Privacy Tools

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

12/03/2024

THE UNIVERSITY *of* EDINBURGH

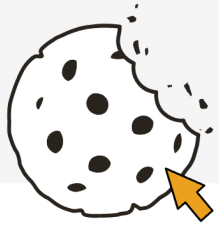
Overview

- Warm-up
- Contextual integrity - continued
- Privacy tool
- Ad blocker
- Take-home


Tor
TorProject.org

AdblockPlus

Download About Premium Help English (US)



NEW! **Block annoying cookie banners**

Tired of those frustrating pop-ups about cookies on every website? Start blocking them with Adblock Plus Premium and enjoy a better browsing experience today.

Learn More

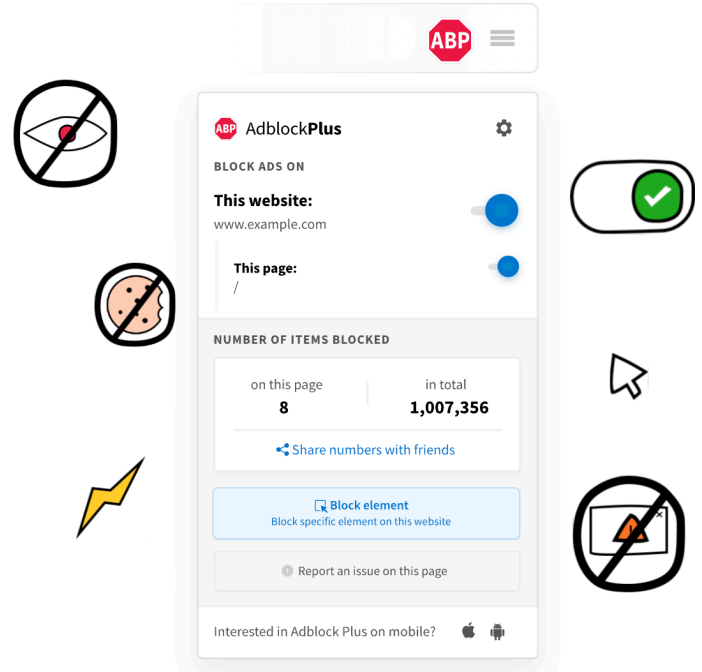
Surf the web with no annoying ads

- Experience a cleaner, faster web and block annoying ads
- Acceptable Ads are allowed by default to support websites (learn more) [1]
- Adblock Plus is free and open source (GPLv3+)

By clicking the button below, you agree to our Terms of Use.

GET ADBLOCK PLUS FOR CHROME

Download Adblock Plus for another browser



Is ad blocker a privacy-preserving tool? Why?

A TAXONOMY OF PRIVACY

INFORMATION PROCESSING

AGGREGATION
Combining of various pieces of personal information

A credit bureau combining an individual's payment history from multiple creditors.

SECONDARY USE
Using personal information for a purpose other than the purpose for which it was collected

The U.S. Government using census data collected for the purpose of apportioning Congressional districts to identify and intern those of Japanese descent in WWII.

EXCLUSION
Failing to let an individual know about the information that others have about them and participate in its handling or use

A company using customer call history, without the customer's knowledge, to shift their order in a queue (i.e. "Your call will be answered in the order [NOT] received")

INSECURITY
Failing to protect information

An ecommerce website allowing others to view an individual's purchase history by changing the URL (e.g. enterprivacy.com?id=123)

IDENTIFICATION
Linking of information to an individual. [Sometimes called 'singling out']

A researcher linking medical files to the Governor of a state using only date of birth, zip code and gender.

COLLECTION

SURVEILLANCE
Watching, listening to, or recording of a person's activities

A website monitoring cursor movements of a visitor while visiting the website.

INTERROGATION
Questioning or probing for personal information

An interviewer asking an inappropriate question, such as marital status, during an employment interview.

INVASION

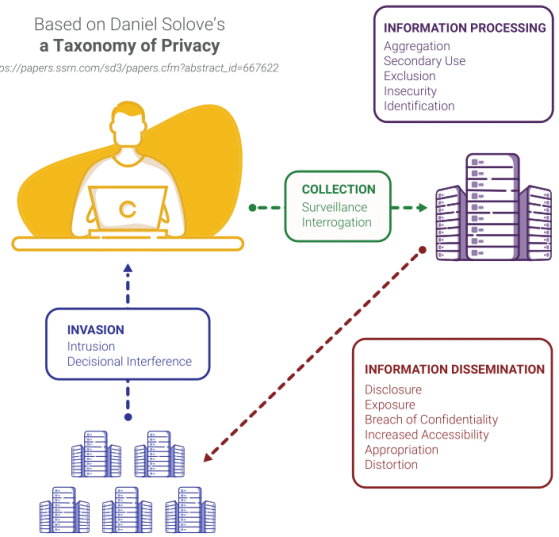
INTRUSION
Disturbing a person's tranquility or solitude

An augmented reality game directing players onto private residential property.

DECISIONAL INTERFERENCE
Intruding into a person's decision making regarding their private affairs

A payment processor declining transactions for contraceptives.

Based on Daniel Solove's
a Taxonomy of Privacy
https://papers.ssrn.com/sd3/papers.cfm?abstract_id=667622



INFORMATION DISSEMINATION

DISCLOSURE
Revealing truthful information about a person that impacts their security or the way others judge their character

A government agency revealing an individual's address to a stalker, resulting in the individual's murder.

EXPOSURE
Revealing a person's nudity, grief, or bodily functions

A store forcing a customer to remove clothing revealing a colostomy bag.

BREACH OF CONFIDENTIALITY
Breaking a promise to keep a person's information confidential.

A doctor revealing patient information to friends on a social media website.

INCREASED ACCESSIBILITY
Amplifying the accessibility of personal information

A court making proceeding searchable on the Internet without redacting personal information.

APPROPRIATION
Using an individual's identity to serve the aims and interests of another

A social media site using customer's images in advertising.

DISTORTION
Disseminating false or misleading information about a person

A creditor reporting a paid bill as unpaid to a credit bureau.

