thing entirely.

**Table 1. Types of Dark Patterns, quoted from [17].**

# The Dark (Patterns) Side of UX Design - Gray et al. [42]

 <b>NAGGING</b> Redirection of expected functionality that persists beyond one or more interactions.	 <b>OBSTRUCTION</b> Making a process more difficult than it needs to be, with the intent of dissuading certain action(s). <b>INCLUDES:</b> Brignull "Roach Motel," "Price Comparison Prevention," and Intermediate Currency	 <b>SNEAKING</b> Attempting to hide, disguise, or delay the divulging of information that is relevant to the user. <b>INCLUDES:</b> Brignull "Forced Continuity," "Hidden Costs," "Sneak into Basket," and "Bait and Switch"	 <b>INTERFACE INTERFERENCE</b> Manipulation of the user interface that privileges certain actions over others. <b>INCLUDES:</b> Hidden Information, Preselection, Aesthetic Manipulation, Toying with Emotion, False Hierarchy, Brignull "Disguised Ad," and "Trick Questions"	 <b>FORCED ACTION</b> Requiring the user to perform a certain action to access (or continue to access) certain functionality. <b>INCLUDES:</b> Social Pyramid, Brignull "Privacy Zuckering," and Gamification
---	--	--	---	--

**Figure 1. Summary of dark pattern strategies derived from analysis of our corpus.**



# Areas of Inquiry Within HCI

**Dark Patterns** are [user interface designs](#) that trick users into unwanted or unintentional behavior, typically against users' best interests [20]

Examples: [capture attention on social media](#), [nudge](#) people to disclose personal information, [consent interactions](#)

Multifactor analysis like the “n-dimensional” approach for research considering factors like time, [interaction](#), [design](#), psychology, and law (Gray et al. [40])

**Internet of Things (IoT) devices** often do not provide feedback to [users](#) when they are listening or recording.

IoT devices have [limited surfaces for interaction](#) and complicated companion apps that designers can obfuscate or discourage privacy functions

IoT devices and mobile phones can have different [user interfaces](#), [interaction modalities](#), and [sensors](#). How do their dark patterns differ? What are malicious implications of their dark patterns?

# Areas of Inquiry **Outside of HCI**

Law

**FTC Act - Section 5(a), 15 U.S.C. § 45(a)**

Prohibits deceptive acts or practices that misrepresent or omit material facts.

USA | FTC Act (US) | September 26, 1914

Business

**FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay \$245 Million for Tricking Users into Making Unwanted Charges**

Ethics

FTC will use the money to provide refunds to consumers

Privacy

March 14, 2023

Psychology

**Google's "dark patterns" trick users into revealing personal data; lawsuit settled for \$392 million**

<https://www.deceptive.design/>

GOOGLE

PUBLISHED: NOV 15, 2022, 10:52 AM

# Research Questions

1. To what extent do dark patterns observed in other modalities apply to IoT? Do IoT modalities change our understanding of dark patterns and give rise to new dark patterns?
2. How do dark patterns in IoT devices relate to device type, manufacturer, modality, and the context in which interactions were performed?
3. What are the implications of observed IoT dark patterns?

# Methods

Used existing taxonomies (Gray et al. 39, Di Geronimo et al. 26, and Gunawan et al. 42).

Pilot study used to refine interaction scripts and codebook for final round of data collection.

Developed common set of speaker scripts including navigation of settings and exit interactions.

Screen recorded interactions and used video annotation software to count both binary presence and # of dark patterns per interaction.

Grouped dark patterns into context categories, mapped them to associate traits, strategies and harms.

# Contributions

Empirical

Artifact

Methodological

Theoretical

Dataset

Survey

Opinion

# Contributions

Empirical

Artifact

Methodological

Theoretical

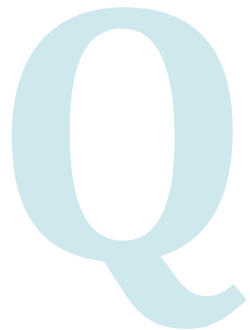
Dataset

Survey

Opinion

- Empirical contributions were made through their careful documentation and analysis of dark patterns across 57 IoT devices. This was one of the first papers to focus on IoT devices and multi-modality so it makes an important empirical contribution to the dark pattern HCI literature.
- Methodological contributions were made in the discovery of new dark patterns to add to existing taxonomies. The researchers also developed processes (interaction scripts) for interacting with IoT devices for dark pattern discovery. Both of these contributions will improve future dark patterns research.

