# Using Telemetry to Illuminate Policy Interactions: A Case Study with RequestPolicy

*Justin Samuel*

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2013-62
http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-62.html

May 15, 2013

Acknowledgement

I would like to thank my advisor, Vern Paxson, for his mentorship, guidance, and dedication.
I would also like to thank my readers, Bjoern Hartmann and Dawn Song, for their feedback
and assistance. I am grateful to the users of RequestPolicy for their patience and feedback
over the years as well as for their participation in our study. This work was supported by
an NSF fellowship.

**Using Telemetry to Illuminate Policy Interactions: A Case Study with RequestPolicy**

by

Justin Samuel

A thesis submitted in partial satisfaction of the
requirements for the degree of
Master of Science

in

Computer Science

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Vern Paxson, Chair
Professor Dawn Song
Professor Björn Hartmann

Spring 2013

The thesis of Justin Samuel, titled Using Telemetry to Illuminate Policy Interactions: A Case Study with RequestPolicy, is approved:

Chair _____ Date _____

_____ Date _____

_____ Date _____

University of California, Berkeley

**Using Telemetry to Illuminate Policy Interactions: A Case Study with RequestPolicy**

## Abstract

Using Telemetry to Illuminate Policy Interactions: A Case Study with RequestPolicy

by

Justin Samuel

Master of Science in Computer Science

University of California, Berkeley

Professor Vern Paxson, Chair

Modern websites perform many cross-site requests that can be detrimental to user privacy. Cross-site requests undermine privacy by allowing third-party websites—the websites that are the recipients of cross-site requests—to track a user's browsing behavior. As a result, some users turn to browser extensions that give them control over these requests. One such extension, RequestPolicy, implements a default-deny policy for cross-site requests and provides users an interface through which they manage a whitelist to allow blocked requests. This approach breaks many websites and requires frequent user interaction.

We set out to gain insight into how RequestPolicy is used. We study RequestPolicy's usage through an opt-in telemetry study. Over a period of 24 weeks, we collected data from more than 2,500 RequestPolicy users about how they interact with RequestPolicy. We use this data, user feedback, and our own experiences to guide a redesign of RequestPolicy.

# Contents

# List of Figures

# List of Tables

## Acknowledgments

I would like to thank my advisor, Vern Paxson, for his mentorship, guidance, and dedication. I would also like to thank my readers, Björn Hartmann and Dawn Song, for their feedback and assistance. I am grateful to the users of RequestPolicy for their patience and feedback over the years as well as for their participation in our study. This work was supported by an NSF fellowship.

# Chapter 1

# Introduction

In recent years, privacy in web browsing has moved from being a concern of a few technologists to being a mainstream issue. One important area of web privacy concern is that of information leakage and user tracking through cross-site requests. Cross-site requests occur when a page from one website instructs the browser to make requests to a different site. Third-party sites can correlate HTTP requests made by the same user through stateful information such as HTTP cookies as well as statelessly through browser fingerprinting [5, 17]. This ability to correlate requests allows third-party sites to track a user's behavior as they browse the web [16]. In the case of third-party sites that are nearly omnipresent on the web, the third-party site often has the ability to track a user's behavior across visits to unrelated sites [8]. The information learned by third-party sites can range from the specific pages a user visited to search queries revealing sensitive medical conditions [14]. User tracking is performed for a variety of purposes ranging from web analytics to behaviorally targeted advertising. In some cases, the organization doing the tracking has no stated policy on what they do with the information [22].

Providing practical privacy solutions for users is challenging. A 2007 study by Krishnamurthy et al. concluded that all methods of preserving privacy in the face of cross-site requests were inferior to blocking the requests outright [13]. However, that same study concluded that blocking all cross-site requests often had a very negative impact on page quality by breaking functionality or degrading the experience of using the site.

In 2008, we developed a browser extension, RequestPolicy, to provide users a reliable way

to block unwanted cross-site requests through a user-controlled whitelist. RequestPolicy uses a default-deny policy, blocking requests unless the user has created rules that allow the requests. This default-deny policy "breaks" many websites. For these websites, their appearance and functionality is severely impaired until the user instructs RequestPolicy to allow the necessary cross-site requests. As a result, RequestPolicy's potential user base is limited to people who are willing to sacrifice a significant amount of usability.

Despite more than four years of real-world usage, our understanding of how RequestPolicy users interact with the extension and manage their policies is limited to our own experiences and anecdotal evidence. We have no data about fundamental usage characteristics such as how frequently users interact with the extension, the number and types of rules in their whitelists, which preferences they change in the extension, how many users have additional privacy and security extensions installed, and how long it takes users to make whitelisting decisions.

Ultimately, we want RequestPolicy to be useful to people with all levels of privacy needs, from those who are willing to sacrifice usability to those who are not. In this work, we work toward this goal in two ways:

1. We use an opt-in telemetry study to learn about RequestPolicy users and how they interact with the extension. A core requirement of our study is to maintain user privacy by limiting the types of data we collect. The data we gather and analyze includes how often users open the RequestPolicy menu, which actions they perform through the menu, and the sizes and staleness of their whitelists. Our study shows varied usage patterns among RequestPolicy users and provides a strong motivation for us to perform further telemetry.

2. We redesign RequestPolicy with the intention of improving its usability. Our redesign includes a new user interface, a new rule system, and defaults optimized for non-advanced users. One important feature we add to enable ongoing improvements is subscription policies. Subscription policies are rule sets maintained by us that automatically update, allowing us to address website breakage and new privacy threats without requiring user interaction. We leave a usability study of the redesigned RequestPolicy to future work.

# Chapter 2

# Background

## 2.1 RequestPolicy

RequestPolicy is an extension for Firefox and other Mozilla browsers that implements a user-controlled cross-site request whitelist [23]. When a user who has RequestPolicy installed visits a web page, RequestPolicy uses Mozilla browser APIs to identify the origin and destination URLs of every request the web page initiates. For cross-site requests (requests where the origin and destination domains are different), RequestPolicy looks for a whitelist rule in the user's policy indicating that the request should be allowed. RequestPolicy is default-deny: if there is no rule allowing a request, the request is blocked. Users are informed when requests are blocked through a toolbar icon that turns red when a page has blocked requests. Users can see which specific third-party sites have been blocked or allowed as well as manage their whitelist through a menu accessible from the RequestPolicy toolbar icon.

The available types of whitelist rules are shown in Table 2.1. For any rule, the user can add the rule persistently so that it remains across browser sessions or temporarily so that it

| Whitelist Rule Type | Example |
|---|---|
| Origin | Allow requests from `foo.com` |
| Destination | Allow requests to `bar.com` |
| Origin-to-Destination | Allow requests from `foo.com` to `bar.com` |

Table 2.1: Available types of whitelist rules in RequestPolicy.

is forgotten after the current browser session ends (that is, when the browser is closed). All rules can be revoked by the user at any time.

The ability for RequestPolicy users to understand the concept of "cross-site requests" may be a fundamental obstacle to the usability of RequestPolicy. In this work, we do not focus on this important but open question. We assume the majority of users install RequestPolicy after they have developed privacy concerns. We believe a privacy-concerned user without a technical understanding of cross-site requests will interpret the blocking of cross-site requests as privacy-preserving and the allowing of cross-site requests as privacy-reducing.

The current version of RequestPolicy is version 0.5. Since its original release in 2008, development has focused primarily on fixing bugs and maintaining compatibility with Firefox as the browser and its APIs evolve.

## User Interface

### Initial Setup Window

When users install RequestPolicy, they are presented with a window that offers to import a set of predefined rules into their whitelist. There are a total of 107 available predefined rules divided across six geographic regions. These regions include an "international" region that is selected by default and currently contains 49 rules. These initial rules are categorized by region based on their origin or destination domains being specific to a geographic region. For example, the rule with the origin domain `yahoo.co.jp` is in the Asia region.

This initial setup window (Figure 2.1) informs the user that the suggested rules involve requests that are either requests between domains belonging to the same organization or requests that will reduce website breakage and have a low privacy impact. The list of predefined rules was initially generated by our own use of RequestPolicy with popular websites. Occasionally, rules suggested by users have been added.

### Menu

The RequestPolicy menu is the user's primary interface to RequestPolicy. The menu tells the user which destination domains the current page made requests to and whether requests

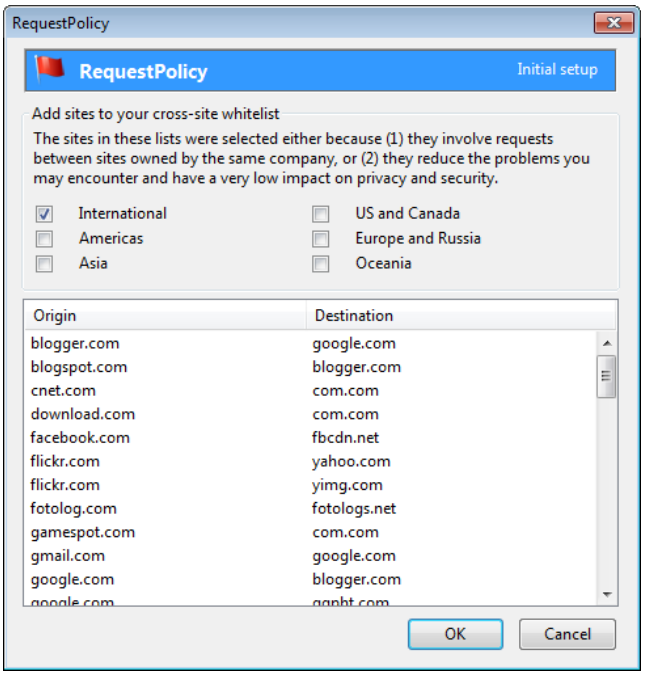



Figure 2.1: RequestPolicy 0.5 first-run window.

to each destination were allowed or blocked. The menu also gives users the ability to add and remove whitelist rules (Figure 2.2).

Arguably the most complex aspect of the menu is the management of rules related to *other origins*. In RequestPolicy terminology, an other origin exists when a framed cross-site web page initiate its own cross-site requests. Each other origin has its own submenu hierarchy similar to that of the main menu. To add or remove whitelist rules related to destinations of other origins, the user has to navigate submenus three levels deep from the main RequestPolicy menu (Figure 2.3).

### Preferences Window

Users can manage various settings, import and export their whitelist, and edit their whitelist through the RequestPolicy preferences window. Figure 2.4 shows the whitelist management interface available through the preferences window. The settings users can change include whether RequestPolicy should automatically reload the current page after rules are added or removed through the menu, whether RequestPolicy should show placeholders for blocked

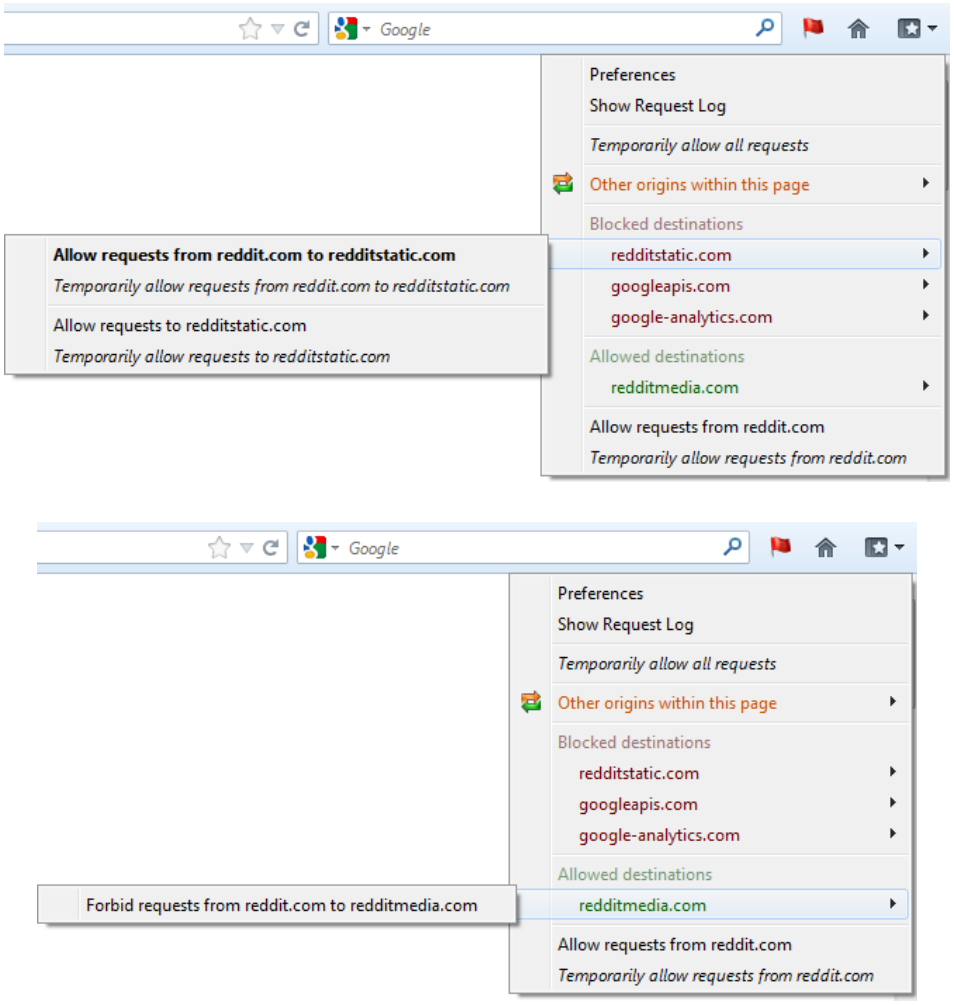



Figure 2.2: RequestPolicy 0.5 menu. (Top) Submenu for blocked destination. (Bottom) Submenu for allowed destination.