Version 6 (2022)

PRIVACY BY DESIGN

https://privacybydesign.training

https://www.jstor.org/stable/40041279

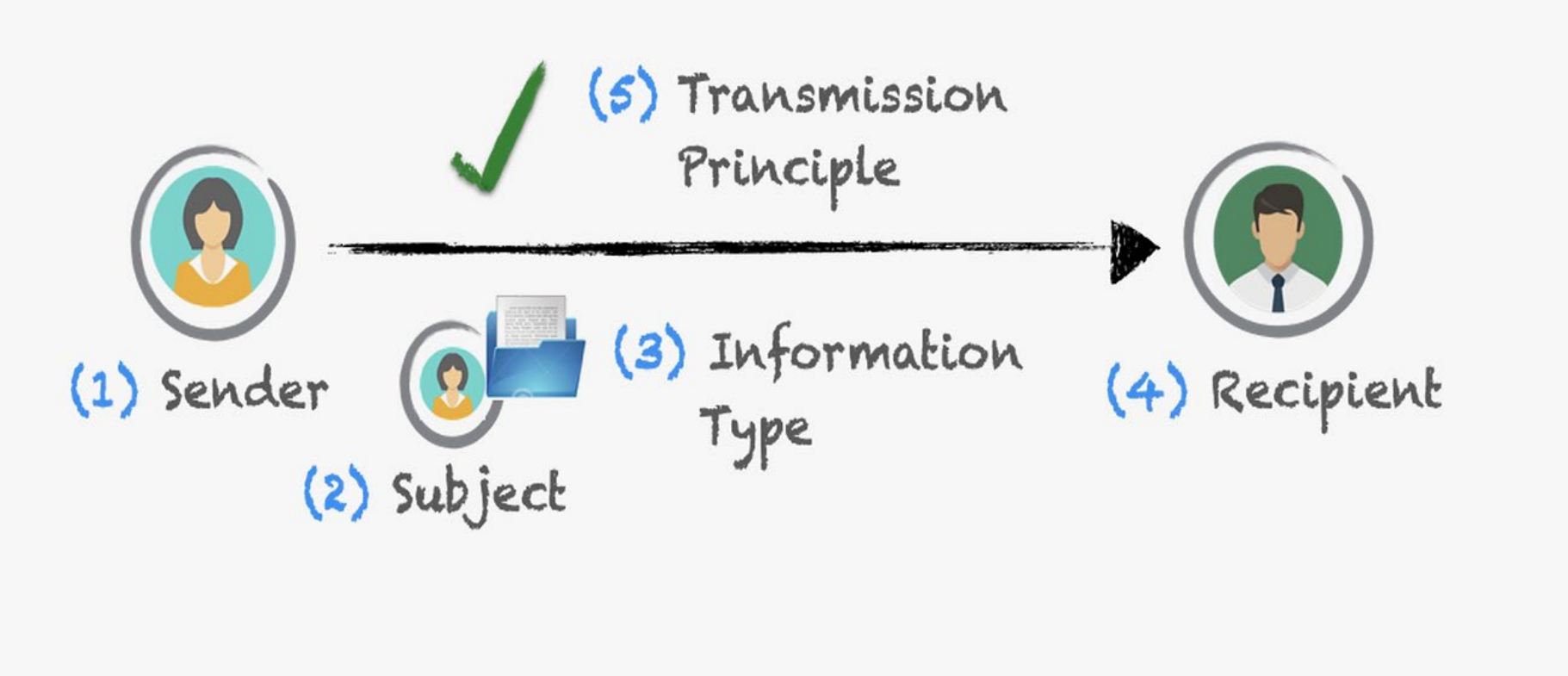
Contextual integrity

Contextual integrity

- Privacy is defined by how **information flows**
- Information flow is appropriate when it conforms with **contextual privacy norms**
- A contextual norm can be described by (at least) five parameters
  - data type (what sort of information is being shared)
  - data subject (who/what the information is about)
  - sender (who/what is sharing the data)
  - recipient (who/what is getting the data)
  - transmission principle (the constraints imposed on the flow/how), e.g., with one's consent.
- New norms and flows are evaluated through their context

Malkin, N., 2022. Contextual Integrity, Explained: A More Usable Privacy Definition. *IEEE Security & Privacy*, *21*(1), pp.58-65.

Contextual integrity



https://www.dli.tech.cornell.edu/post/privacy-policies-as-contextual-integrity-beyond-rules-compliance

Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates

Shikun Zhang
Carnegie Mellon University
Pittsburgh, PA, USA
shikunz@cs.cmu.edu

Yan Shvartzshnaider
York University
Toronto, Canada
yansh@yorku.ca

Yuanyuan Feng
University of Vermont
Burlington, VT, USA
yuanyuan.feng@uvm.edu

Helen Nissenbaum
Cornell Tech
New York, NY, USA
hn288@cornell.edu

Norman Sadeh
Carnegie Mellon University
Pittsburgh, PA, USA
sadeh@cs.cmu.edu

ABSTRACT

We present an empirical study exploring how privacy influences the acceptance of vaccination certificate (VC) deployments across different realistic usage scenarios. The study employed the privacy framework of Contextual Integrity, which has been shown to be particularly effective in capturing people's privacy expectations across different contexts. We use a vignette methodology, where we selectively manipulate salient contextual parameters to learn whether and how they affect people's attitudes towards VCs. We surveyed 890 participants from a demographically-stratified sample of the US population to gauge the acceptance and overall attitudes towards possible VC deployments to enforce vaccination mandates and the different information flows VCs might entail. Analysis of results collected as part of this study is used to derive general normative observations about different possible VC practices and to provide guidance for the possible deployments of VCs in different contexts.

1 INTRODUCTION

The prolonged and devastating COVID-19 pandemic has affected every aspect of people's lives as well as the global economy. In an attempt to curb the spread of highly contagious variants, governments around the world have contemplated or adopted vaccination mandates (VMs) and vaccination certificates (or passports) (VCs) in schools, hospitals, public transportation, and other social contexts [15, 27, 42, 43, 50, 53, 62]. COVID VMs and VCs challenge established societal norms and conventions. While vaccination mandates and certificates are not new (e.g., vaccination mandates for children attending schools, "yellow cards" for travel to or from a country with a high risk of diseases such as yellow fever [55]), the sudden and unprecedented requirement to show proof of vaccination to gain access to public venues or engage in a range of daily activities has triggered a fierce global debate on the appropriateness of COVID-19 VMs and VCs in light of established societal norms and conventions, perceived privacy harms, and civil liberty expectations [9, 34, 36, 61, 69].

Background

- Health and safety are crucial objectives during COVID-19 pandemic
- Vaccine mandates and certificates were rolled out to track people
- COVID vaccine mandates and certificates challenge established societal norms and conventions related to privacy

What are the new privacy norms (e.g., acceptance of data collection) related to vaccine certificates?