## Discussion Question



How do you think we can improve dark patterns measurement across devices and interfaces? What metrics would need to be included if we were able to create an automatic measuring tool?

Take a few minutes to talk with a partner/group and we'll ask for you to share :)

# Contributions (findings)

12 new dark patterns found



(b) A header for sponsored content in the Fire TV. It is unclear whether this content is free, and what the nature of the sponsorship is.

Extraneous social media features	Feature seems premium but is not	Hidden feature behavior
Device sensed without permissions	Hard to navigate settings	Feature detours to a different modality
Non-permanent opt out	Inconsistent Settings UI	Nagging self-promotional content
Pay for long term use	No local subscription cancellation	Cannot delete data from device



## Quick Question

Q

What dark pattern uncovered in this study did you find most concerning? Do you think this dark pattern is designed with intention or is it simply from poor or normative design?

Take a minute to think and we'll ask for you to share :)

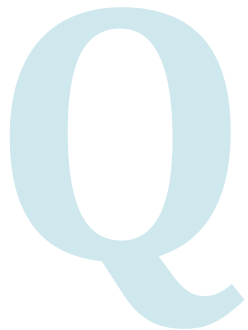
# Research Question Conclusions

1. Findings highlight the necessity of multi-factor analysis for dark patterns, different dark patterns arise in different device flavors (e.g., TVs vs VAs)
2. Amazon and Google devices tend to contain more dark patterns
3. Nontransparent designs in IoT devices may enhance the likelihood of financial and privacy harms for consumers

# Main Takeaways (consumer findings)

- IoT experiences raise **financial harms** for customers who make purchases without complete or incorrect understandings
- Some IoT dark patterns constitute **privacy harms** by denying users the ability to manage privacy preferences during and after using an IoT device
- High rates of nagging patterns in IoT experiences may influence user behavior towards trackable engagement, which would lead to further financial or privacy harms

## Discussion Question



How do you think dark patterns could exacerbate (or help) the abuser attacks, survivor privacy and security practices, and harms detailed in the IPA paper we discussed last class?

Take a few minutes to talk with a partner/group and we'll ask for you to share :)

# Main Takeaways (moving forward)

- One regulatory mitigation of IoT dark patterns could be the idea of **“design loyalty” rules**
- Standardization of autonomous and transparent templates that counter ones geared towards consumer harms
- There is a need to increase transparency in feature design
- Draw on existing laws and expand them:
  - The California Age-Appropriate Design Code Act
  - Privacy law’s data minimization principle

## Discussion Question

Q

How can we enforce laws (or lack of laws) governing design practices and dark patterns? Does the idea of design templates make sense? Are there any issues that could arise from the integration of design templates into industry practice?

## Wrap Up Question

Q

If we can imagine all the worst possible scenarios (ala design fiction) that can arise from dark patterns, would people be more concerned about them?

Take a moment to think and we'll ask for you to share :)

# Discussion Question

Q

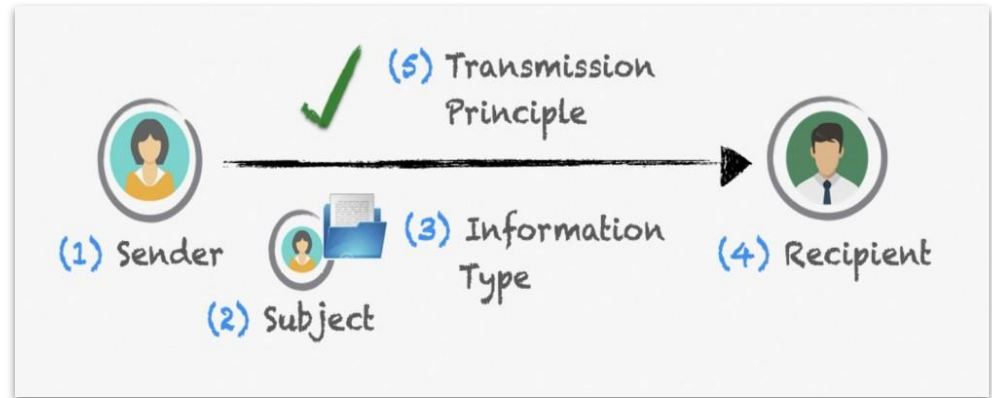
How can users become more aware and empowered to recognize and navigate dark patterns effectively?