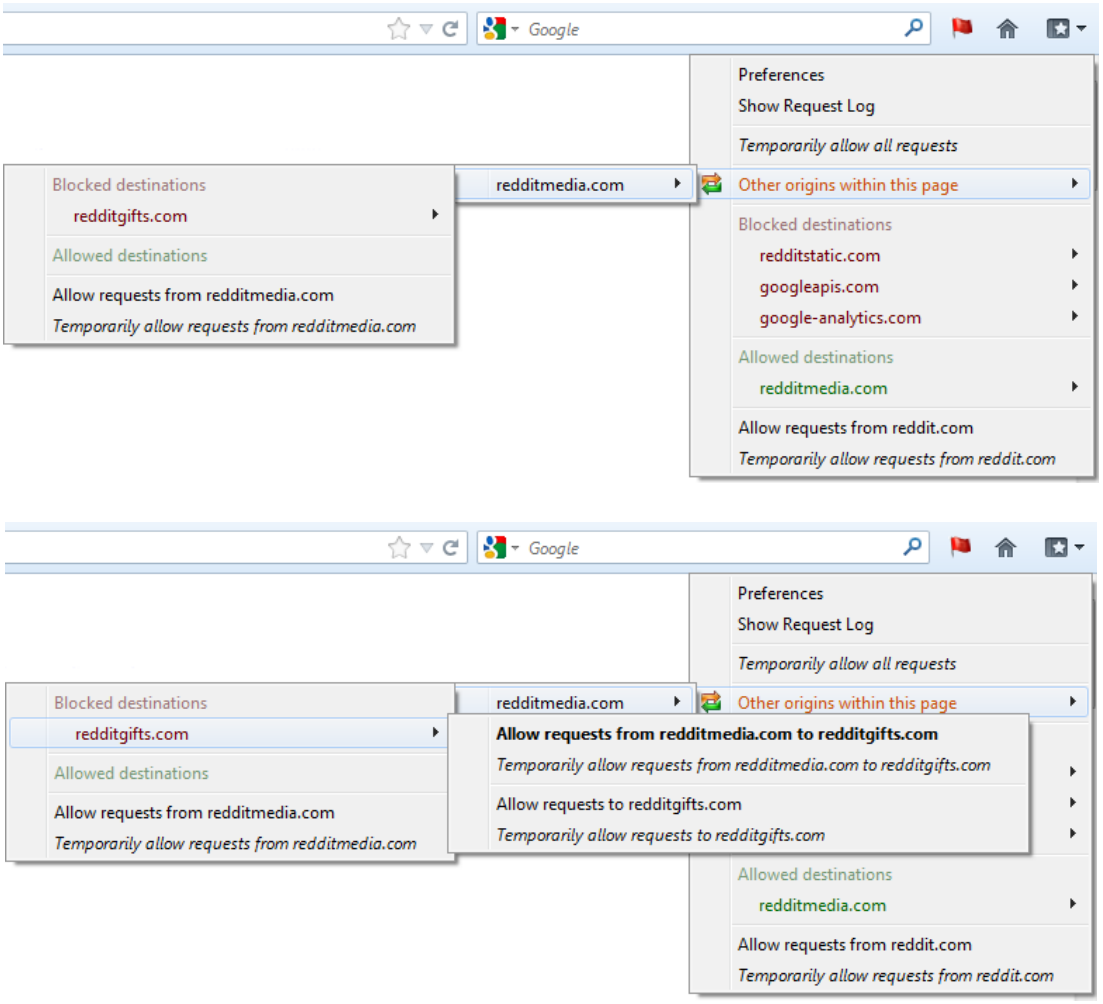



Figure 2.3: RequestPolicy 0.5 menu showing other origin. (Top) Submenu for other origin. (Bottom) Submenu for blocked destination of an other origin.

images, and how strict RequestPolicy should be when classifying requests as same-site or cross-site.

## Strictness Mode

The *strictness mode* is the approach RequestPolicy uses to classify URLs as either same-site or cross-site. Using RequestPolicy's default strictness mode, a request is only allowed if the

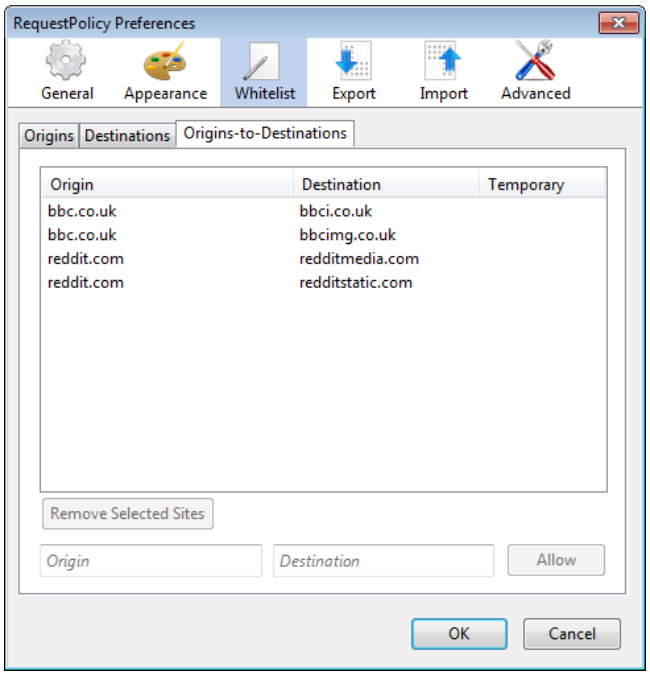



Figure 2.4: RequestPolicy 0.5 preferences window showing user policy management.

registered domain name of the origin is the same as that of the destination.[1] A registered domain is the portion of the domain name which an organization has control over through their domain's registrar (e.g. `example.com` or `example.co.uk`). Classifying URLs only by registered domain name is a simple but imperfect approach to cross-site request identification. For example, organizations may point DNS CNAME records for subdomains to hostnames that belong to other organizations for purposes of analytics and advertising [15].

In order to provide finer-grained control for advanced users, RequestPolicy offers stricter same-site classification modes that users can enable through the preferences window. In addition to the default of classifying URLs as same-site if their registered domain names match, the user can select *full hostname* strictness or *protocol + full hostname + port* strictness. When either of these stricter classification modes is enabled, the whitelist rules that the RequestPolicy menu offers to create include either the full hostname or the protocol, full hostname, and port.

[1] If the host specified in the URL is an IP address, the address is used instead of a domain name.

### Rule System

RequestPolicy internally represents whitelist rules as strings in the format "origin|destination" where either the origin or the destination is optional. For example, a rule for allowing all requests from `foo.com` in the default strictness mode would be represented as "`foo.com|`". Rules for non-default strictness modes contain the full hostname or the combination of the protocol, full hostname, and port. For example, a destination rule created when the user is in strictest classification mode might be "`|http://www.foo.com:81`". Whitelist rules are, for the most part, specific to a single strictness mode. The one exception to rule incompatibility is that a rule such as "`|foo.com`" will work in full hostname strictness mode for requests to the full hostname `foo.com`.

For persistence, the user's non-temporary rules are stored using the Firefox preference system. Thus, they are written to the profile's `prefs.js` file where all other user preferences are stored. At browser startup, these rules are read into a hash table and rule lookups are performed by key lookups in the hash table.

## 2.2 Related Work

Hilbert and Redmiles surveyed attempts to automate analysis of data collected from user interface events to identify usability issues [10]. Their focus is on inferring information from program behavior. They note that it is useful when a developer can instrument a program to explicitly report events of interest but such manual instrumentation increases the burden on application developers. Further, they note that relying on manual instrumentation may result in missing usability-related information that the developer has not explicitly reported.

The use of telemetry is well established in software engineering for tracking program resource usage, environment information, system settings, and user interactions. Telemetry is used by all of the major browsers [18, 7, 9]. Of the major browsers, only Internet Explorer enables telemetry by default [18].

Identifying usability problems in security and privacy software is an important area of research in order to increase the number of users who can benefit from the software. Norcie et al. studied points in the installation and use of the Tor Browser Bundle, an application

for anonymous web browsing, where users would stop using the software due to confusion or frustration [20]. Of their recommendations, most relevant to RequestPolicy may be the importance of setting realistic expectations for users. For RequestPolicy, this would mean ensuring users know that website breakage is normal and to be expected as well as ensuring users know how to identify when breakage is the result of blocked requests. Similarly, Clark et al. used cognitive walkthroughs to study the usability of multiple client applications that exist for the Tor anonymity network [4].

Besides RequestPolicy, there are other extensions that block cross-site requests. Adblock Plus [21] provides blacklist-based blocking of advertisements. By default, Adblock Plus does not indicate to users when it blocks requests. Ghostery [2] notifies users of cross-site requests that it believes are for user tracking. Ghostery notifies the user of potentially user-tracking requests through a small box it overlays at the top-right of the webpage. Ghostery does not block requests by default but instead gives the user options to block requests through a menu it adds to the browser. Both Adblock Plus and Ghostery use curated lists of URL patterns against which they check each request the browser intends to make. These lists are automatically updated by the extensions. Another blacklist-based extension, BlockSite [11], allows manual blacklisting of request destinations.

# Chapter 3

# Telemetry Study

To understand how the current version of RequestPolicy is used, we conducted an opt-in telemetry study of RequestPolicy users. We collected information about each participating user's whitelist rules, menu interactions, preferences, and other data that could help us understand RequestPolicy's usage and inform our redesign of the extension. As the study involved collecting potentially identifying data, we obtained IRB approval for the study. To assist other researchers, we've included our IRB application as Appendix A.

## 3.1 Design

Our telemetry system is designed around *events*. An event is a JSON object generated by RequestPolicy that it sends back to our data collection server. In addition to the event contents, each event contains enough information for us to know which events were sent by the same user, the order in which the events were generated, the time when each event was generated, how many browser sessions the user has had while participating in the study (that is, how many times the user has started and exited the browser), and which browser session each event was generated from.

## Event Categories

The following is the complete list of events we used in our study. In no cases are URLs or domain names included in the events.

### Whitelist Rules

These events uniquely identified and reported each of a user's whitelist rules as a salted hash of the rule's origin and destination components. Therefore, the rule "allow requests from `foo.com` to `example.com`" would be reported to us using a different identifier than the rule "allow requests from `foo.com`." The per-user, browser-generated salt ensured that the same rule reported by two different users would have a different identifier.

For each rule, we tracked the most recent hour that the rule was used to allow a request, each time the rule was created or deleted, whether the rule is one of the rules in the initial suggested whitelist, and what types of content the rule has allowed (e.g. "image", "stylesheet", etc.)

For persistent rules we stored this rule-related data and the salt in a file in the browser's profile directory so that information gathering could be continued across browser restarts.

### Addons of Interest

These events reported the name, version, install date, and status (enabled/disabled) of specific addons if they were installed. Reporting was only done at browser startup. Therefore, extensions that were installed but subsequently uninstalled before the browser was restarted were not reported.

The addons we reported were chosen for one of two reasons:

1. We were interested in the addon because it has known or potential conflicts with RequestPolicy. These addons were Web Developer, GreaseFire, Sage-Too, NewsFox, Brief, Xmarks Sync, Norton Toolbar, Update Scanner, SimilarWeb, and Dr. Web Link Checker.

2. We were interested in the addon because it is privacy or security related. These addons were Better Privacy, HTTPS Everywhere, NoScript, Ghostery, Adblock Plus, and Col-

lusion. Knowing which of these addons the user has installed gives us insight into the user's concerns and overall browsing experience.