Study method

- Vignette-based survey using contextual integrity framework
- Recruited 890 people in the US online in July 2021
- Quantitative analysis of survey data

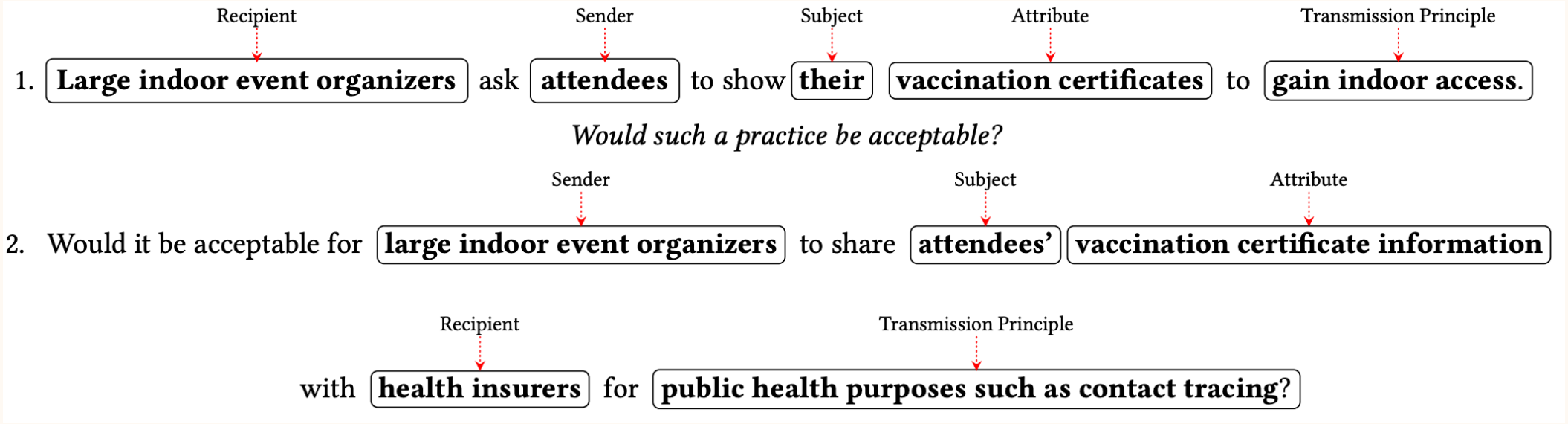
Study method: vignette

> [Recipient] ask [Sender] to show their (Subject) vaccination certificates (Attribute) to [Transmission Principle]. Would such a practice be acceptable?

> Would it be acceptable for [Sender] to share [Subject] [Attribute] with [Recipient] for [Transmission Principle]?

- First hand sharing & resharing scenarios
- 5-point Likert scale to rate the acceptance level

Study method: vignette



Study method: vignette

Sender	Subject
stores and restaurants	customer's
recreational services or facilities	
long-distance transportation	passenger's
public transportation operators	
rideshare and taxi companies	
cruise companies	
customs and border control agencies	traveler's
large event operators	attendee's
places of worship	
workplaces	employee's
residential and real estate management	visitor's
schools	
hospitals and assisted living facilities	
government buildings	

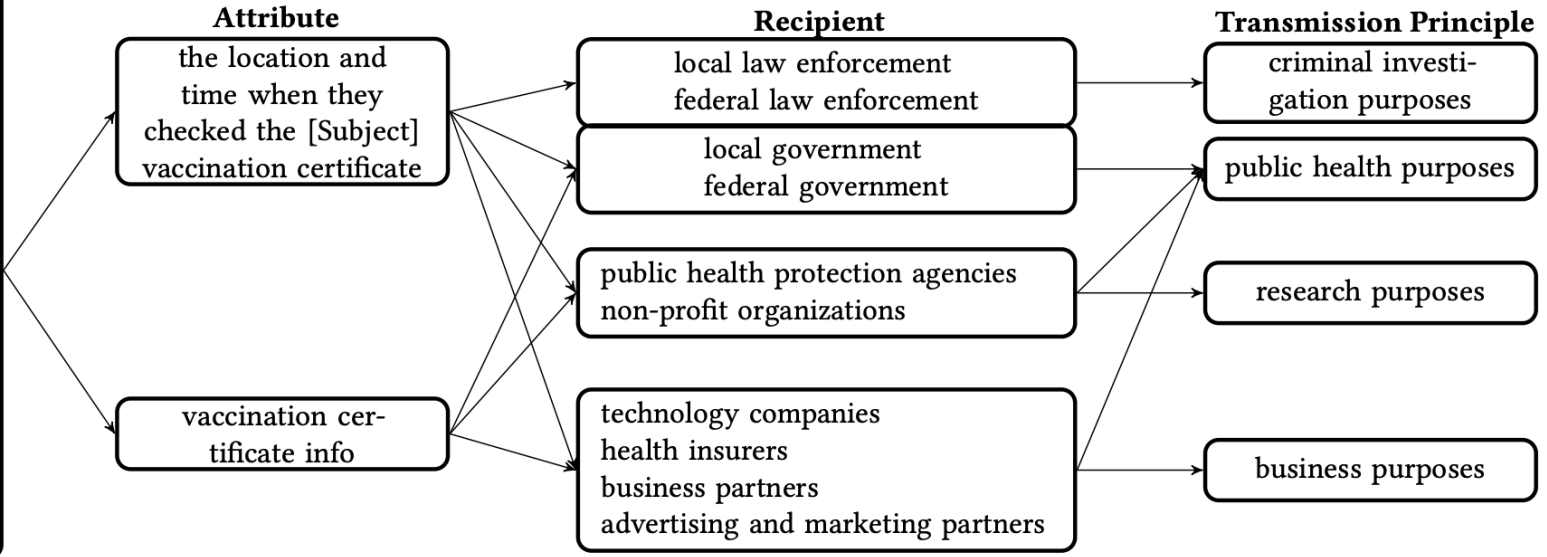
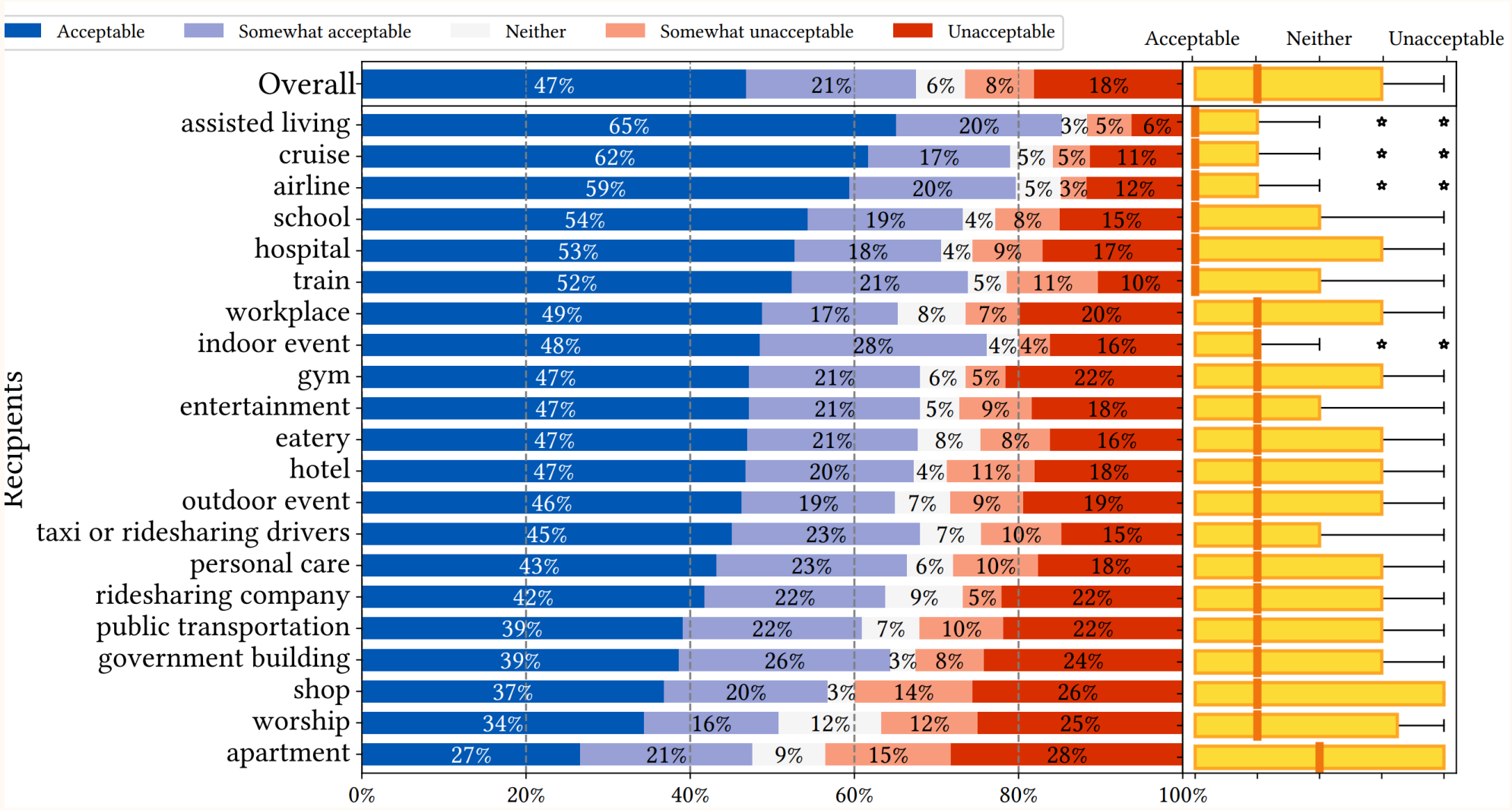


