Enhancing Online Privacy: The Development of Practical Privacy Choice Mechanisms

Isabella Tassone, Chunyue Ma, Eliza Kuller, Joe Champeau, Sebastian Zimmeck

Department of Mathematics and Computer Science
Wesleyan University, Middletown, CT, 06459

Introduction

Third-party tracking occurs online when a website you intentionally visit collects your data, and then shares or sells it with other sites you did *not* visit. According to The California Consumer Privacy Act (CCPA) and other laws, people have a legal right to opt out from the sharing/selling of their data. However, **there remains to be a lack of practical mechanisms for people to exercise their legal right to privacy on the internet.**

The obvious solution to this problem is to develop a **useable, neutrally-worded privacy choice mechanism that provides users with an active choice.** To further break it down:

- **Usability:** The mechanism should not be disruptive to the user's online experience, and must be simple enough for anybody to understand with little background knowledge
- **Neutrality:** The mechanism should not pressure or bias the user to make one decision over another
- **Active Choice:** With use of the mechanism, users should feel that they have adequate control over who obtains their data

In order to develop a privacy choice mechanism that best fulfills these requirements, we are conducting a research study that analyzes how people respond to different privacy choice mechanisms that vary in levels of **personalization** versus **generalization**. That is, to what extent people must make specific privacy decisions site-by-site. These mechanisms work by sending **Global Privacy Control (GPC)** signals, a specification that tells sites if a user does not want to be tracked. Although we are currently conducting the study, early results suggest that **although people will voice that they prefer personalization, when given both options they will instead make a generalized privacy choice.**

Current Findings

Early findings support the initial hypothesis that users will *say* that they desire personalization, but ultimately use generalized settings.
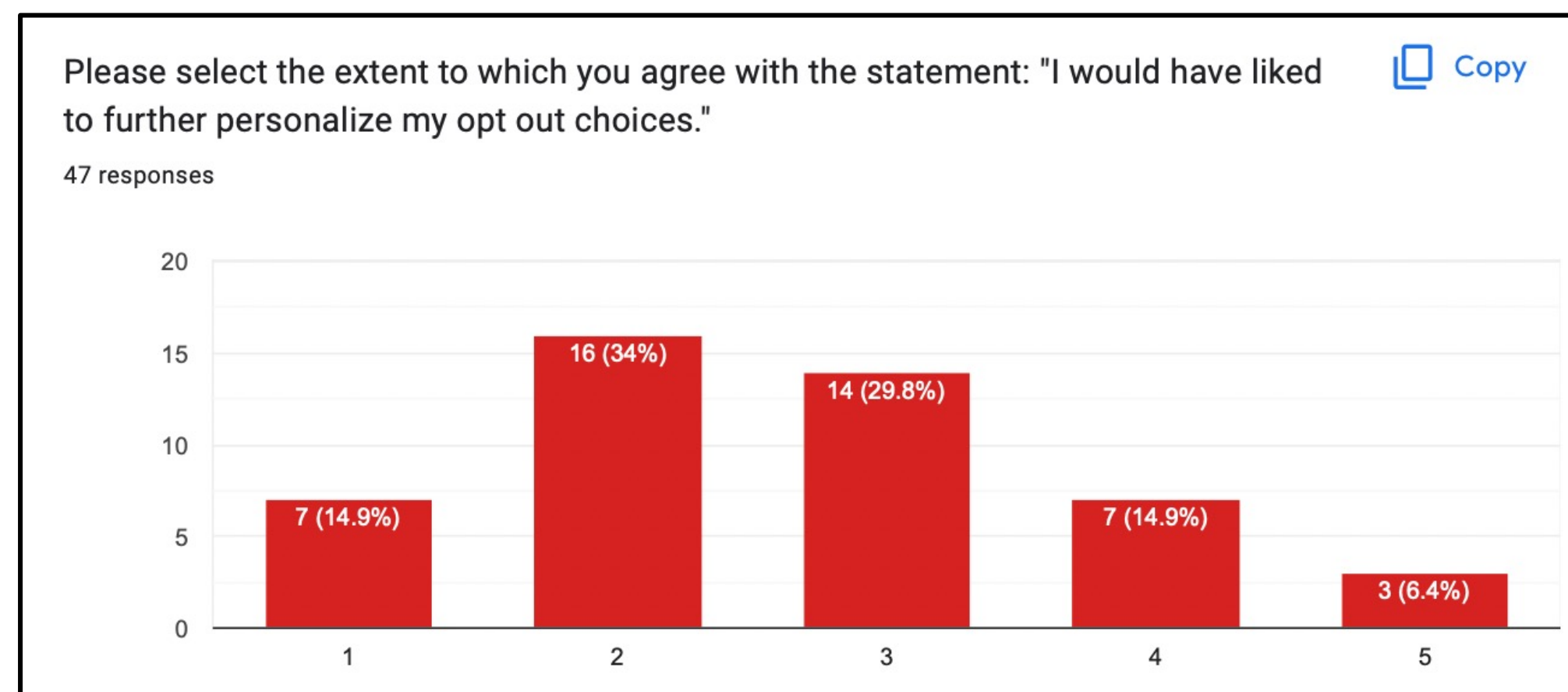
Scheme 2