### Browser Preferences

These events reported the values of specific browser preferences. The preferences whose values were reported indicate whether recording of browsing history is enabled, whether Do-Not-Track (DNT) is enabled, the user's locale, and whether the browser starts in private browsing mode (PBM).

### RequestPolicy Preferences

These events reported the values of the RequestPolicy preferences as well as when they changed.

### Browser Environment

These events reported the browser name (e.g. "Firefox"), browser version (e.g. "13.0.1"), and operating system name (e.g. "Linux", "WINNT", or "Darwin").

### Non-Standard Port Requested

These events reported whenever a document or resource was requested that used a non-standard port (e.g. port 8080 for HTTP instead of the standard port 80). We did not track the actual port number. We included a domain ID for the origin and destination domains. The IDs are sequential integers that started over on each browser session and did not correspond to the rule hashes we reported.

### Mixed HTTP/HTTPS Content Requested

These events reported whenever an HTTPS document included plain HTTP resources. We tracked the type of content that was included insecurely (e.g. an image, script, etc.) as well as origin and destination domain IDs as discussed above.

#### Preferences Window Actions

These events tracked the opening and closing of the RequestPolicy preferences window as well as the modification of rules and rule import/export actions performed through the preference window.

#### Origins-per-Destinations, Destinations-per-Origin

These events reported two separate lists of integer counts without any identifiers:

- The number of unique destination domains that each origin domain requested during the browser session.
- The number of unique origin domains that each destination domain requested during the browser session.

#### Document Loads and Menu Interactions

These events tracked the time and the current document's domain ID for each RequestPolicy menu interaction (open, close, or menu item selection) as well as for each top-level document load (a document loaded in a tab or window, not an iframe). Additionally, for menu open events, the event reported the number of allowed and blocked destinations that were visible in the menu.

## 3.2 Implementation

### Extension Changes

The only user-visible change in our instrumented version of RequestPolicy was the addition of a new item in the RequestPolicy menu. The new item read "Participate in research study" in blue text. When selected, a new tab opened showing a consent form. In order to participate in the study, the user had to click on an agreement button at the bottom of the consent form, as shown in Appendix A. Once the user was participating in the study, the "Participate in research study" menu item was replaced with a new menu item that

read "End participation in research study" in black text. Selecting the menu item to end participation sent any pending events to our server and deleted study-related data stored in the user's profile directory. The menu would then once again show the option to begin participating in the study.

Telemetry was implemented in RequestPolicy as an event queue to which other code in RequestPolicy could add events. Every ten minutes the items in the event queue, if any, were sent to our data collection server using SSL. For some of the data related to the user's non-temporary rules, the aggregated data was also stored in a file in the user's profile directory. This persistent data allowed us to track certain information—such as the last time a rule was used, added, or deleted—across browser sessions. Like the rule data sent to us, the rules stored in this file were salted and hashed. Unlike the rule data sent to us, the salt was also stored in this file. Altogether, the changes added approximately 1,500 lines of JavaScript in three new files and 450 lines of JavaScript in eight existing files.

Within the extension, we set December 31, 2012 as the end date for the study. After this date, the user's participation in the study was automatically terminated and the menu options related to the study were hidden.

### Data Collection Server

Our data collection server stored events in a MongoDB database and was implemented in approximately 100 lines of Python. This Python server sat behind an Nginx instance running on the same system which terminated SSL connections and proxied requests through to the Python server. Our data collection server did not log IP addresses.

## 3.3 Results

Our study ran from July 11, 2012 to December 31, 2012. In that time, 2,522 users[1] of RequestPolicy opted in to participation in the study.

[1]We will refer to each installation of RequestPolicy as a user. It is likely that some users have multiple browser profiles each with RequestPolicy installed and participating in our study. We have no way to know how many truly unique users there are in our study.

| Operating System | Users (%) |
|---|---|
| Windows | 69.0 |
| Linux | 23.2 |
| Mac | 7.5 |
| FreeBSD | 0.3 |
| NetBSD | 0.1 |

Table 3.1: Operating systems of study participants.

| Browser Name | Users (%) |
|---|---|
| Firefox | 93.8 |
| Iceweasel | 2.5 |
| Pale Moon | 1.1 |
| SeaMonkey | 1.0 |
| Abrowser | 0.8 |
| Firefox-Trunk | 0.4 |
| IceDragon | 0.4 |

Table 3.2: Browsers used by study participants.

One interesting trend among participating users is that they appear less likely to participate in the study if they already had RequestPolicy installed at the time we began the study. The study lasted 24 weeks and user participation is noticeably lower for users who had RequestPolicy installed for more than 24 weeks at the time of the study's end. Figure 3.1 shows the number of users participating in the study grouped by the number of weeks they had RequestPolicy installed as of the end of the study. A CDF of the same data is shown in Figure 3.2. One possible explanation for the greater participation of new users is that they considered the study to be a standard part of RequestPolicy, whereas existing users may have had more privacy concerns due to it being unusual. It is also possible that the rate of RequestPolicy installations increased around the time the study began.

The operating systems of users are shown in Table 3.1. Relative to the global operating system usage statistics of a popular website [26], RequestPolicy users participating in the study had significantly greater usage of Linux (23.2% vs. 5.0%) and less usage of Windows (69.0% vs. 83.8%).

RequestPolicy supports the Firefox and SeaMonkey web browsers. There are also a handful of lesser-known Firefox-based browsers that RequestPolicy is compatible with, as

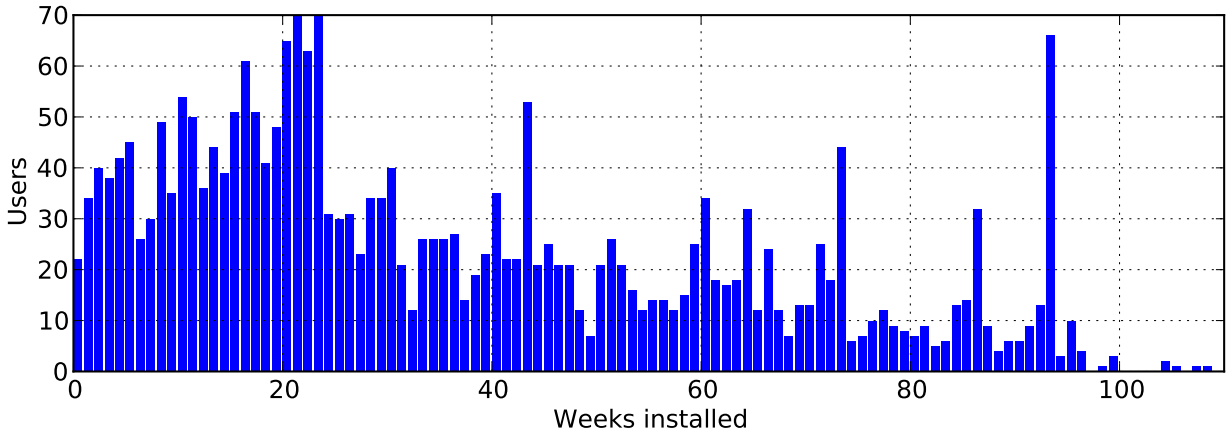



Figure 3.1: Histogram of length of time users had RequestPolicy installed as of the end of the study.

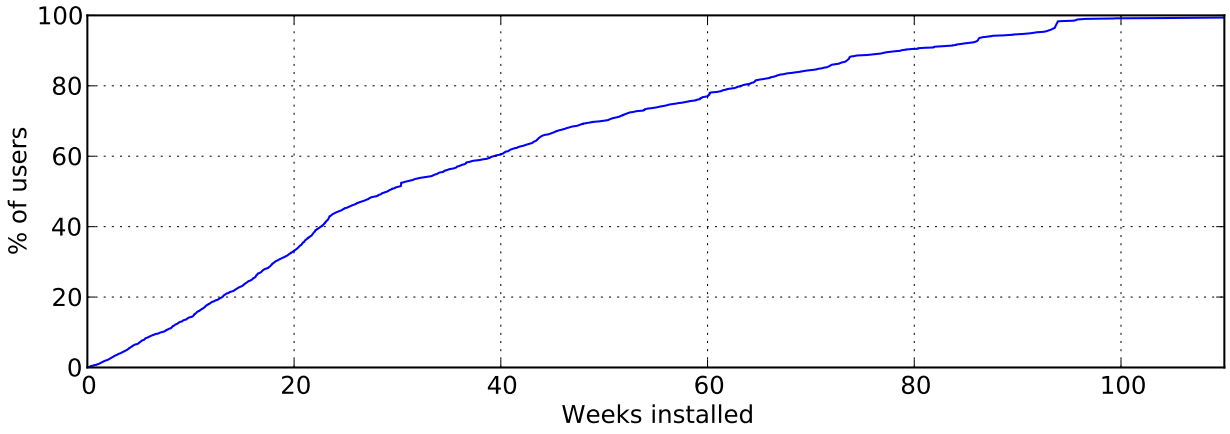



Figure 3.2: CDF of length of time users had RequestPolicy installed as of the end of the study.

| Locale | Users (%) | L10n |
|---|---|---|
| en (English) | 59.6 | ✓ |
| ru (Russian) | 12.5 | ✓ |
| de (German) | 10.6 | ✓ |
| ja (Japanese) | 5.2 | ✓ |
| es (Spanish) | 1.7 | ✓ |
| fr (French) | 1.6 | ✓ |
| zh (Chinese) | 1.3 | ✓ |
| pt (Portuguese) | 1.3 | ✓ |
| nl (Dutch) | 1.0 | ✓ |
| ar (Arabic) | 0.8 | |
| sk (Slovak) | 0.6 | ✓ |
| pl (Polish) | 0.5 | |
| it (Italian) | 0.4 | ✓ |
| cs (Czech) | 0.4 | |
| fa (Farsi) | 0.3 | |
| da (Danish) | 0.2 | |
| vi (Vietnamese) | 0.2 | |

| Locale | Users (%) | L10n |
|---|---|---|
| fi (Finnish) | 0.2 | |
| sv (Swedish) | 0.2 | ✓ |
| id (Indonesian) | 0.2 | |
| nb (Norwegian Bokmål) | 0.2 | |
| is (Icelandic) | 0.1 | |
| et (Estonian) | 0.1 | |
| tk (Turkish) | 0.1 | |
| tk (Thai) | 0.1 | |
| el (Greek) | 0.1 | |
| ca (Catalan) | 0.1 | |
| hu (Hungarian) | 0.1 | |
| lt (Lithuanian) | 0.0 | ✓ |
| ro (Romanian) | 0.0 | |
| bg (Bulgarian) | 0.0 | |
| sr (Serbian) | 0.0 | |
| sl (Slovenian) | 0.0 | |

Table 3.3: Locales of study participants and the localizations (L10n) available in RequestPolicy. Localizations are translations of RequestPolicy's user interface. When a localization is available for the user's locale, the RequestPolicy menu and preferences window show text in the user's language rather than in English.

can be seen in Table 3.2. The standard Firefox browser accounts for more than 93% of all RequestPolicy usage in our study.

The most common three locales of participating RequestPolicy users—English, Russian, and German—make up over 80% of users (Table 3.3). The rest of the study participants are spread across 30 additional locales.

## RequestPolicy Preferences

RequestPolicy has eight preferences users can configure from the preferences window. These preferences, their default values, and the percentage of users who changed each preference's default value are shown in Table 3.4. One of these preferences, the user's strictness level, has three possible values. As can be seen in Table 3.5, approximately 90% of installations kept the default and most liberal strictness policy of classifying requests as same-site if the registered domain name of the origin and destination were the same. More than two-thirds of users kept all preference values as the defaults (Table 3.6).

| Preference | Default value | Non-default (%) |
|---|---|---|
| Allow persistent whitelisting in PBM | False | 10.6 |
| Strictness | Reg. domain | 9.6 |
| Reload page after whitelist change | True | 8.5 |
| Show RequestPolicy menu in context menu | True | 6.5 |
| Start with "allow all" enabled | False | 6.3 |
| Disable DNS prefetching on startup | True | 4.6 |
| Indicate blocked images | True | 4.1 |
| Disable link prefetching on startup | True | 4.0 |

Table 3.4: RequestPolicy preference settings of study participants.

| Strictness Setting | Users (%) |
|---|---|
| Registered domain [default] | 90.4 |
| Hostname (i.e. full domain) | 4.9 |
| Protocol + hostname + port | 4.7 |

Table 3.5: RequestPolicy strictness settings of study participants.

By default, RequestPolicy reloads web pages after the user creates or removes a whitelist rule through the menu. More than 8% of users disabled automatic reloading of web pages.