Figure 2: CI parameters used for vignettes involving re-sharing VC information

Findings


Acceptable
Somewhat acceptable
Neither
Somewhat unacceptable
Unacceptable
Recipients
Overall 47% 21% 6% 8% 18%
assisted living 65% 20% 3% 5% 6%
cruise 62% 17% 5% 5% 11%
airline 59% 20% 5% 3% 12%
school 54% 19% 4% 8% 15%
hospital 53% 18% 4% 9% 17%
train 52% 21% 5% 11% 10%
workplace 49% 17% 8% 7% 20%
indoor event 48% 28% 4% 4% 16%
gym 47% 21% 6% 5% 22%
entertainment 47% 21% 5% 9% 18%
eatery 47% 21% 8% 8% 16%
hotel 47% 20% 4% 11% 18%
outdoor event 46% 19% 7% 9% 19%
taxi or ridesharing drivers 45% 23% 7% 10% 15%
personal care 43% 23% 6% 10% 18%
ridesharing company 42% 22% 9% 5% 22%
public transportation 39% 22% 7% 10% 22%
government building 39% 26% 3% 8% 24%
shop 37% 20% 3% 14% 26%
worship 34% 16% 12% 12% 25%
apartment 27% 21% 9% 15% 28%
0%
20%
40%
60%
80%
100%
Acceptable
Neither
Unacceptable

Findings

- A VC mandate for international travel is perceived appropriate to take a flight or use at the border
- A VC mandate for employment: Perceived appropriate to apply for a job at assisted living facilities or hospitals
- A VC mandate for education: Perceived appropriate for teachers, less so for students
- A VC mandate in residential settings: Perceived as inappropriate overall

