Privacy Tools

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

12/03/2024
Overview

• Warm-up
• Contextual integrity - continued
• Privacy tool
• Ad blocker
• Take-home
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
- Adblock Plus is free and open source (GPLv3+)

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

Download Adblock Plus for another browser

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.
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 creators.

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 inhibit 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 this order, please hang up”)

INSECURITY
Failing to protect information
An e-commerce 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
又称 “singing out”
A researcher linking medical files to the Governor of a state using only state 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 interview 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.

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 restricting 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.

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

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]. Some proponents of VMs and VCs argue for overriding these
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

1. **Large indoor event organizers** ask **attendees** to show **their** **vaccination certificates** to **gain indoor access.**

   *Would such a practice be acceptable?*

2. Would it be acceptable for **large indoor event organizers** to share **attendees’ vaccination certificate information** with **health insurers** for **public health purposes such as contact tracing?**
Study method: vignette

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

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

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

![Image](image_url)

(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

Jane Doe
⭐⭐⭐⭐⭐
Slows or stops pages from loading.

Ghostery Support
Hello Jane,
Thanks for reaching out. Sorry to hear you are having …

John Smith
⭐⭐⭐⭐⭐
Needs to be constantly and consistently updated to stay untraceable. Certain websites have countered adblock with a window demanding it be turned off... making this thing almost useless outside youtube.

Jackie Joe
⭐⭐⭐⭐⭐
Wow, it works. It flipping works!
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.**
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

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) Tech Radar - Microsoft Defender will finally stop claiming Tor is malware