Please select the extent to which you agree with the statement: "I would have liked to further personalize my opt out choices."
47 responses

Figure 1

Scheme 4

Please select the extent to which you agree with the statement: "I would have liked to further personalize my opt out choices."
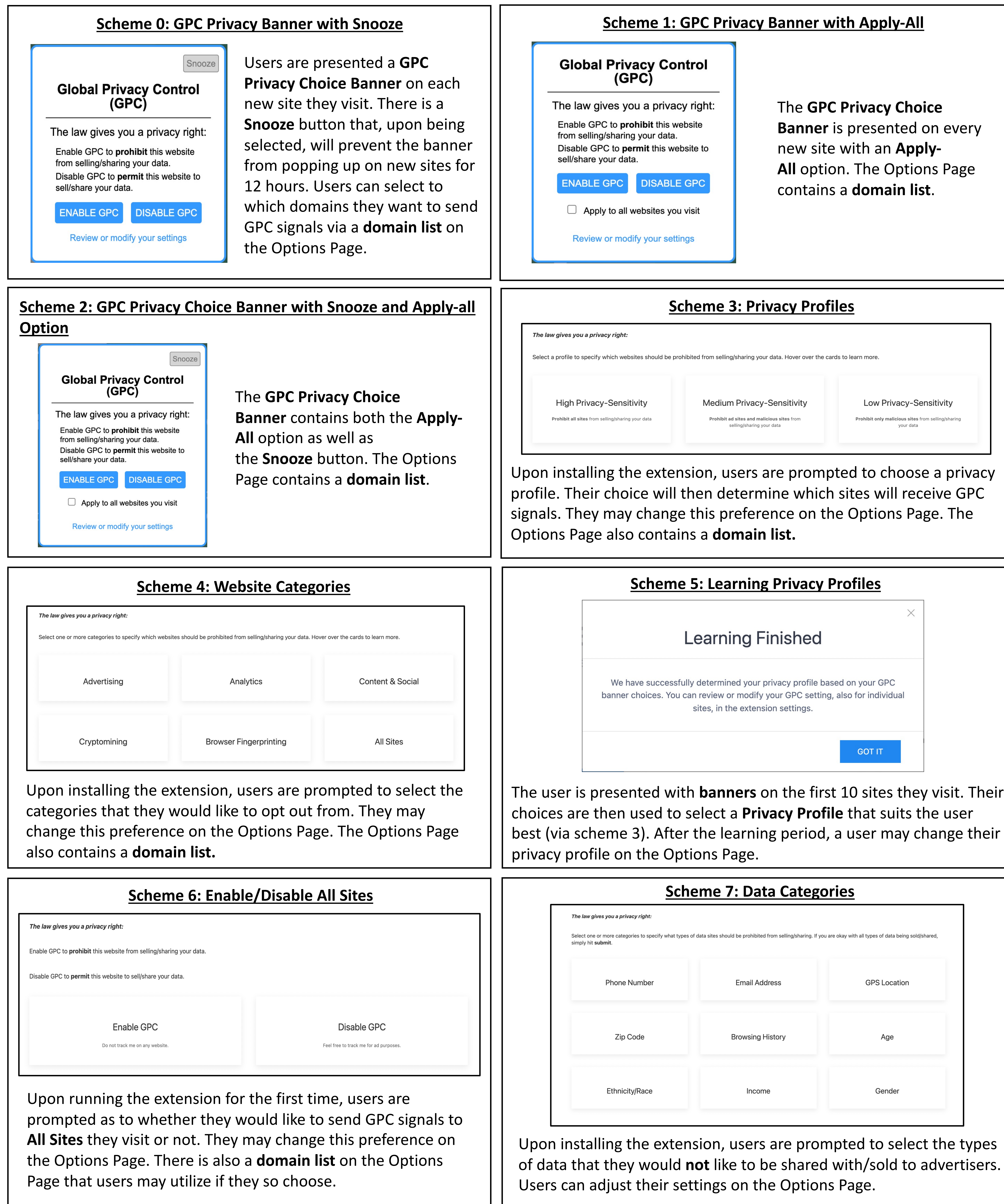48 responses