Findings

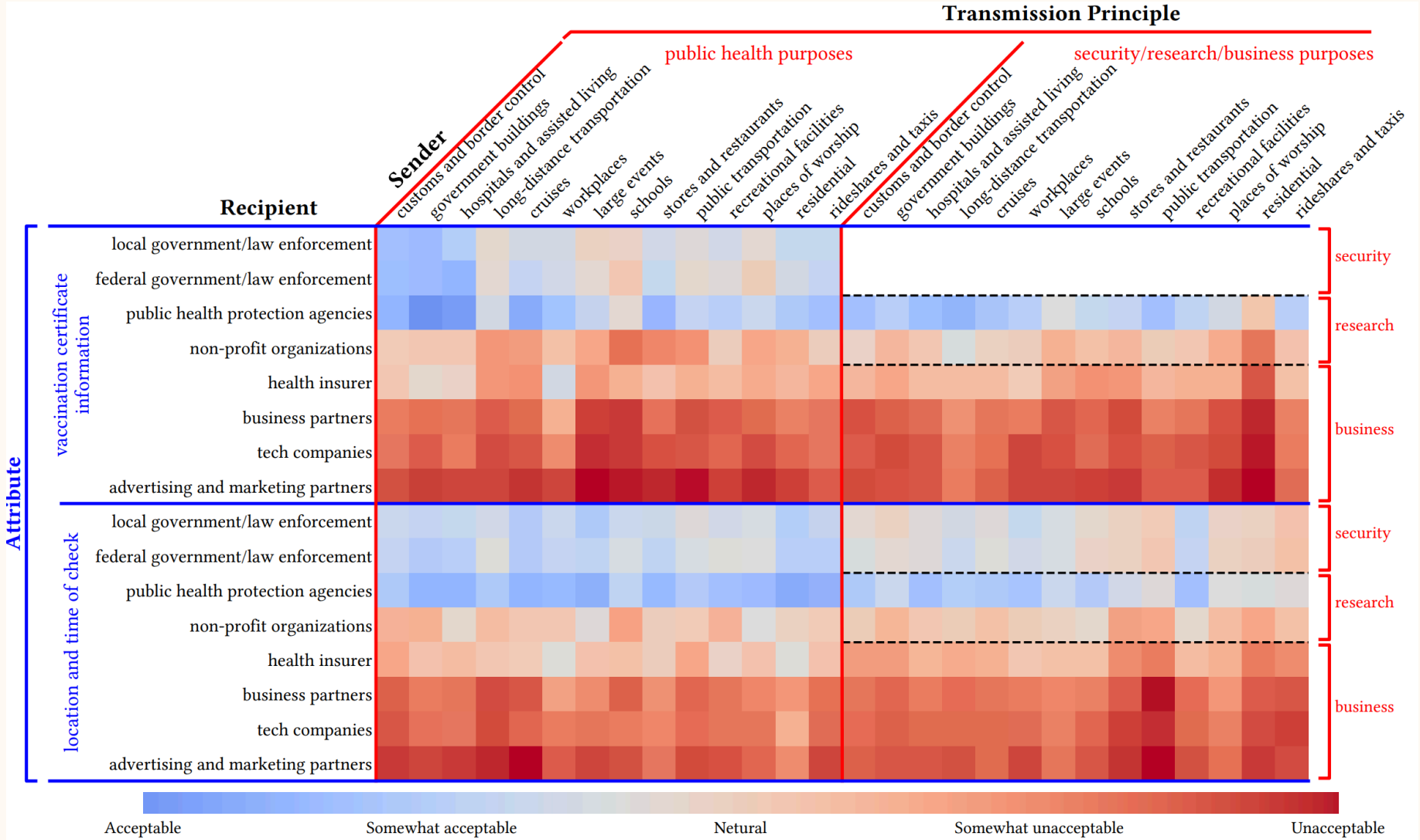
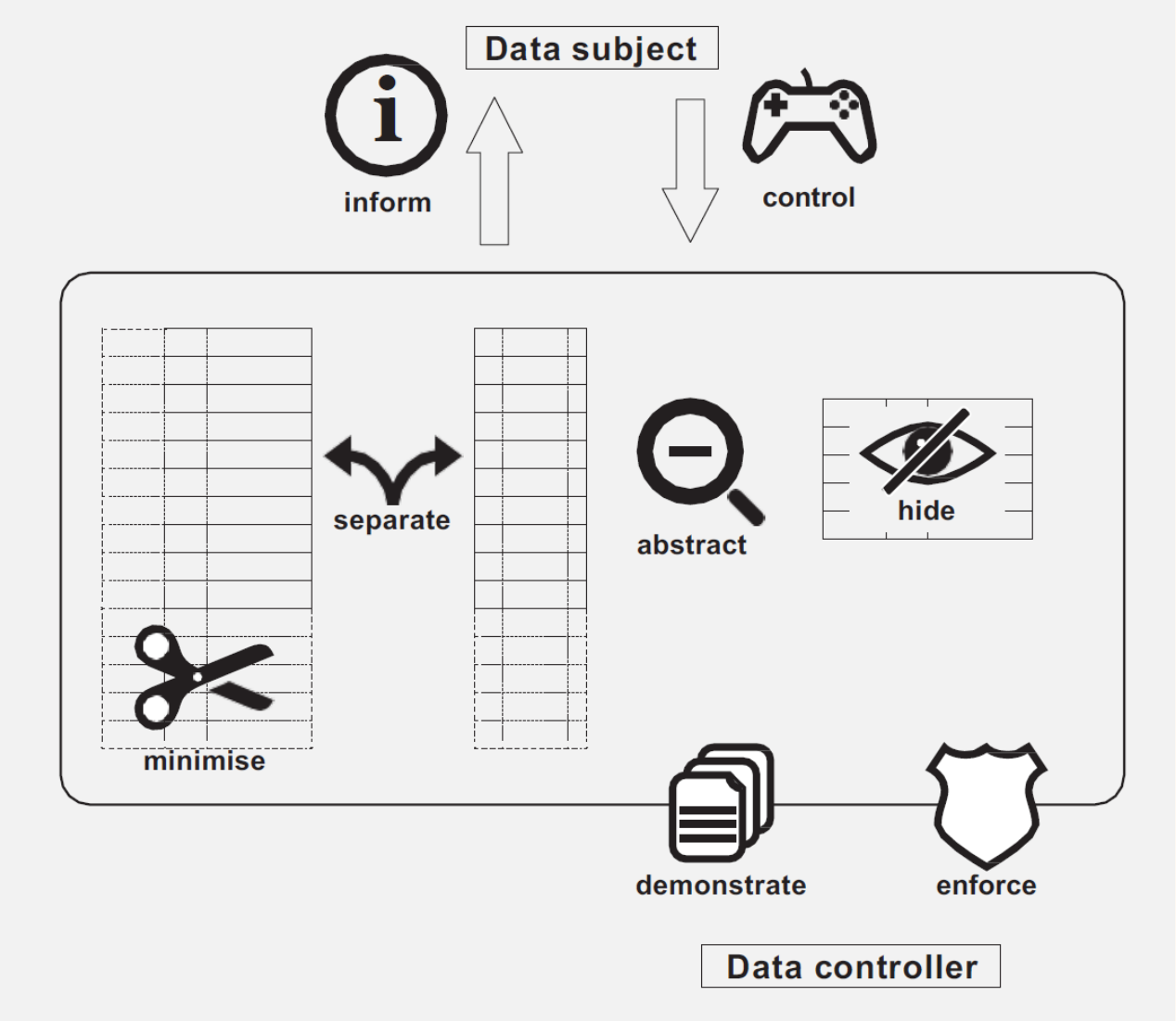


Figure 5: A heat map of the average of all participants' responses under a combination of four CI parameters (sender, recipient, attribute, and transmission principle). For instance, the color of the top left cell represents the acceptance level of the information flow—customs and border control agencies share their customers' vaccination certificate information with the local government for public health purposes.

How do we design usable privacy tools?