Take a few minutes to talk with a partner/group and we'll ask for you to share :)



# Discussion Paper #2

Arnout Terpstra, Alwin De Rooj, and Alexander Schouten. **Online Proctoring: Privacy Invasion or Study Alleviation?: Discovering Acceptability Using Contextual Integrity.** CHI (2023).



# Experiences with Online Proctoring

Q

Have you used online proctoring systems before?

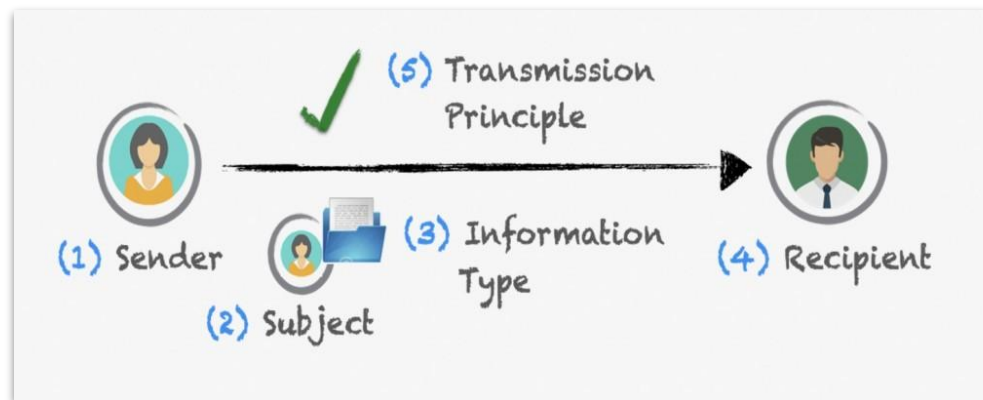
What are your feelings about these systems?

Did you experience any privacy-related issues or concerns with these systems?

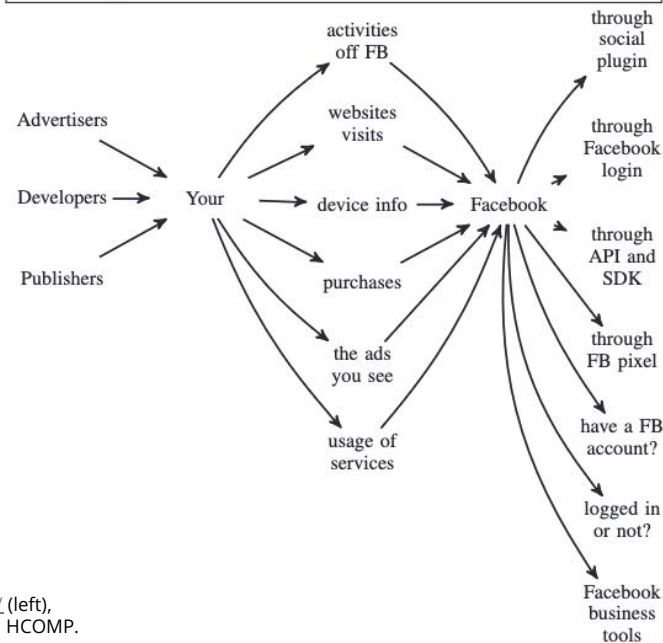
# Contextual Integrity (CI)

- Theory of Privacy
  - Developed by Helen Nissenbaum, Professor at Cornell University
  - Introduced in "Privacy as Contextual Integrity," Washington Law Review, 2004
- Context
  - Discussions of public surveillance through technology
  - Rooted in philosophy, law, ethics, and technology
- Goal
  - "Contextual Integrity (CI) defines privacy as the appropriateness of information flows determined by conformance with existing legitimate, informational norms specific to given social contexts"
    - Y. Shvartzshnaider, N. Aphorpe, N. Feamster, H. Nissenbaum (2019) ["Going Against the \(Appropriate\) Flow: A Contextual Integrity Approach to Privacy Policy Analysis"](#) The Seventh AAAI conference on Human Computation and Crowdsourcing (HCOMP)

# Contextual Integrity (CI)



[Advertisers, app developers and publishers]<sup>senders</sup> can send [us]<sup>recipient</sup> information [through Facebook Business Tools that they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs or the Facebook pixel]<sup>TP</sup>. These partners provide information about [your]<sup>subject</sup> [activities off Facebook including information about your device, websites you visit, purchases you make, the ads you see and how you use their services]<sup>attributes</sup> [whether or not you have a Facebook account or are logged in to Facebook]<sup>TP</sup>.