Figure 2

Note that scheme 2 is a banner scheme (that appears on all sites unless configured otherwise) and scheme 4 is a category scheme. Although users have the *same amount of personalization* available to them (via the domain list) in either scheme, according to Figures 1 and 2, there is a higher percentage of users reporting to have liked more personalization options in scheme 4 than in scheme 2.
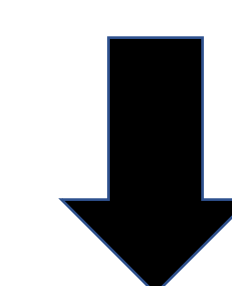
Moreover, Figure 3 shows that over half of scheme 4's users made a generalized 'All Sites' decision when they first installed the browser extension, indicating a preference for generalization; this presents a contradiction of sorts.
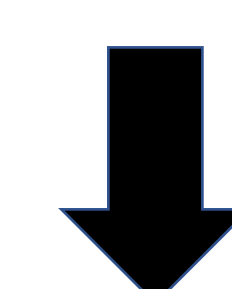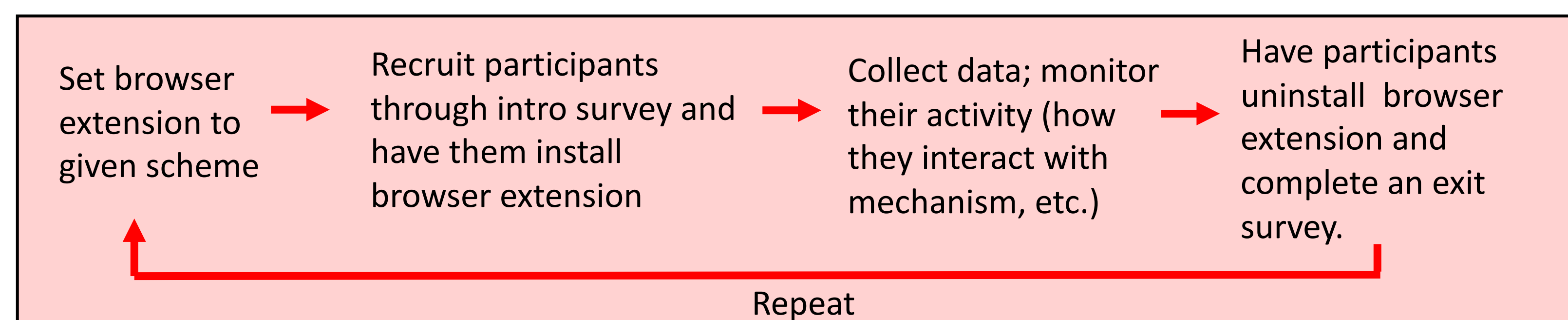
Privacy Choice Schemes