Privacy by design – strategies



Privacy space framework

Category	Description	Examples
Awareness	Informative	Display information about trackers on current webpage, whether location is being sent
Detection	Actively look for problems	Find trackers on current webpage
Prevention	Used as a precaution	Encryption tools, anonymity tools
Response	Taking action after a problem is detected	Tracking blocker
Recovery	Help you get back to normal	Patching bugs

Benjamin Brunk. A user-centric privacy space framework. In Cranor and Gafinkel, eds. *Security and Usability*. O'Reilly 2005. p. 401-420.

Types of privacy tools

- Cookie blockers
- Opt-out
- Encryption
- Anonymity
- Obfuscation
- Physical (blinds, etc.)
- ....

Where to put privacy tools?

- Built-in functions
- Plugin (e.g., browser, etc.)
- Server
- Operating system
- Mobile app
- Networking
- ....

How to get started? Think about system/threat modeling

Think and share: who will be motivated to design an ad blocker, and how?

Defining "Broken": User Experiences and Remediation Tactics When Ad-Blocking or Tracking-Protection Tools Break a Website's User Experience

Alexandra Nisenoff, *University of Chicago and Carnegie Mellon University;*
Arthur Borem, Madison Pickering, Grant Nakanishi, Maya Thumpasery,
and Blase Ur, *University of Chicago*

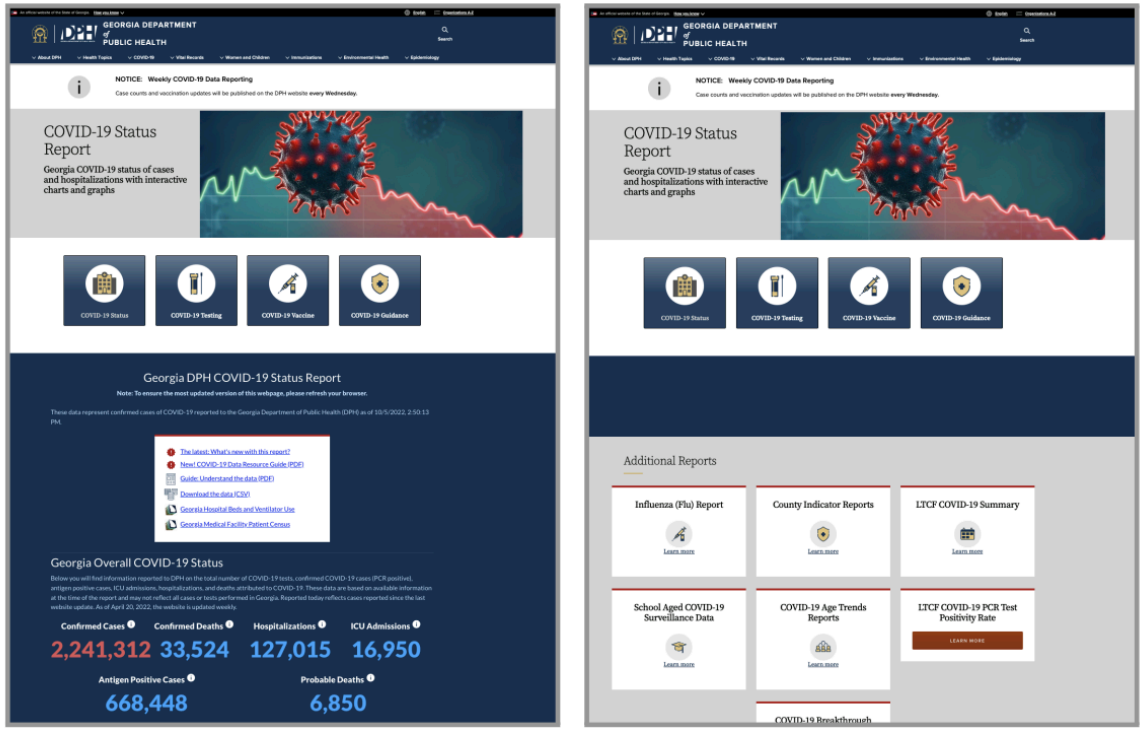
https://www.usenix.org/conference/usenixsecurity23/presentation/nisenoff-broken

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

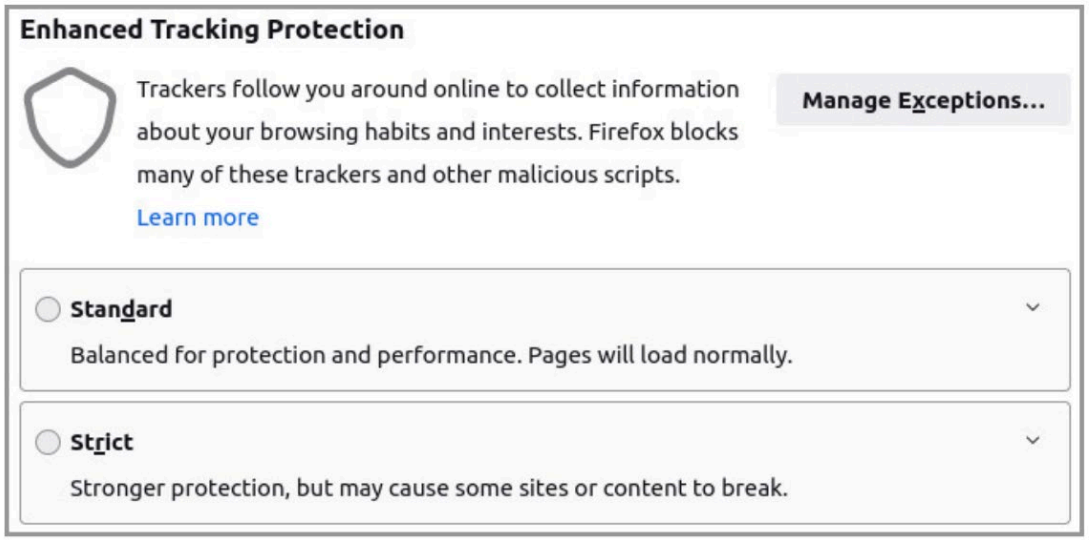
978-1-939133-37-3

Background



(a) Normal functionality. (b) "Broken" functionality.

Figure 1: Many tracking-protection tools cause the status report (blue background) to disappear from this website [28].