The RequestPolicy menu normally only offers temporary whitelisting options when the user is in PBM or has history disabled.[2] RequestPolicy's default removal of persistent whitelisting options in PBM is to prevent these users who do not want browsing data stored across sessions from accidentally leaving records of their browsing in their RequestPolicy whitelist. Nearly 10% of users overrode this default and enabled the ability to create persistent whitelist rules through the menu while they are in PBM or have history disabled.

RequestPolicy adds a copy of its menu to the right-click context menu that is available on web pages. More than 6% of users disabled this addition to the context menu.

## Browser Preferences

In December 2012, Mozilla collected data on the browser privacy preference settings of Firefox users [3]. Table 3.7 shows how RequestPolicy users compare to the general Firefox

[2]PBM is a mode offered by the browser, not by RequestPolicy. Extensions must take into account whether the user is in PBM so that they do not violate the user's assumptions. For example, the user's browsing history should not be saved during PBM.

| Non-default Preferences | Users (%) |
|---|---|
| 0 | 67.5 |
| 1 | 19.3 |
| 2 | 7.9 |
| 3 | 2.9 |
| 4 | 1.5 |
| 5 | 0.6 |
| 6 | 0.1 |
| 7 | 0.1 |
| 8+ | 0.0 |

Table 3.6: Counts of non-default RequestPolicy preferences.

| Preference | Default value | RP users non-default (%) | Fx users non-default (%) |
|---|---|---|---|
| Do-Not-Track header | False | 41.4 | 11.3 |
| Clear data on shutdown | False | 23.0 | 2.8 |
| Keep history | True | 12.4 | 1.5 |
| Start in PBM | False | 9.9 | 5.0 |

Table 3.7: Browser preference settings for RequestPolicy (RP) users and the general Firefox (Fx) user population.

user population in terms of changing browser privacy preferences. For each of the preferences we studied, RequestPolicy users were 2 to 8 times as likely to change a browser preference in order to increase privacy.

More than 41% of study participants enabled the Do-Not-Track (DNT) header. If we assume that most RequestPolicy users would want to enable DNT, it seems likely that many users are either unaware of or have forgotten to change this browser preference. To change this preference, Firefox users have to open the browser preferences, go to the "Privacy" tab, and check the box for "Tell websites I do not want to be tracked."

Almost one quarter of study participants have their browser configured to delete data when the browser is shut down. The data that these users can have deleted on shut down includes browsing history, download history, cookies, and cache.

Approximately 12% of users have their browser history disabled. Almost 10% have configured their browser to start in PBM.

| Addons | Users (%) |
|---|---|
| 0 | 15.7 |
| 1 | 18.8 |
| 2 | 20.9 |
| 3 | 21.3 |
| 4 | 15.9 |
| 5 | 6.7 |
| 6 | 0.6 |

Table 3.8: Count per user of other privacy and security addons installed alongside RequestPolicy (includes only addons our study tracked).

| Addon | Users (%) |
|---|---|
| Adblock Plus | 65.8 |
| NoScript | 58.5 |
| BetterPrivacy | 34.3 |
| Ghostery | 33.0 |
| HTTPS-Everywhere | 26.3 |
| Collusion | 7.5 |

Table 3.9: Frequency of other privacy and security addons installed alongside RequestPolicy (includes only addons our study tracked).

## Addons

More than 84% of study participants had at least one other privacy or security addon installed (Table 3.8). As there are many privacy and security addons we did not track, the percentage of users with other privacy/security addons may be even higher. More than half of study participants used Adblock Plus or NoScript (Table 3.9), the two most popular privacy/security addons for Firefox [19].

## Rules

Approximately 80% of users have 400 rules or less in their whitelist (Figure 3.3). Origin-to-destination rules are much more common than either origin rules or destination rules (Figure 3.4). The corner in the origin-to-destination rules plot in Figure 3.4 is likely due to the 49 suggested whitelist rules that are selected by default in the initial setup window (Section 2.1).

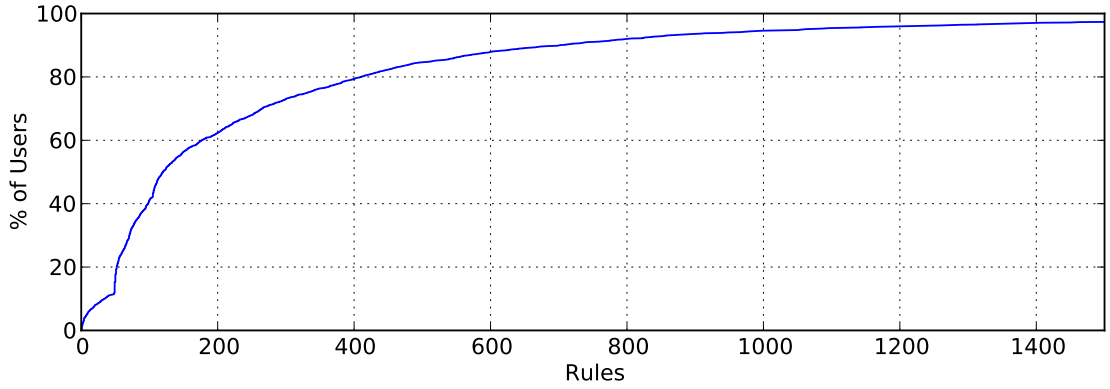



Figure 3.3: Users' total number of whitelist rules.

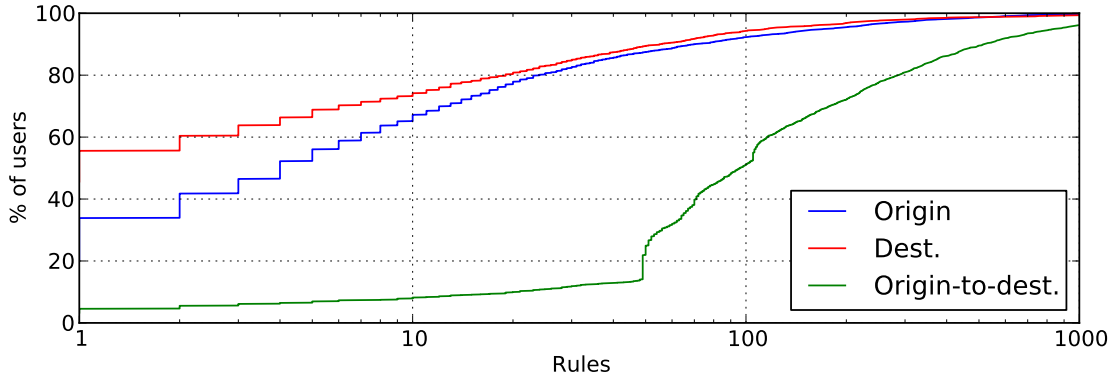



Figure 3.4: Users' number of whitelist rules by rule type.

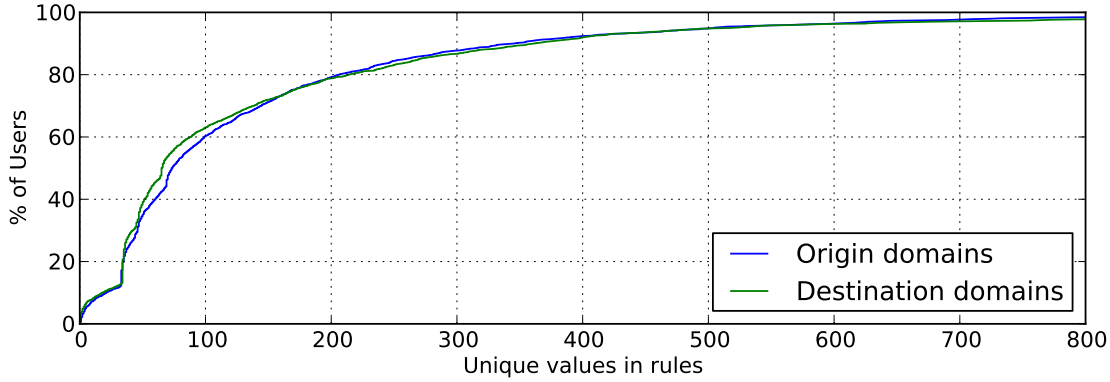



Figure 3.5: CDF of unique domains in user whitelists.

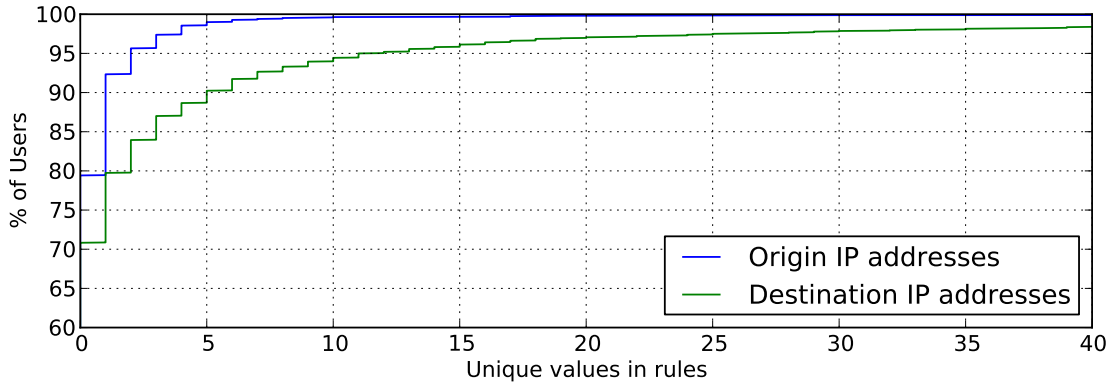



Figure 3.6: CDF of unique IP addresses in user whitelists.

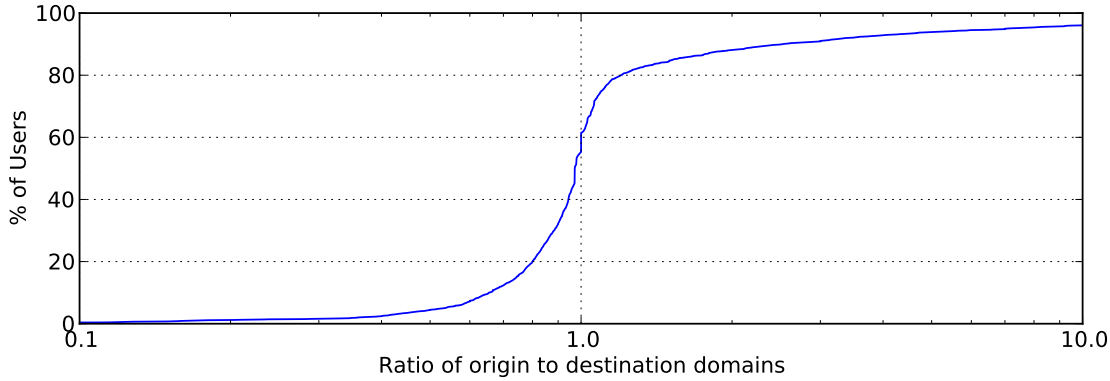



Figure 3.7: Ratios of unique origin and destination domains in user whitelists.

According to Figure 3.5, the number of unique origin domains in user whitelists is quite similar to the number of unique destination domains. (Unique IP addresses are shown in Figure 3.6). However, the per-user ratios of unique origin domains to unique destination domains in user whitelists (Figure 3.7) shows that the similarity of unique origin and destination domains in Figure 3.5 is due to considering the entire study population as a whole.