Images: <https://voicesofvr.com/998-primer-on-the-contextual-integrity-theory-of-privacy-with-philosopher-helen-nissenbaum/> (left), Shvartzshnaider et al. 2019. "Going Against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis", HCOMP.

# Overview of Study

- Explore the acceptability of online proctoring information flows regarding to privacy concerns among students.
- Use the Contextual Integrity (CI) framework to analyze the acceptability of various information flows within online proctoring.
  - Five parameters in Contextual Integrity (CI) framework: (1) the sender of the information, (2) the **recipient** of the information, (3) the **type of information** being transmitted, (4) the subject about whom the information is, (5) the **transmission principle(s)**
- Conduct a survey with 456 students rate the acceptability of 1064 proctoring information flows with varying information types, recipients, and transmission principles (each participant only answer a set of questions).
- Aims to
  - Apply the CI framework to provide more nuanced understanding of privacy concerns instead of general feeling.
  - Discover people's attitudes towards each of the individual contextual factors during online proctoring and how they affect each other.
  - Discuss the implications of the findings and provide recommendations for educational institutions using online proctoring.

# How does this paper argue that its topic is worthy of study?

“Due to the nature of what must be observed or recorded by online proctoring software, it comes as no surprise that privacy issues have been raised ...”

“Yet, no prior studies have investigated which specific factors fall under these topics and how they might affect privacy concerns and acceptability of online proctoring software.”

“In many studies, people are asked in general how they feel about privacy while the during the actual behavioural experiment which then follows, people make much more nuanced privacy decisions based on the five contextual factors described by the CI framework. Thus, conceptualisations and assessments of privacy should incorporate more nuanced contextual factors as opposed to generally stated privacy preferences in order to better understand why individuals want to share data or not.”

# Key Findings & Arguments

1. In general, **the acceptability of many information flows** in online proctoring was found to be neutral or somewhat unacceptable.
  - Most information types were considered **neutral. Acceptable:** Recording of the participant's computer screen and personal details. **Unacceptable:** A video recording of the entire room and tracking eye movements.
  - **Neutral:** Recipients relevant to online proctoring, such as the proctor and the course teacher. **Unacceptable:** Recipients unrelated to fraud detection.
  - **Neutral:** Some transmission principles such as data viewed by a real person and data removed after receiving the final grade. **Unacceptable:** principles such as data analyzed using AI and data used for personalized Ad.

# Key Findings & Arguments

2. When specific contextual factors were included, some combinations led to increases in acceptability. The acceptability of certain information types and transmission principles varied significantly, but differences between recipients were quite small.

- Information types: **Student's answers to exam questions**, were highly sensitive to contextual factors. Transmission principles: **Data used for personalized Ad and unknown data storage duration**, significantly decreased acceptability.

3. If highly sensitive information types are not shared with recipients outside of the context of education, students' objections are somewhat alleviated.



# Areas of Inquiry Within HCI

## Privacy in HCI

Privacy concerns related to the use of online proctoring software.