- Ad blockers may distort non-ad elements on the page

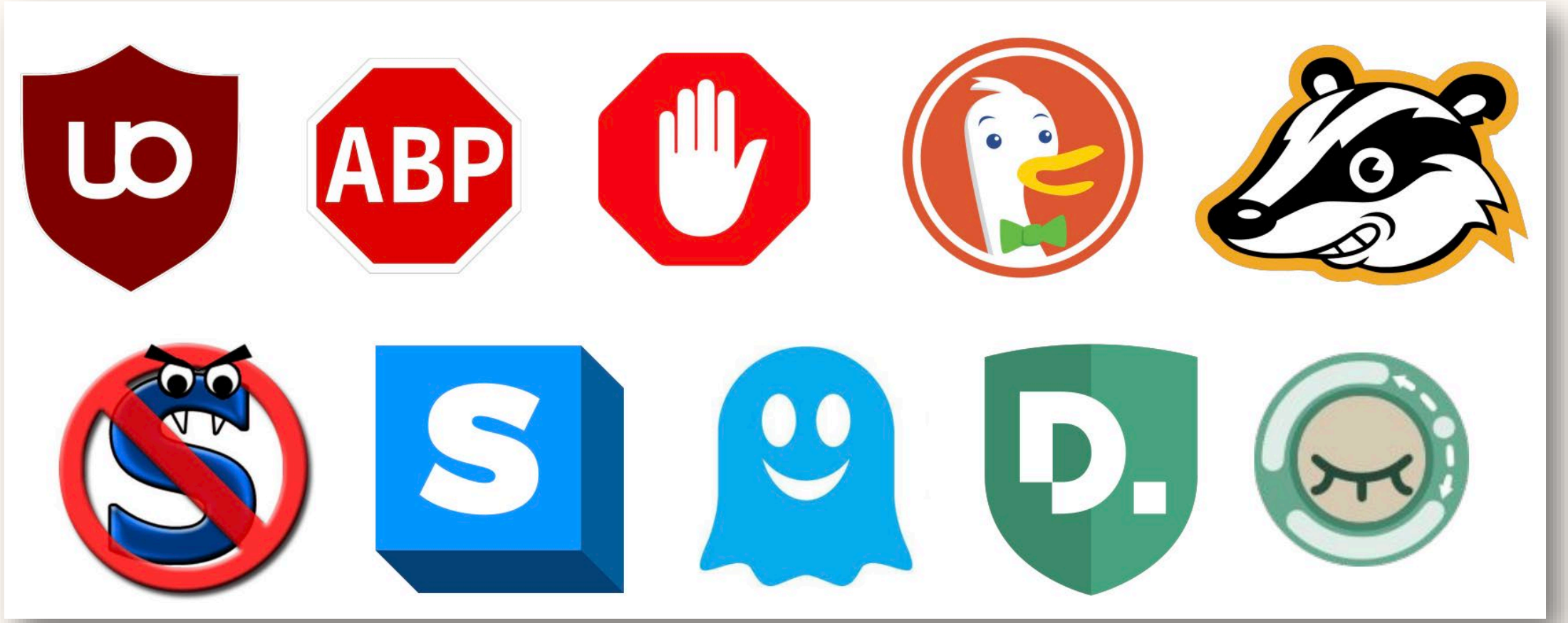
Research question

- What are all the ways these tools can break webpages?
- What do users do when they encounter breakage?
- How much do users care about these types of breakage?

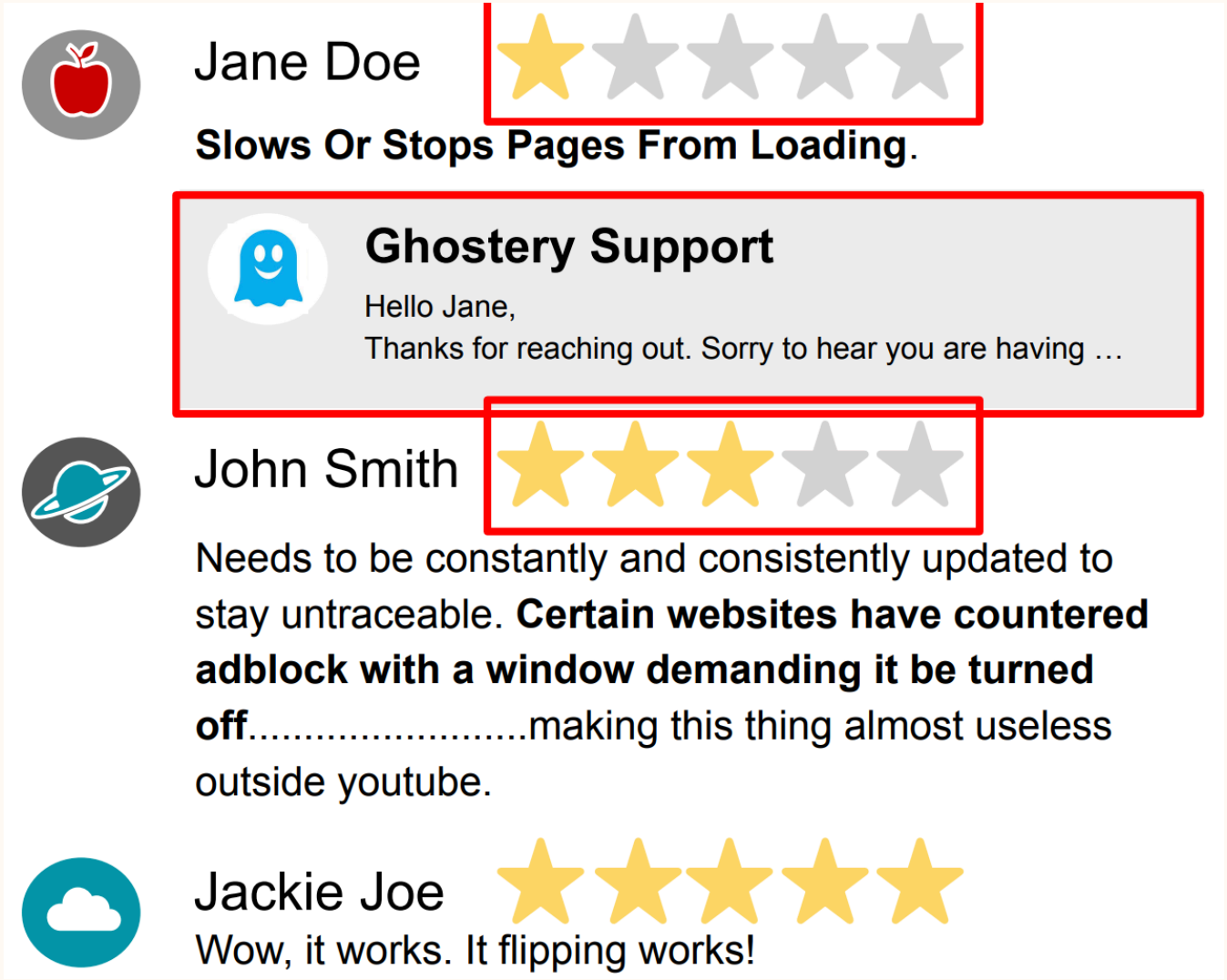
Method

- Analyze online user review and issue report
  - Goal: understand what are the issues and strategies
- Surveyed 100 US participants who have prior experience
  - Goal: understand people’s reactions in different contexts
- Qualitative and quantitative analysis