As with Figure 3.4, the corner in the plot of Figure 3.5 is likely due to the 49 suggested whitelist rules that are selected by default in the initial setup window. The users who choose not to import any of the suggested whitelist rules start with a completely empty whitelist. It may also be the case that some users import the suggested whitelist rules and then remove

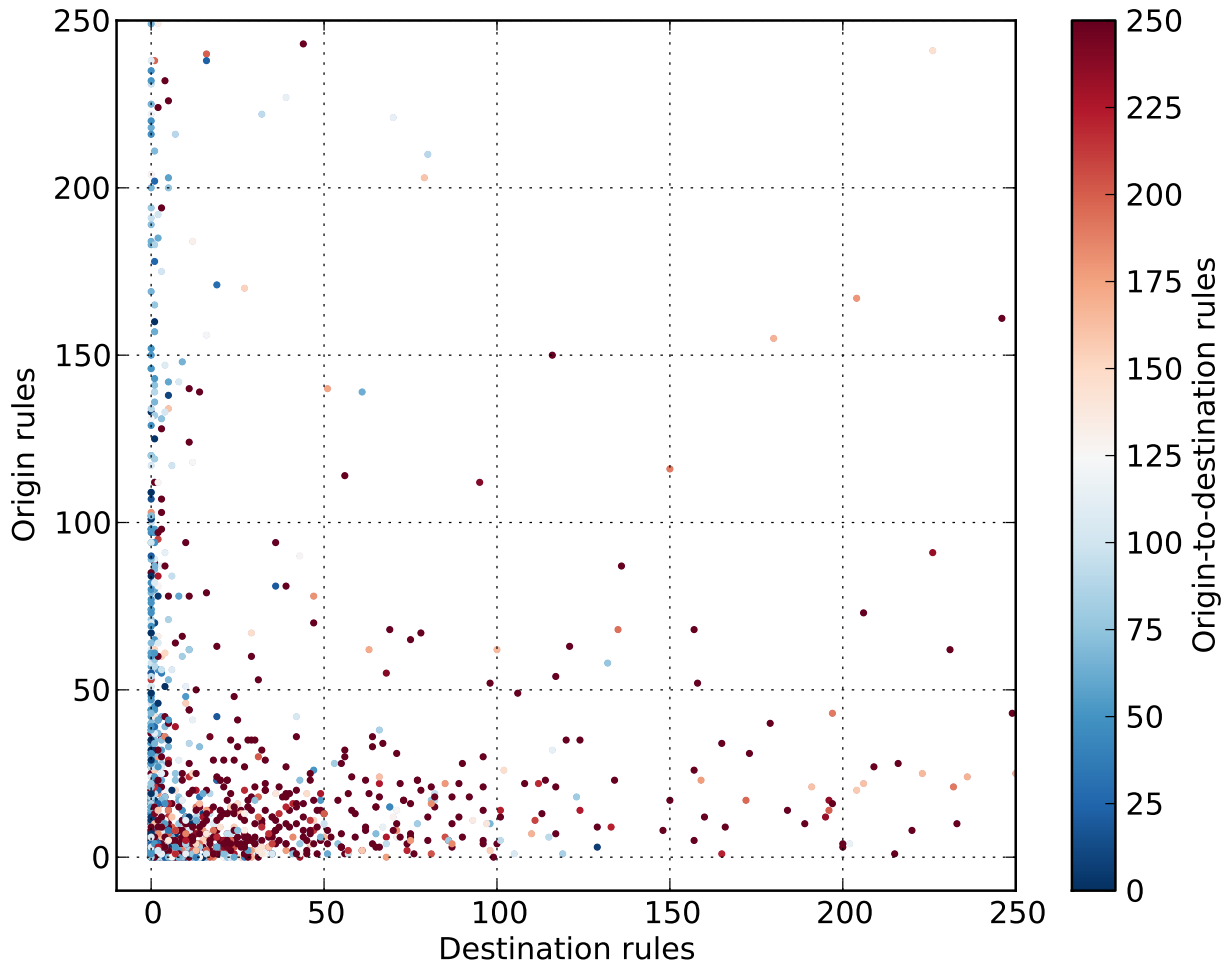



Figure 3.8: Scatter plot of user rule counts.

some of these rules without adding additional rules.

In an attempt to illuminate rule creation patterns among users, Figure 3.8 plots individual users' numbers of origin rules, destination rules, and origin-to-destination rules. Figure 3.8 hints that there may be interesting ways to classify users by the number of each type of rule they have created. However, further analysis would be needed to draw conclusions. We believe it may be interesting to consider additional information when looking for patterns of rule creation among users. For example, there may be differences in rule creation for users when considering their operating system, locale, RequestPolicy preferences, and browser preferences. Additionally, it would be interesting to study whether the types of

rules individual users create changes over time.

Figure 3.9 shows the rate at which users added whitelist rules based on the number of weeks since they installed RequestPolicy. Similarly, Figure 3.10 shows users' rule counts by time since installation. In our earlier work, we noted that feedback indicated the first two weeks of use required the heaviest whitelisting [23]. Figure 3.9 does indicate users perform heavier whitelisting during their first few weeks of use. Despite the linear regression we have plotted in Figure 3.10, the rate of change of rule counts is unlikely to be linear because the rate of rule creation shown in Figure 3.9 appears to decrease linearly. That is, if the rate of rule creation decreases, total rule counts should not increase linearly. We show Figure 3.10 only through week 40 due to limited data.

When a rule is used, that rule has been responsible for allowing a request. Figure 3.11 shows how recently rules had been used based on their age. For rules that were 20 days old, approximately 20% of them had not been used within the preceding seven days. For rules that were 120 days old, approximately 30% of them had not been used within the preceding thirty days.

We also looked at the types of content that were allowed by rules. For rules that were used during the study, Table 3.10 shows the percentage of rules that allowed specific types of content. We see that three-quarters of rules allowed images, half of rules allowed scripts, and one-third of rules allowed stylesheets. Relatedly, Table 3.11 shows the number of different types of content that used rules allowed. Almost half of rules were used to allow a single type of content.

## Menu Interaction

As our telemetry tracked each top-level document load as well as which top-level document a user was on when they interacted with the menu, we can determine the percentage of top-level documents on which the user interacted with the menu.[3] A top-level document is a document loaded in a tab or window, not an iframe. Top-level document loads occur when a user enters an address in their address bar, clicks a link, or is redirected to another top-level

[3]We remind the reader that user privacy was paramount to our study. How we collected data about loaded top-level documents was discussed in Section 3.1.

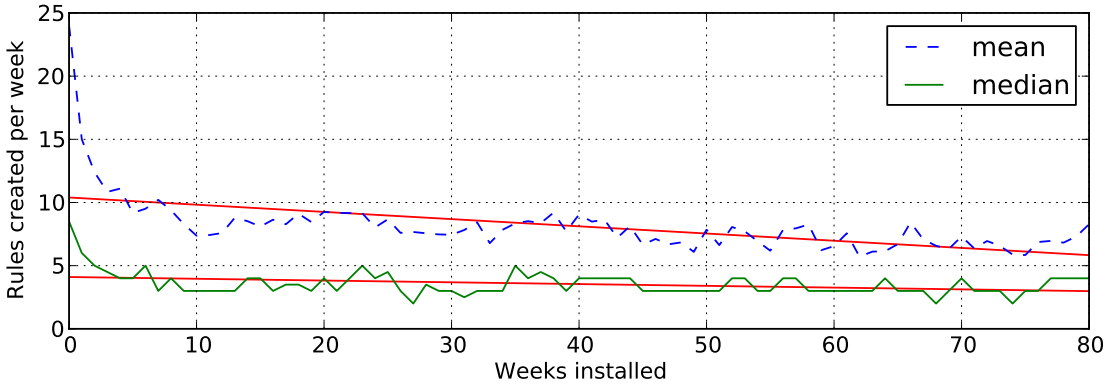



Figure 3.9: Rate of rule creation by how long RequestPolicy has been installed.

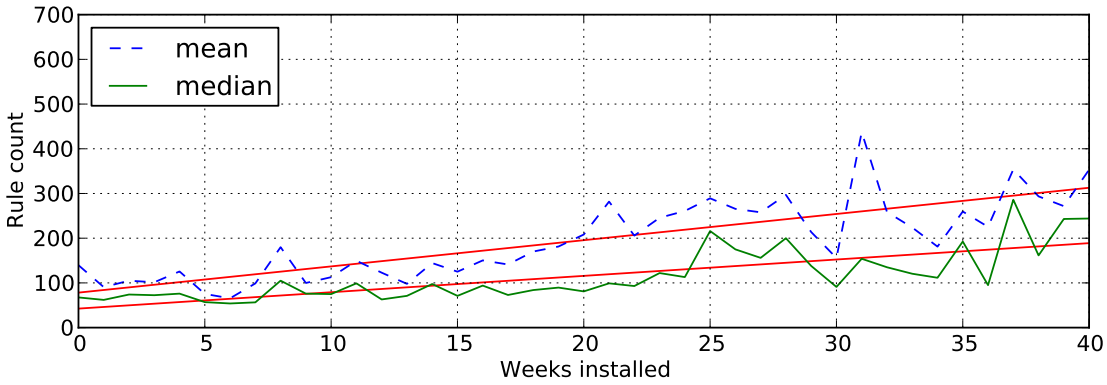



Figure 3.10: Whitelist rule counts by how long RequestPolicy has been installed.

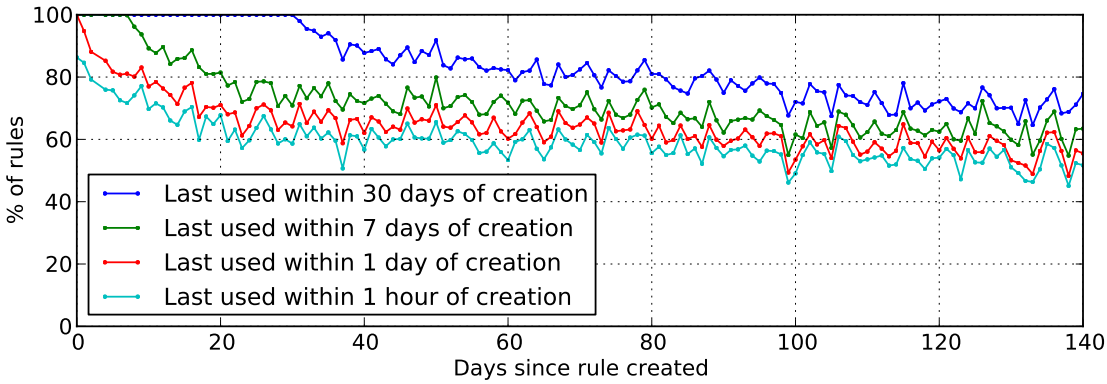



Figure 3.11: Rule staleness by age of rules.

| Content types allowed | Rules (%) |
|---|---|
| Image | 74.0 |
| Script | 53.3 |
| Stylesheet | 34.5 |
| Subdocument | 20.0 |
| Object | 11.3 |
| Object Subrequest | 10.5 |
| Document | 9.5 |
| Font | 4.7 |
| XMLHttpRequest | 1.9 |
| Media | 0.8 |
| Websocket | 0.2 |

Table 3.10: Content types allowed by used rules.

| Number of content types allowed | Rules (%) |
|---|---|
| 1 | 45.4 |
| 2 | 19.0 |
| 3 | 17.7 |
| 4 | 9.7 |
| 5 | 5.0 |
| 6 | 2.0 |
| 7 | 0.8 |
| 8 | 0.3 |
| 9 | 0.1 |

Table 3.11: Number of content types allowed by used rules.

document by JavaScript running in a page they are visiting.

Figure 3.12 shows the percentage of top-level documents visited by each user where the user opened the RequestPolicy menu. Approximately half of users opened the RequestPolicy menu on less than 2% of the documents they viewed. Approximately 90% of users opened the RequestPolicy menu on less than 10% of the documents they viewed.

When users open the menu, the number of allowed and blocked destinations shown in the menu varies. We call the total number of destinations shown in the menu the menu's *complexity*. Figure 3.13 shows a CDF of the complexity of the menu when it was opened.

Figure 3.14 shows the amount of time the menu remained open relative to the complexity of the menu. We see a very clear increase in the time required for the user to close the menu or make a menu selection as the complexity of the menu increases. For menus showing a

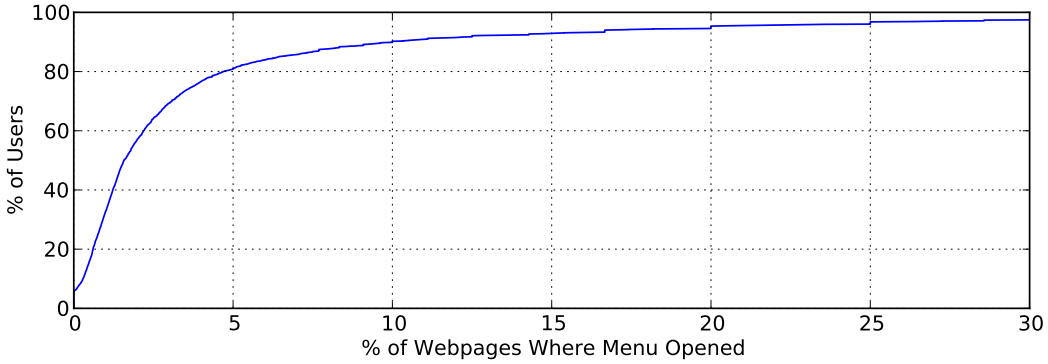



Figure 3.12: Percentage of top-level documents on which users opened the RequestPolicy menu.