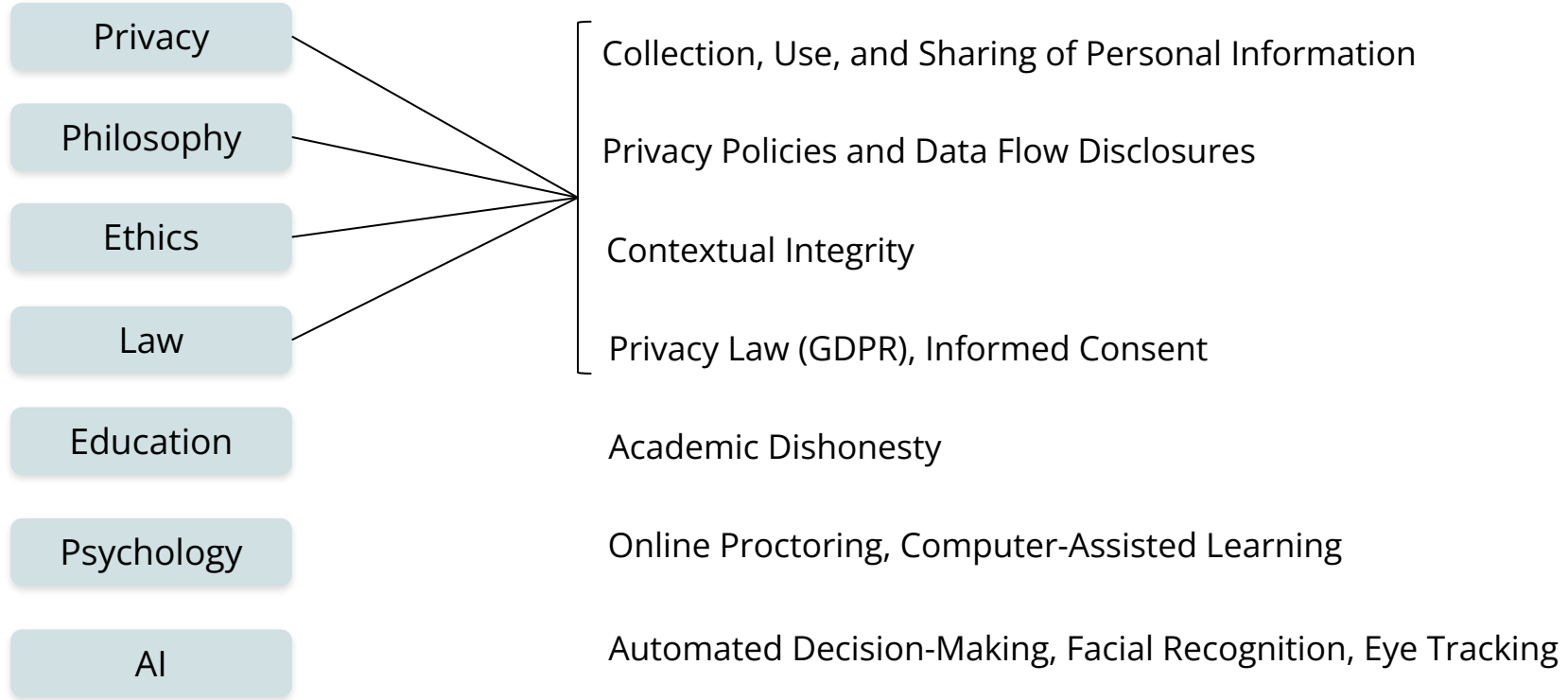
## Technology in Education

Use of technology in education, specifically online testing. Involves understanding how technology can support learning and assessment processes while also considering the needs and concerns of students.