Scheme 0: GPC Privacy Banner with Snooze

Users are presented a **GPC Privacy Choice Banner** on each new site they visit. There is a **Snooze** button that, upon being selected, will prevent the banner from popping up on new sites for 12 hours. Users can select to which domains they want to send GPC signals via a **domain list** on the Options Page.

Scheme 1: GPC Privacy Banner with Apply-All

The **GPC Privacy Choice Banner** is presented on every new site with an **Apply-All** option. The Options Page contains a **domain list**.

Scheme 2: GPC Privacy Choice Banner with Snooze and Apply-all Option

The **GPC Privacy Choice Banner** contains both the **Apply-All** option as well as the **Snooze** button. The Options Page contains a **domain list**.

Scheme 3: Privacy Profiles

The law gives you a privacy right:
Select a profile to specify which websites should be prohibited from selling/sharing your data. Hover over the cards to learn more.

High Privacy-Sensitivity	Medium Privacy-Sensitivity	Low Privacy-Sensitivity
Prohibit all sites from selling/sharing your data	Prohibit ad sites and malicious sites from selling/sharing your data	Prohibit only malicious sites from selling/sharing your data

Upon installing the extension, users are prompted to choose a privacy profile. Their choice will then determine which sites will receive GPC signals. They may change this preference on the Options Page. The Options Page also contains a **domain list.**

Scheme 4: Website Categories

The law gives you a privacy right:
Select one or more categories to specify which websites should be prohibited from selling/sharing your data. Hover over the cards to learn more.

Advertising	Analytics	Content & Social
Cryptomining	Browser Fingerprinting	All Sites

Upon installing the extension, users are prompted to select the categories that they would like to opt out from. They may change this preference on the Options Page. The Options Page also contains a **domain list.**

Scheme 5: Learning Privacy Profiles

Learning Finished

We have successfully determined your privacy profile based on your GPC banner choices. You can review or modify your GPC setting, also for individual sites, in the extension settings.

GOT IT

The user is presented with **banners** on the first 10 sites they visit. Their choices are then used to select a **Privacy Profile** that suits the user best (via scheme 3). After the learning period, a user may change their privacy profile on the Options Page.

Scheme 6: Enable/Disable All Sites

The law gives you a privacy right:

Enable GPC to **prohibit** this website from selling/sharing your data.

Disable GPC to **permit** this website to sell/share your data.

Enable GPC	Disable GPC
Do not track me on any website.	Feel free to track me for ad purposes.

Upon running the extension for the first time, users are prompted as to whether they would like to send GPC signals to **All Sites** they visit or not. They may change this preference on the Options Page. There is also a **domain list** on the Options Page that users may utilize if they so choose.

Scheme 7: Data Categories

The law gives you a privacy right:
Select one or more categories to specify what types of data sites should be prohibited from selling/sharing. If you are okay with all types of data being sold/shared, simply hit **submit.**

Phone Number	Email Address	GPS Location
Zip Code	Browsing History	Age
Ethnicity/Race	Income	Gender

Upon installing the extension, users are prompted to select the types of data that they would **not** like to be shared with/sold to advertisers. Users can adjust their settings on the Options Page.

Percentage of Users that selected 'All Sites'
Scheme 4

FALSE 37.9%
TRUE 62.1%

Figure 3

Research Methodology

Development of Browser Extension

↓

Data Collection

Set browser extension to given scheme → Recruit participants through intro survey and have them install browser extension → Collect data; monitor their activity (how they interact with mechanism, etc.) → Have participants uninstall browser extension and complete an exit survey.

Repeat

↓

Data Analysis/Visualization