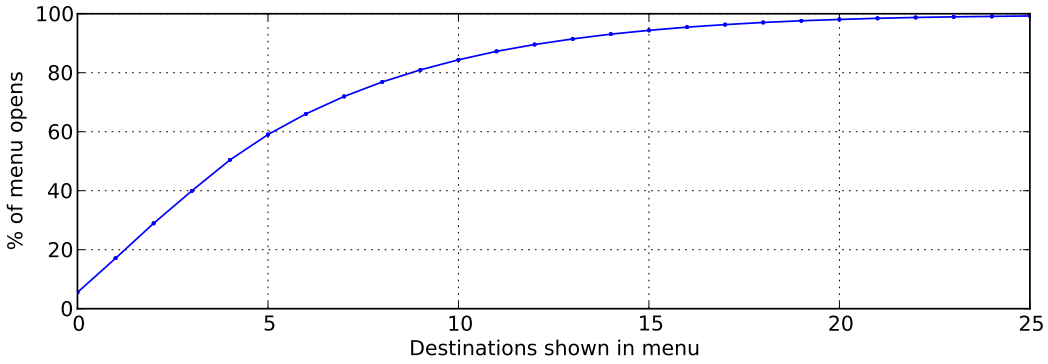



Figure 3.13: CDF of menu complexity seen by users.

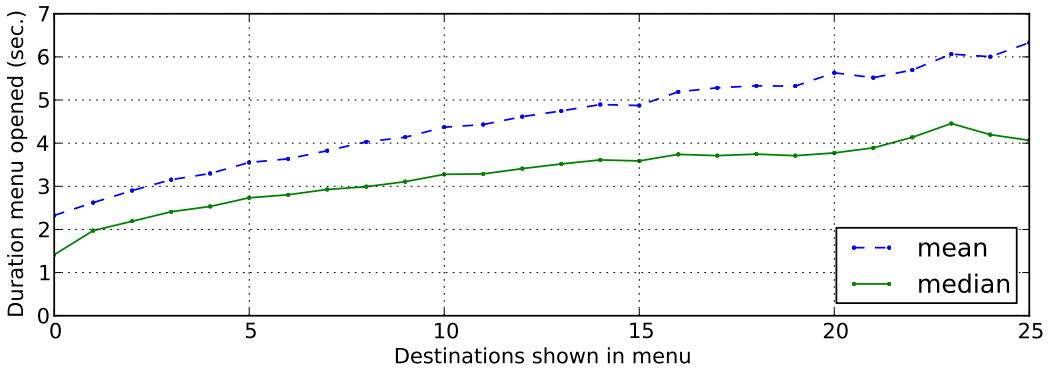



Figure 3.14: Duration menu remained open relative to menu complexity.

| Menu selection | % |
|---|---|
| Menu closed without selection | 36.0 |
| Allow origin to dest. | 20.1 |
| Temp. allow origin to dest. | 18.1 |
| Temp. allow origin | 10.0 |
| Allow origin | 3.7 |
| Temp. allow all enabled | 3.3 |
| Allow dest. | 3.2 |
| Temp. allow dest. | 1.2 |
| Temp. allow all disabled | 0.9 |
| Forbid origin to dest. | 0.9 |
| Revoke temp. permissions | 0.8 |
| Preferences opened | 0.6 |
| Request log opened | 0.4 |
| Request log closed | 0.3 |
| Forbid origin | 0.3 |
| Forbid dest. | 0.1 |

Table 3.12: Frequency of options selected from the RequestPolicy menu.

single destination, the median time required to make a decision was two seconds. For menus showing ten destinations, the median time required to make a decision was more than three seconds. Taking into account both Figure 3.13 and Figure 3.14, about 75% of menu opens had a median time-to-decision of less than three seconds.

Table 3.12 shows the relative frequencies of menu option selections. When users open the RequestPolicy menu, more than one-third of the time they close the menu without selecting any items from the menu. There are various reasons a user may close the menu without making a selection, though we do not know the relative frequencies of these or if there are reasons we are unaware of. For example, a user may open the menu only out of curiosity as to which destination domains the web page makes requests to and which were blocked and allowed. If the user has additional browser extensions that block requests, they may look at which requests are blocked by each extension before making decisions about what action to perform. Users may also close the menu because they are unable to decide what action to perform.

Approximately 38% of the time users open the menu, they choose to create either persistent or temporary origin-to-destination rules. About 14% of menu selections were to create persistent or temporary origin rules. Almost 5% of the time, users create persistent or

| Content Type | Users (%) |
|---|---|
| Any | 90.2 |
| Image | 87.1 |
| Subdocument | 68.2 |
| Script | 67.9 |
| Object Subrequest | 58.2 |
| Stylesheet | 56.5 |
| Object | 38.9 |
| Media | 29.1 |
| XMLHttpRequest | 27.9 |
| Font | 22.6 |

Table 3.13: Users who encountered mixed content requests (HTTPS to HTTP).

temporary destination rules.

## Mixed Content

Plain HTTP resources requested from HTTPS pages are often referred to as mixed content. Table 3.13 shows that 90% of users encountered mixed content during the study. The risk posed by mixed content depends on the situation, though scripts (JavaScript files) and objects are generally the most dangerous forms of mixed content.[4] In our study, about 68% of users encountered HTTPS pages that requested scripts as mixed content.

Mozilla has recently implemented optional blocking of mixed content in Firefox 18, released in January 2013. Mozilla will enable blocking of mixed content by default in Firefox 23, to be released in August 2013.

## Non-Standard Ports

As shown in Table 3.14, 77% of users in our study encountered requests for content on non-standard ports. One-third of users encountered requests for top-level documents on non-standard ports. Normally, the only time a user would be aware of non-standard ports is when viewing a top-level document retrieved over a non-standard port as the port would be

[4]In Firefox, stylesheets can use XBL bindings to execute scripts when the stylesheets are obtained from the same origin as the document. XBL is a markup language used by Firefox for declaring the behavior of user interface widgets.

| Content Type | Users (%) |
|---|---|
| Any | 77.2 |
| Image | 57.9 |
| Script | 47.6 |
| Object Subrequest | 37.5 |
| Document | 33.3 |
| Subdocument | 24.5 |
| XMLHttpRequest | 22.5 |
| Stylesheet | 22.0 |
| Object | 12.2 |
| Media | 2.3 |
| Font | 1.3 |

Table 3.14: Users who encountered non-standard ports for HTTP(S) requests.

visible in the URL shown in the address bar. Only the small fraction of study participants who use the strictest cross-site classification mode would have blocked requests to resources on non-standard ports from web pages on standard ports or different non-standard ports.

It is possible that RequestPolicy users encounter non-standard ports more frequently than the general population due to an increased proportion of web developers and similar users among RequestPolicy users. In particular, web developers may run services on non-standard ports for development purposes.

# Chapter 4

# Usability Issues

To inform our redesign of RequestPolicy, we identify various usability issues we should consider and usability problems we should strive to correct. In addition to telemetry data, we look at user feedback, public discussion on blogs for privacy software projects [24, 25], and our own observations as both users and developers.

## 4.1 Barriers to Usage

### Strictness and Impact on Browsing

One of the most commonly mentioned problems seen in public discussions about RequestPolicy is that its strictness makes it too difficult to use. When a RequestPolicy user first visits a site, the site will often appear as a plain document with no images as shown in Figure 4.1. Figure 4.2 shows the same site after the user has allowed cross-site requests that are required for the site's appearance and functionality. The impact of RequestPolicy's strictness on usability has been given as a reason to not include RequestPolicy with privacy-focused browsers such as the Tor Browser Bundle (TBB) and Tails [24, 25].

The root of this problem is RequestPolicy's fundamental design decision to enforce a default-deny policy on cross-site requests. There is no option in RequestPolicy for a default-allow mode. For a default-allow mode to be useful, RequestPolicy would need to support a user-defined blacklist. Additionally, as these two default policies appeal to very different

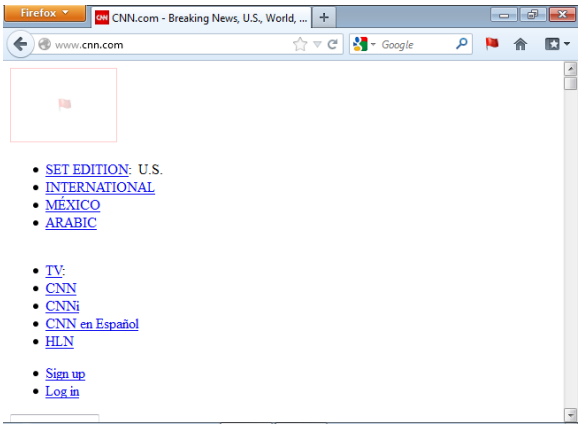



Figure 4.1: Example of a "broken" site due to blocked cross-site requests.

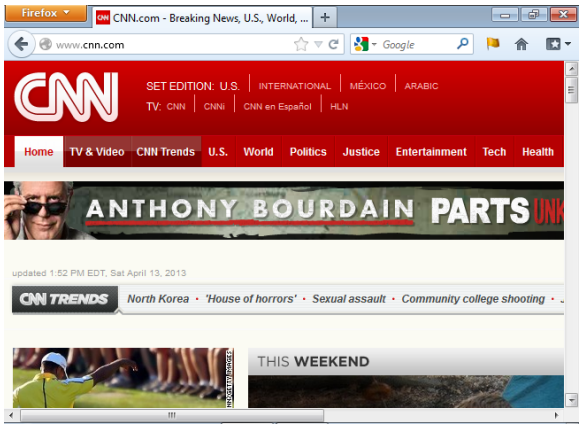



Figure 4.2: Example of a fully functional site with cross-site requests allowed.

types of users, many other design decisions would need to take into account the greater variety of users and use cases.

## Difficulty Correcting Broken Sites

When a RequestPolicy user encounters a site whose functionality or appearance is severely impaired, the cause is likely blocked requests. Users seeking fine-grained control over requests will often proceed to begin allowing requests to the page's destinations via the RequestPolicy menu. Based on our own experience as users as well as user feedback, identifying which destination or combination of destinations must be allowed in order to return functionality to the website can be difficult. In many cases, the domain names of destinations are not useful in making these decisions and the only option is trial and error: progressively allowing requests to the page's destinations until the site's functionality returns.

At a high level, there are two primary ways to alleviate this problem. First, RequestPolicy could do a better job of allowing cross-site requests that are critical to a website. The suggested initial whitelist attempts to mitigate this problem but is extremely inadequate and a different solution such as subscription policies may be appropriate. That is, rather than having the user import a set of rules into their own policy, RequestPolicy could include separate policies maintained by us or third parties that update automatically. This would be similar to the subscriptions used by Adblock Plus. Second, RequestPolicy could provide the

user more detailed information about what was blocked, the context of the blocked request, and potentially make suggestions for what requests the user should allow to enable a site to work again.

Aside from decreasing the need to whitelist or making whitelisting decisions easier, we can also make the process of creating multiple whitelist rules less frustrating. One of the most frequent feature requests we receive is to allow the selection of multiple menu options before the menu closes and the page refreshes. This may be one of the factors contributing to nearly 10% of users disabling automatic page reloading after whitelist changes (Section 3.3).

## 4.2 Limitations of Usage

RequestPolicy's most significant limitations relate to its simplistic rule system and completely manual approach to rule management. We will discuss how we address these limitations in Section 5.

### Whitelist-only

Even with only a default-deny policy, RequestPolicy suffers from the lack of a blacklist: rules that specify requests that should be blocked rather than allowed. For example, a user may want to allow all requests from an origin `example.com` except for requests to the destination `foo.com`. With a more advanced rule system, this could be accomplished in default-deny mode with one allow rule and one deny rule.

For a rule system that included both allow rules and deny rules, an important decision to be made is how powerful and complex to make the rule interactions. A very powerful approach would be to order rules and base rule priority on rule order. This is similar to how many firewalls implement rule priorities. However, an order-based approach to rule priority may be unnecessarily complex for the majority of RequestPolicy's users and could significantly complicate the menu.

### Users Repeating Whitelisting Work

The initial whitelist import offered by RequestPolicy 0.5 serves a worthwhile goal: to reduce the need for individual RequestPolicy users to manually create the same whitelist rules. However, the one-time import approach suffers from multiple problems. A one-time import means that additions to the initial whitelist will never be made available to existing users. Similarly, a one-time import means that any rule which later may need to be removed cannot be removed from the policies of users who have already imported the initial whitelist. Notably, this situation has happened with the RequestPolicy initial whitelist after Google bought Recaptcha. We believed many of our users would not want to allow requests from any site they visit to a Google-owned website. Therefore, we removed the "allow requests to `recaptcha.net`" rule from RequestPolicy's initial whitelist. A possible solution to this problem is the use of subscription policies.