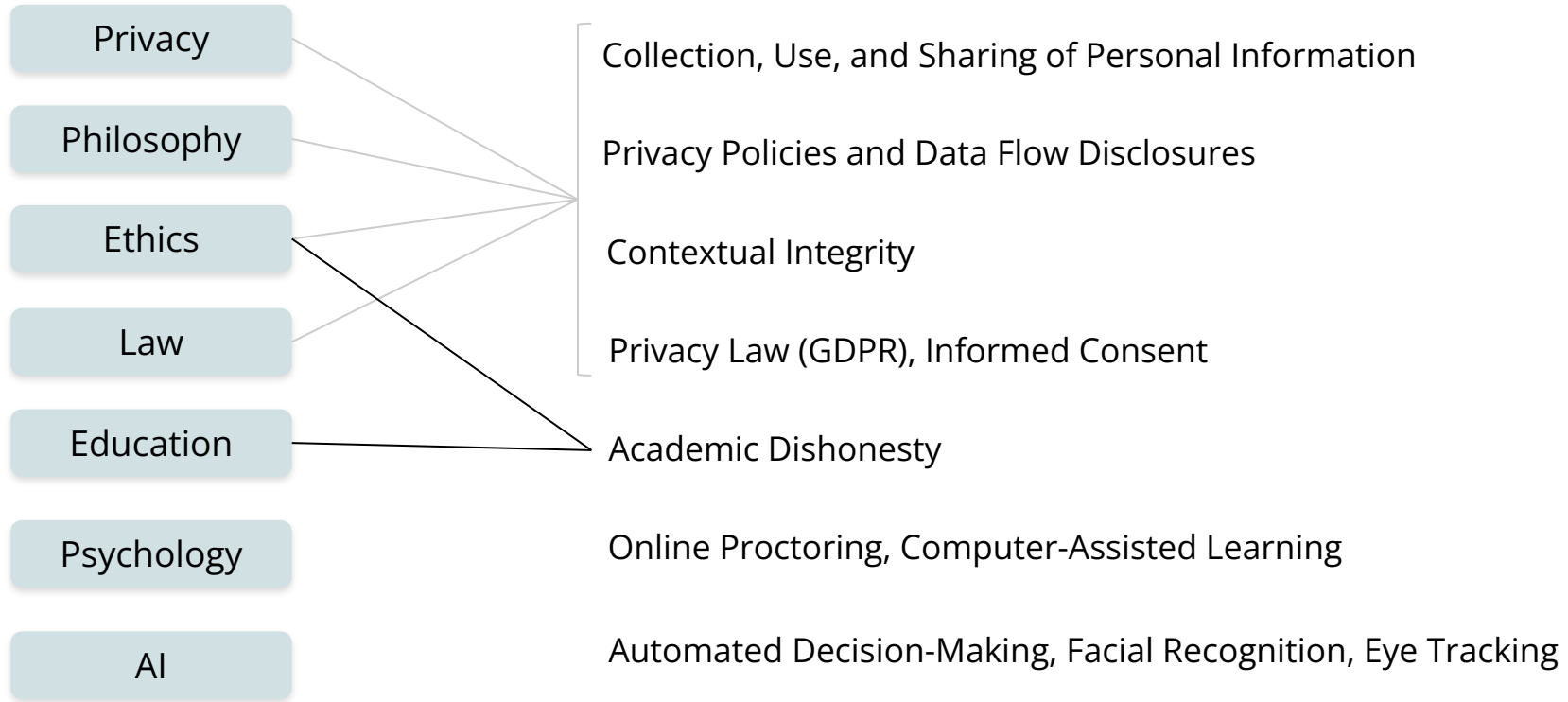
## Ethics in HCI

Also touches on ethical considerations and suggestions in HCI, in terms of users perception towards privacy and the use of their personal data