Method



User review and report analysis

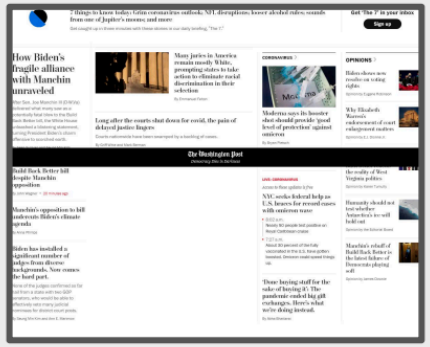


User review and report analysis

washingtonpost.com: breakage #1234

taylor1989 opened this issue on Dec 20, 2021 · 1 comment

When uBO is enabled, it sometimes **blocks actual news stories**, leaving spaces on the page. Screenshots show page with uBO enabled and same page with uBO disabled. This same breakage also occurs on other pages of the site, and with all content in their Travel Tips "By the Way" section; see: https://www.washingtonpost.com/travel/tips/omicron-holiday-travel-health-experts/
In all cases, **disabling uBO restores the missing articles**.



GitHub

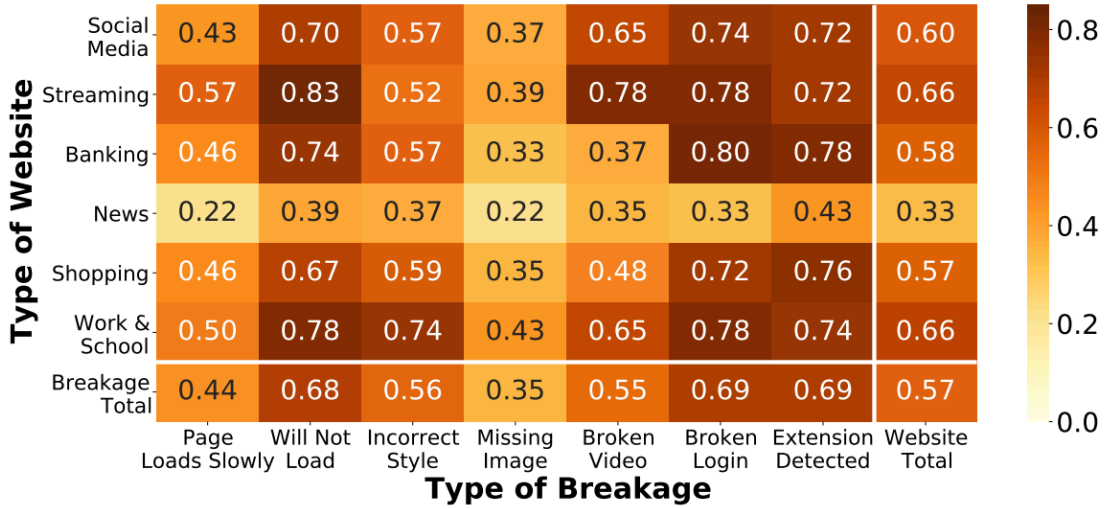
Taxonomy of breakage

- Loading and responsiveness (lag, reload issue, etc.)
- Resources and third party content (sound, style, image...)
- Extension detection and interaction (access blocked)
- HTML elements
- Browser level (browser crash, etc.)
- Authentication and sessions
- Vague

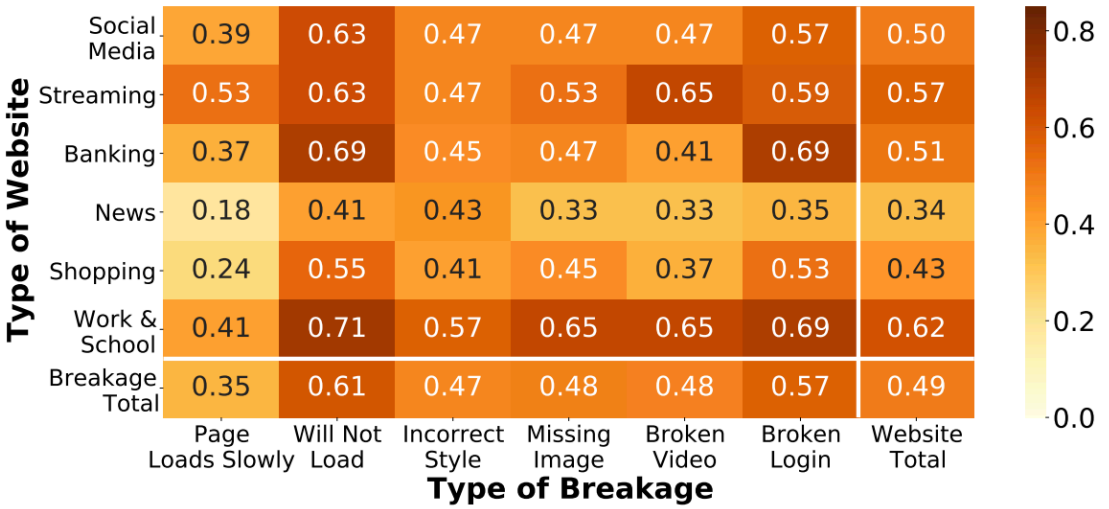
Taxonomy of mitigation strategies

- Limiting functionality
  - Modifying the block list
  - Disabling the tool for the page
  - Disabling the tool entirely
  - ...
- Browser-level interventions
  - Checking the developer console
  - ...
- Page level interventions
  - Reloading pages
  - ....
- Vague

Findings from survey



(a) Extension.



(b) Browser.

Figure 5: The proportion of participants that stated they would attempt to fix the type of breakage for a given browsing context.

Take-home

- **(Blog)** Frik, A., Haviland, A. and Acquisti, A., 2020. The Impact of {Ad-Blockers} on Product Search and Purchase Behavior: A Lab Experiment. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 163-179).
- **(Blog)** Tech Radar - Microsoft Defender will finally stop claiming Tor is malware