### Fine-Grained Rules Require Strict Default

As discussed in Section 2.1, rules created for one strictness mode are not compatible with other strictness modes. Thus, it is not possible to use fine-grained rules such as those containing subdomains when using the default mode of cross-site request classification which considers only registered domain names. Similarly, course-grained rules are not available when using very strict classification modes.

This lack of rule compatibility across strictness modes limits the amount of control one has in the default strictness mode and makes RequestPolicy usage more difficult in the stricter classification modes. The lack of compatibility also makes switching strictness modes burdensome because the user essentially starts over with an empty policy.

### Limited Rule Expressibility

Aside from problems of rule compatibility across strictness levels, the RequestPolicy rule system can only express very simple rules and is difficult to extend to support new features because of the way rules are stored and used. The most frequently requested feature for the RequestPolicy rule system is support for subdomain wildcards. Having rules with subdomain

wildcards would allow a user to create a single rule that allows requests to all subdomains of `foo.com` while still being able to create a rule that only allows requests to `bar.com`, not its subdomains. The two other major feature requests for the rule system are the ability to specify URL paths and rules that restrict the type of content (e.g. stylesheet, image, etc.).

## 4.3 User Interface

The RequestPolicy user interface has remained the same since its launch in 2008. Here we discuss what we believe are inherent problems in the UI. These problems were identified by our own experience with RequestPolicy as well as through user feedback.

### Initial Setup Window

The initial setup window that opens after RequestPolicy is installed prompts users to add a set of pre-defined rules to their whitelist (Figure 2.1). The problems with the initial setup window include:

- The user is being asked to "[a]dd sites to [their] cross-site whitelist" with no explanation of what a cross-site request is and what it means to add sites to their whitelist.
- The user is shown the list of items to be imported despite the fact that non-advanced users are unlikely to find this useful for making an initial import decision.
- The user is shown checkboxes for importing whitelist entries specific to geographic regions. Selecting regions is an unnecessary decision users are forced to make as we do not believe any of these rules have a negative impact on privacy. Further, selecting any of these boxes does not make clear which additional items will be imported.

### Menu

Our use of hierarchical menus has resulted in menus up to four levels deep: there are up to three levels of menus off of the main menu (recall the other origins menus of Figure 2.3). Usability research on depth/breadth trade-offs in menu design indicates that menu breadth should be increased to avoid menus more than two or three levels in depth [12].

RequestPolicy's use of Firefox's traditional application menu system has limited our flexibility of what we can display in the menu and how we can display it. For example, despite the infrequency with which users open the preferences window or the request log from the menu (Table 3.12), both of these menu items are equally as prominent as rule-related menu items.

A major oversight in the menu that is not related to the menu system itself is the lack of a "help" option. For a new user who has just installed RequestPolicy, there is no way to obtain more information about RequestPolicy. There are similarly no menu entries a user might think could ultimately lead them to more information (e.g. "About RequestPolicy") in the absence of a "help" option.

The most common user feedback we have received regarding the menu has been the inability to make multiple whitelist changes through the menu before the menu closes and the current page is automatically reloaded.

## Preferences

The RequestPolicy preferences open as a separate window which attempts to maintain the look and feel of the web browser itself. We are increasingly uncertain of the benefit to users of opening a separate window for preferences and attempting to maintain look-and-feel consistency. Instead, using browser tabs with HTML pages for preferences management provides a powerful and flexible alternative to native windows. Google's Chrome browser was one of the first browsers to use browser tabs populated with HTML for its settings windows.

# Chapter 5

# Redesign

To address the most pressing usability issues discussed in Chapter 4, we undertook a major redesign of RequestPolicy. The primary design changes involved a new rule system, support for blacklists and a default-allow mode, default settings optimized for non-advanced users, and a new user interface.

Throughout the redesign, we have kept in mind the maintainability costs of additional complexity [1]. An important factor in minimizing complexity is to consider the requirements of features that may be implemented in the future without burdening the design with unnecessary generality. In Chapter 6, we discuss the extent to which we have future-proofed our redesign and how we may use this flexibility in the future.

## 5.1 Policies and Rule System

The primitive rule system used by RequestPolicy 0.5 met the very simple requirements of that version. For RequestPolicy 1.0, we needed a rule system to support the following functionality.

- **Default-allow mode.** A default-allow mode should be available for users who want to allow all requests except for those they've created rules to block.
- **"Deny" rules.** Users should be able to create "deny" rules in addition to "allow" rules. This is necessary for a default-allow mode and is a requested feature for the default-deny mode.

```
{
  "o": {
    "h": "*.foo.com"
  },
  "d": {
    "s": "https",
    "h": "www.bar.com",
    "port": 1000
  }
}
```

Figure 5.1: JSON representation of a RequestPolicy 1.0 rule allowing requests from `*.foo.com` to `https://www.bar.com:1000`.

- **Flexible rules.** Rules should support specifying any combination of hostname, scheme (protocol), and/or port for the origin and/or destination. Rule hostnames should support subdomain wildcards.
- **Extensible policy storage format.** The storage format for policies and their rules should allow for future additions (e.g. rules specifying the URL path).
- **Strictness-agnostic rules.** Rules should continue to work when a user changes settings related to RequestPolicy's strictness.
- **Support for subscription policies.** Users should be able to subscribe to automatically updating rule sets that are curated by us or third parties.

## Rule Format and Policy Storage

As discussed in Section 2.1, RequestPolicy 0.5 represented rules as simple strings (e.g. "`foo.com|bar.com`" for an origin-to-destination rule). In order to support richer rules in version 1.0, we have represented rules as objects with origin and destination attributes where the origin and destination values are themselves objects that can have a protocol, host, and port. An example rule is shown in Figure 5.1. Rule hostnames can include subdomain wildcards using the `*` character.

As version 1.0 rules are conveniently represented as JSON, policies (that is, collections of rules) can be represented as JSON objects that contains separate lists of "allow" rules

and "deny" rules. We represent the user's non-temporary policy using this format with some additional metadata such as the policy format version. We store the user's policy in a separate file in the user's profile data directory. The choice to store the data independently of the Firefox preference system and its `prefs.js` file was made for a few reasons. First, functionality such as backup and restore of the user's policy is simplified. Second, we can take more precautions in writing the policy file to disk than Firefox does in writing the `prefs.js` file to disk (e.g. performing atomic writes by writing to a temporary location, reading back and verifying the written contents, and then renaming the temporary file). Third, we can use the same code and storage format for distributing and storing subscriptions policies.

## Rule Lookup

To efficiently support subdomain wildcards, we leverage the fact that domain names are hierarchical. For each policy, we build a prefix tree of the policy where each node corresponds to a dot-separated label of a hostname. At each node in the prefix tree, there is a possibly empty list of rules. Thus, if the policy has a rule for "`example.com`", the policy's prefix tree will have a top-level node "`com`" with a list of rules. That node "`com`" will have a child node "`example`" with a separate list of rules. We also build for each policy a hash table of rule IP addresses.

Each rule entry in a node's list of rules specifies whether it is an allow or deny rule, whether the rule represents an origin or destination, and any non-hostname rule criteria (e.g. protocol and port). To represent origin-to-destination rules, each rule entry is also the root of a possibly empty prefix tree representing destination hostnames. Subdomain wildcards are represented with a `*` character as the label in leaf nodes in a prefix tree.

Rule lookups are performed by splitting a request's origin and destination URLs into their components (scheme, host, and port) and further splitting hostnames into labels. For both the origin and destination URL, the policy's prefix tree is traversed starting from the top-level domain to find an exact match or wildcard match. If a matching node in the prefix tree is found, each rule in the node's list of rules is compared against the other components of the URL. For origin-to-destination rules, we first find a matching origin rule and then search that rule's destinations prefix tree for a matching destination rule.

For simplicity, we chose not to use rule ordering for priority. Instead, when the user is in default-allow mode, allow rules have precedence over deny rules. When the user is in default-deny mode, deny rules have precedence over allow rules.

## 5.2 Subscriptions

Subscription policies for RequestPolicy 1.0 are a mechanism by which policies can be maintained by us or the community and updates to these policies can be received automatically by users. Many subscriptions will involve personal judgment as to what should be included in the subscription. For now, all subscriptions are curated and maintained by us.

We have implemented multiple, optional subscription policies in RequestPolicy 1.0. Our implementation makes different policies available based on whether the user is in default-allow or default-deny mode. The user's policy always takes precedence over subscription policies. Thus, overriding a subscription policy rule is done by creating a user policy rule that does the opposite (e.g. allow instead of deny) of what the subscription policy rule does.

In default-allow mode, a single subscription policy is currently available. This subscription blocks destinations we believe to be likely causes of privacy loss. This subscription policy includes rules to block requests to advertisers such as DoubleClick as well as commonly embedded sites such as Facebook. In the case of a site like Facebook where the site uses multiple domains to serve content used by third parties as well as by the site itself when visited directly, a combination of allow and deny rules are needed. Table 5.1 shows the rules currently used in this subscription to block requests to Facebook domains except when visiting Facebook directly.

In default-deny mode, there are three subscription policies available that include allow rules to minimize website breakage. These are 1) a policy that allows destinations that belong to the same organization as the origin webpage, 2) a policy that allows requests that are needed for websites to function correctly even if the request may have privacy impact, and 3) a policy that allows requests for embedded content such as images from `flickr.com` and videos from `youtube.com`.

Additionally, in default-deny mode there are two subscription policies available that min-

| Rule Type | Origin | Destination |
|---|---|---|
| Allow | *.facebook.com | *.facebook.com |
| Allow | *.facebook.com | *.facebook.net |
| Allow | *.facebook.com | *.fbcdn.net |
| Allow | *.fbcdn.net | *.facebook.com |
| Deny | | *.facebook.com |
| Deny | | *.facebook.net |
| Deny | | *.fbcdn.net |

Table 5.1: Subscription rules used to block requests to Facebook except when visiting the Facebook website.

imize blocking browser-related requests.[1] The first of these policies allows requests to Mozilla websites which are performed as unprivileged content requests through special locations such as `about:addons`. The second of these policies allows requests that other extensions perform as unprivileged content requests. Traditionally, when browser-related requests have been blocked by RequestPolicy, a new version of RequestPolicy would be released that includes hard-coded rules to allow these requests. This has resulted in both a delay in getting these workarounds to users as well as a slow iteration time when the rules added to work around these issues were not correct the first time. By alternatively or additionally including these rules in subscription policies, users can obtain these updates much faster than waiting for a new version of RequestPolicy to be released.

Currently, these policies are maintained solely by us. We discuss ideas for community-maintained subscriptions in Chapter 6.

## 5.3 Default Settings

A primary goal for RequestPolicy 1.0 is to be usable by a wider range of people. As blocking requests by default results in frequent and significant website breakage, RequestPolicy 1.0 defaults to allowing requests. Users can switch to default-deny through the RequestPolicy preferences.

[1] Privileged requests such as those performed to obtain browser updates are never blocked by RequestPolicy.

## 5.4 User Interface

The main elements of the RequestPolicy UI are the menu through which users view the current tab's destinations and do the majority of their rule management, the preferences window where settings are managed and the user's entire rule set can be viewed and edited, and the window users see after they have installed RequestPolicy for the first time. In our redesign, we have made significant changes to each of these. Our goal has been to simplify the user experience despite the addition of new functionality.

### Initial Setup Window

The redesigned RequestPolicy has increased the number of configuration options, adding default-allow vs. default-deny and optional subscriptions. As these options cater to very different types of users, RequestPolicy has a new problem to solve: when and how does a user configure RequestPolicy?

As we have decided that our default settings will be optimized for non-advanced users while allowing advanced users the ability to increase their control as desired, we take the same approach with our redesigned first-run window. When a user installs RequestPolicy 1.0, they are shown a very simple window (Figure 5.2, top) that encourages the user to proceed directly to a tutorial. Available in this window is a de-emphasized link for configuring RequestPolicy which takes the user to a configuration page (Figure 5.2, bottom).

### Menu

Given the limitations of traditional menu systems, for RequestPolicy 1.0 we have opted to create a flat menu of our own design (Figure 5.3). Though flat, the user has access to "deeper" functionality through selections that alter the menu state. Options not related to the currently active browser tab are de-emphasized with a smaller font and placed at the bottom of the menu.