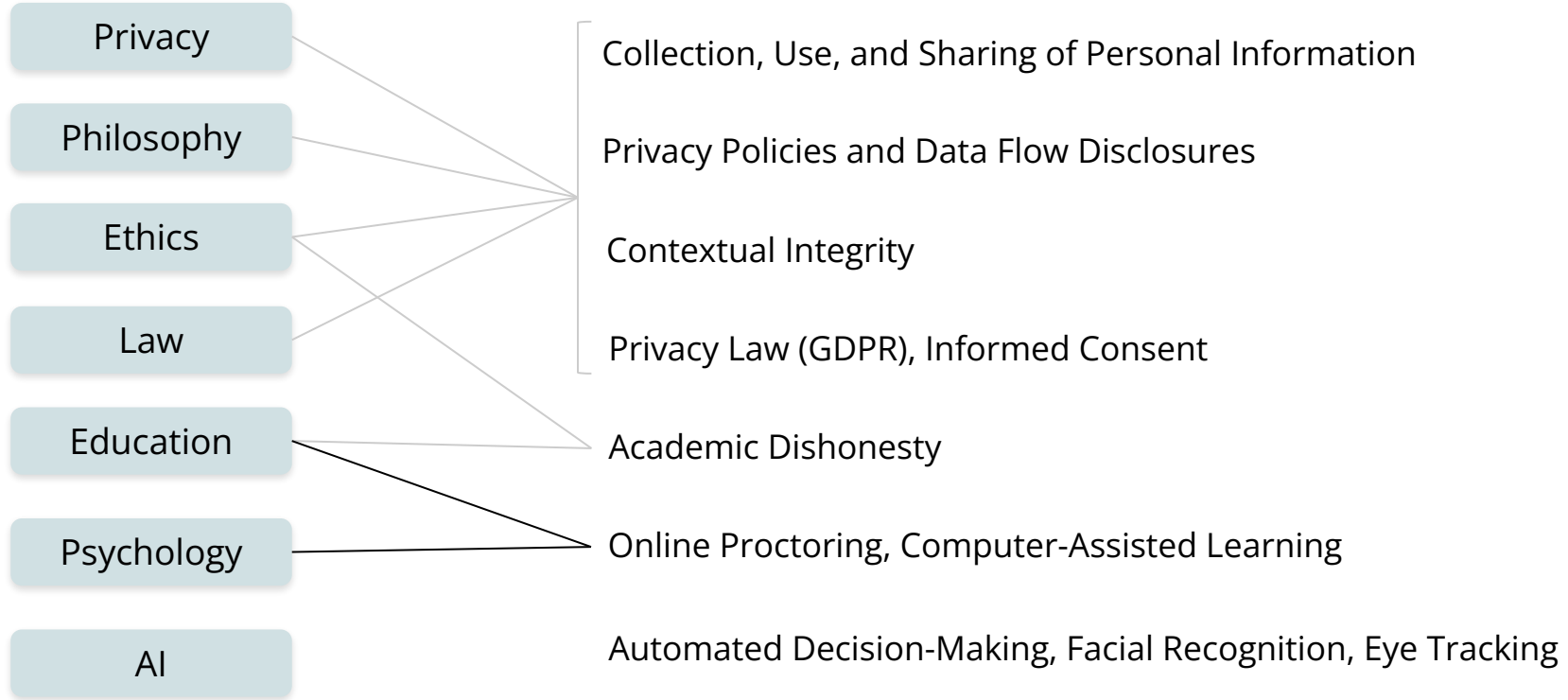
# Areas of Inquiry Outside of HCI



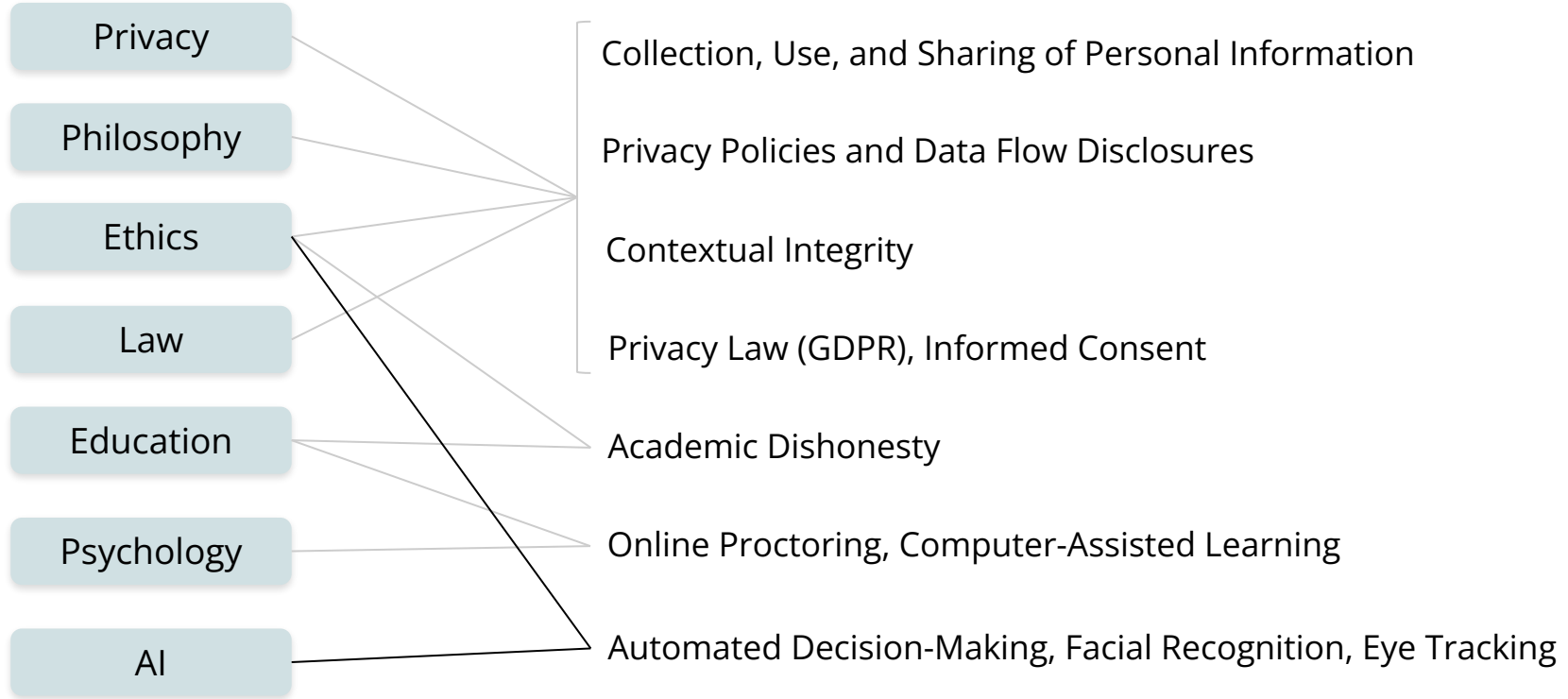
# Areas of Inquiry Outside of HCI



# Areas of Inquiry Outside of HCI



# Areas of Inquiry Outside of HCI



# Contributions

Empirical

Artifact

Methodological

Theoretical

Dataset

Survey

Opinion

# Contributions

Empirical

Artifact

Methodological

Theoretical

Dataset

Survey

Opinion

- This study contributes (*empirical*) insights by using the (*methodological*) Contextual Integrity (CI) framework in designing a survey to discover how students rate the acceptability of proctoring information flows
- It suggests that addressing these concerns requires not only improving the software itself but also raising awareness, clarifying instructions, and improving policies

# Main Takeaways for HCI Community

- **Importance of Context**

- Acceptability of information types, recipients, and transmission principles varies significantly based on context
- This emphasizes the need for a more nuanced understanding of privacy concerns when dealing with online proctoring software.

- **Privacy Violations**

- Crossing contextual boundaries often results in privacy violations (e.g., using the data for personal advertisements, profiling significantly reduces acceptability)
- It's critical to ensure the use of online proctoring software respects privacy norms and regulations.

- **Several Recommendations for Using Online Proctoring**

- Avoiding invasive scans, asking for explicit student permission, carefully configuring the information types used, communicating storage limitations clearly, and restricting the use of proctoring data to fraud detection purposes only.



# Main Takeaways Beyond HCI

- **Tech Privacy Research & CI**

- Insights about applying CI to different technologies and research questions related to varied technological contexts

- **Law & Policy**

- Interrogating students' ability to consent in educational technology context under privacy law (e.g., GDPR)
- Framing privacy violations according to acceptability using CI

- **Privacy Awareness & Education**

- School administrators should scrutinize systems' privacy practices before imposing them on students
- Users may make poor privacy decisions in certain contexts without valid reasons to do so

# Let's Discuss!



How can these findings be extended to other contexts (beyond online proctoring systems) or research areas?

Thoughts:

- **Data minimization:** only collect information that is needed for functionality
- **Service minimization:** don't integrate privacy-invasive technologies when they are not needed
- **Contextual decision-making:** provide context about data being collected and the purpose of collection to enable more informed decisions

# Let's Discuss!



Should we ask for explicit permission for every data flow?

How to avoid turning these into dark patterns or information overload?

Would you voluntarily give up privacy and security for convenience or utility?

# Let's Discuss!



What are your thoughts about the **take-it-or-leave-it** framework (i.e., either you consent to everything or you don't use it)?

Should students be able to **deny** particular data flows when using such services, or be offered alternatives?

What about in other contexts, like gig workers who use apps on their devices for their job, such as for food delivery and ride-hailing services?

# Let's Discuss!



Consider the GDPR definition of consent:

'consent' of the data subject means any **freely given, specific, informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

While this is not case in the US (yet), should it be? As developers and designers, how can we enable users to give this type of consent while balancing information overload and usability?

Source: <https://gdpr.eu/article-4-definitions/>

# Let's Discuss!

Q

What are your thoughts on personalized ads? Pros & cons?

Contextual vs behavioral ads?

*[from Perusall]*

# Some S&P Week Takeaways

- Be skeptical, both as a user and designer/developer
  - Now you know what dark patterns are and how to spot them!
- Every design decision potentially nudges users in one direction or another
- Be wary of how design and development decisions impact privacy and security, especially in sensitive contexts and among vulnerable groups

For more: **highly** recommend looking up *Surveillance Capitalism* & the work of Shoshana Zuboff (<https://shoshanazuboff.com>, <https://youtu.be/hlXhnWUmMvw>)

# Thank you!