When the user opens the menu, the upper left corner of the menu lists the origin domain of the current page. The rest of the left side of the menu optionally lists the following, if needed: the additional origin domains within the page, the blocked destinations domains from the

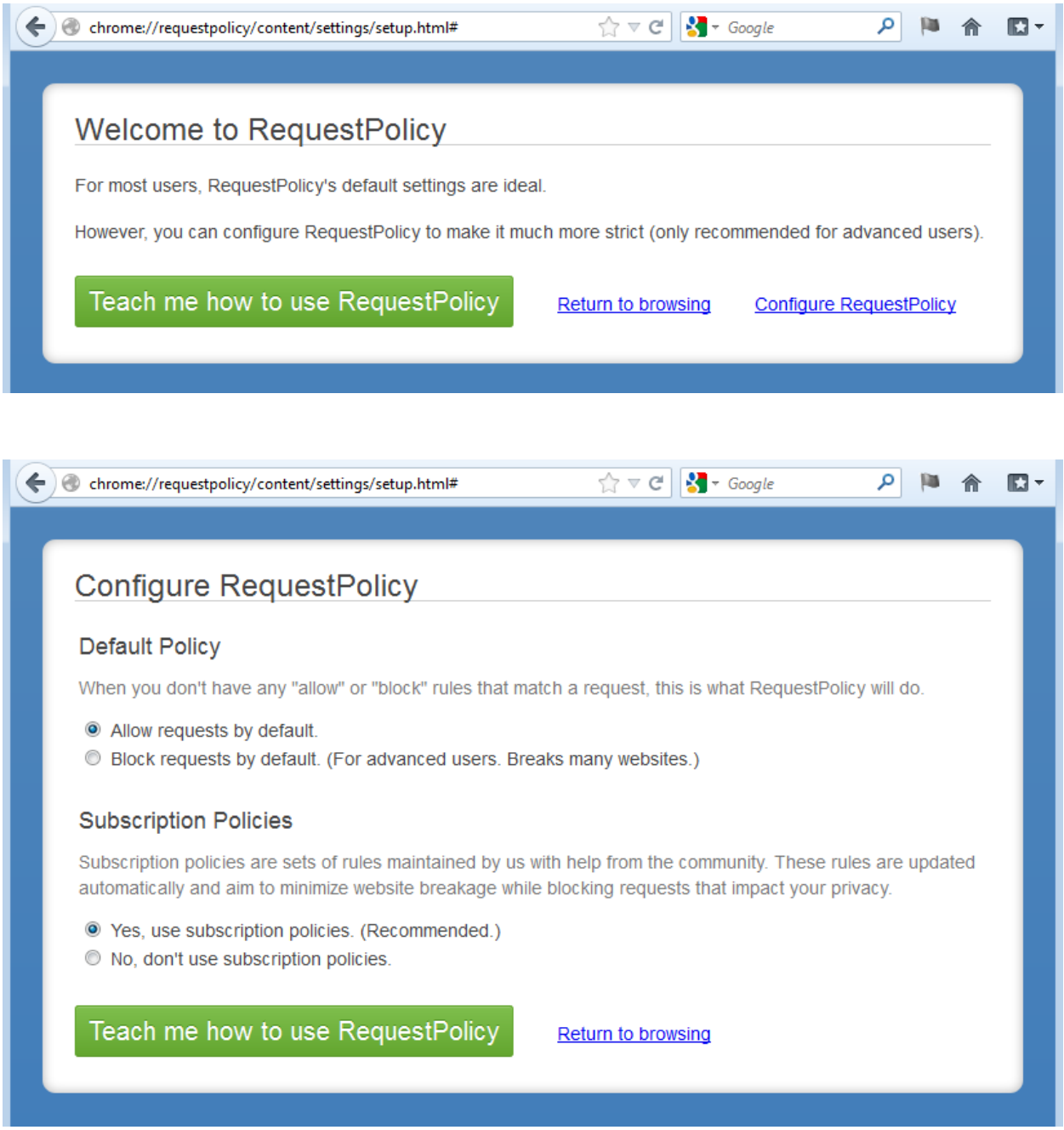



Figure 5.2: RequestPolicy 1.0 initial setup window. (Top) Welcome page. (Bottom) Configuration page.

current origin, the allowed destination domains from the current origin, and destination domains from the current page that have both blocked and allowed requests. If the user has enabled default-deny mode, the right side of the menu will provide options to allow all requests from the current origin.

When the user selects a destination, they are shown destination-specific policy options. These options vary depending on whether the user is in default-allow or default-deny mode. In default-allow mode, destinations are only blocked because a rule caused requests to be blocked. In this case, the menu offers to stop blocking the requests (Figure 5.3, middle). That is, the specific rule that caused requests to be blocked will be removed if it is a rule in the user's policy or overridden if it is a rule in a subscription policy. If relevant, the menu will also offer to allow requests from the origin to the destination (creating a separate allow rule unrelated to the rule that caused the requests to be blocked). In default-deny mode, the options for a blocked destination will simply be to allow requests to the blocked destination (an allow rule will be created). For allowed destinations, similar relevant options are shown based on the user's default policy and any existing rules that have caused requests to be blocked or allowed (Figure 5.3, bottom).

When the menu offers to "stop blocking requests" (remove or override a deny rule) or "stop allowing requests" (remove or override an allow rule), it displays a readable representation of the rule. RequestPolicy 1.0 rules are flexible but ultimately they follow a simple pattern that lends itself well to internationalization: "stop allowing/blocking requests [from *origin*] [to *destination*]". The menu constructs the string to display for the origin and destination values of a rule by combining the parts of the rule that are defined. A rule that specifies the origin with a protocol of "http" and a hostname of "*.foo.com" will have the origin represented as "http://*.foo.com".

When the site has other origins, the user can perform policy management related to an other origin by first selecting the other origin they are interested in. Once selected, the list of destinations on the left side of the menu changes to show only the destinations from that origin (Figure 5.4). From there, the user can select a destination to see destination-specific policy options as they would for the primary origin of the page.

Note that when the user is in default-allow mode, allow rules take precedence over deny rules. This ordering of rule processing based on the default policy is intentionally not com-

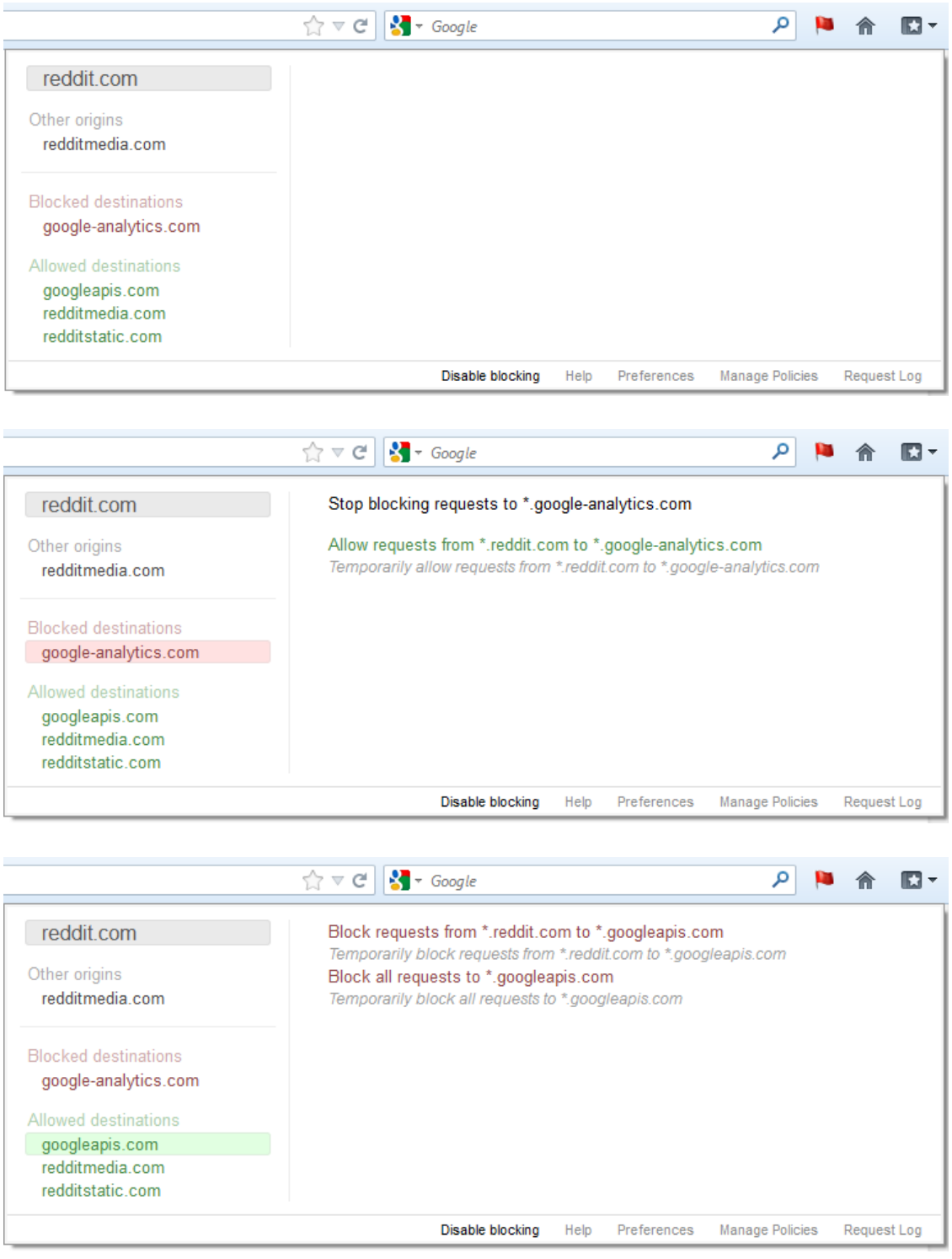



Figure 5.3: RequestPolicy 1.0 menu. (Top) Opened. (Middle) Allowed destination selected. (Bottom) Blocked destination selected.

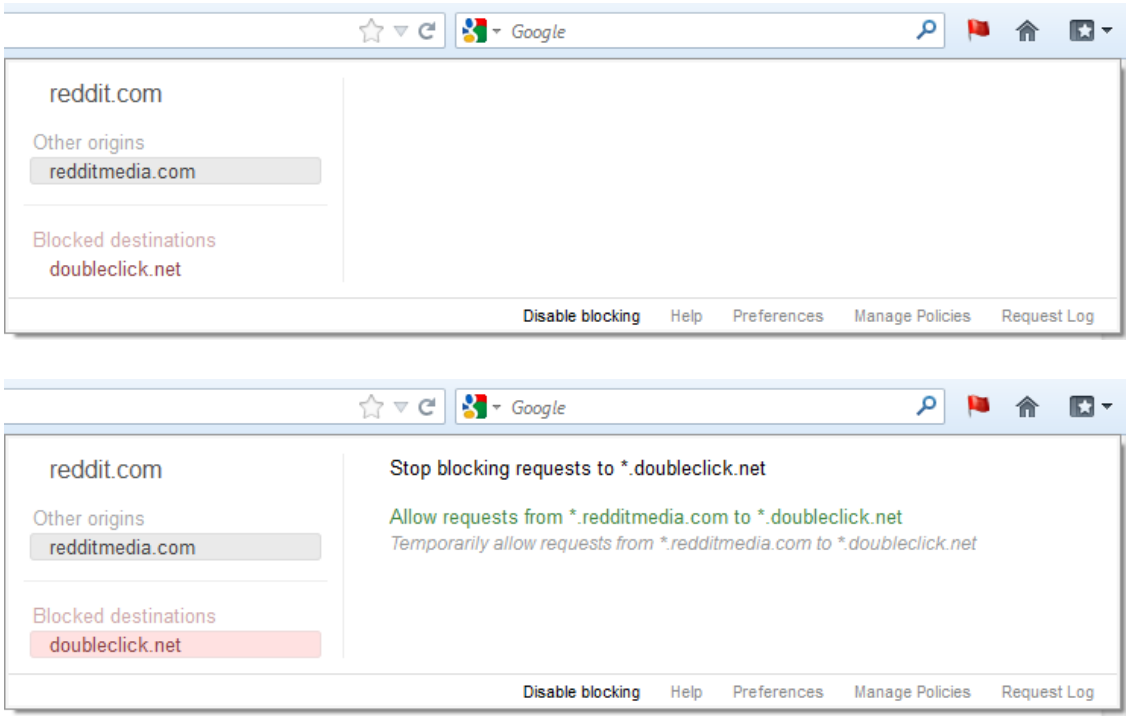



Figure 5.4: RequestPolicy 1.0 menu with other origins. (Top) Other origin selected. (Bottom) Blocked destination of other origin selected.

municated to the user. Our belief is that the appropriate UI design can remove the need for such explanation, though future study of the new menu will be needed to determine whether our design is, in fact, self-explanatory with respect to rule ordering.

## Preferences Window

We have implemented the RequestPolicy 1.0 preferences window using HTML and JavaScript. Instead of opening a fixed-size dialog window, the preferences are opened in a new browser tab as shown in Figure 5.5.

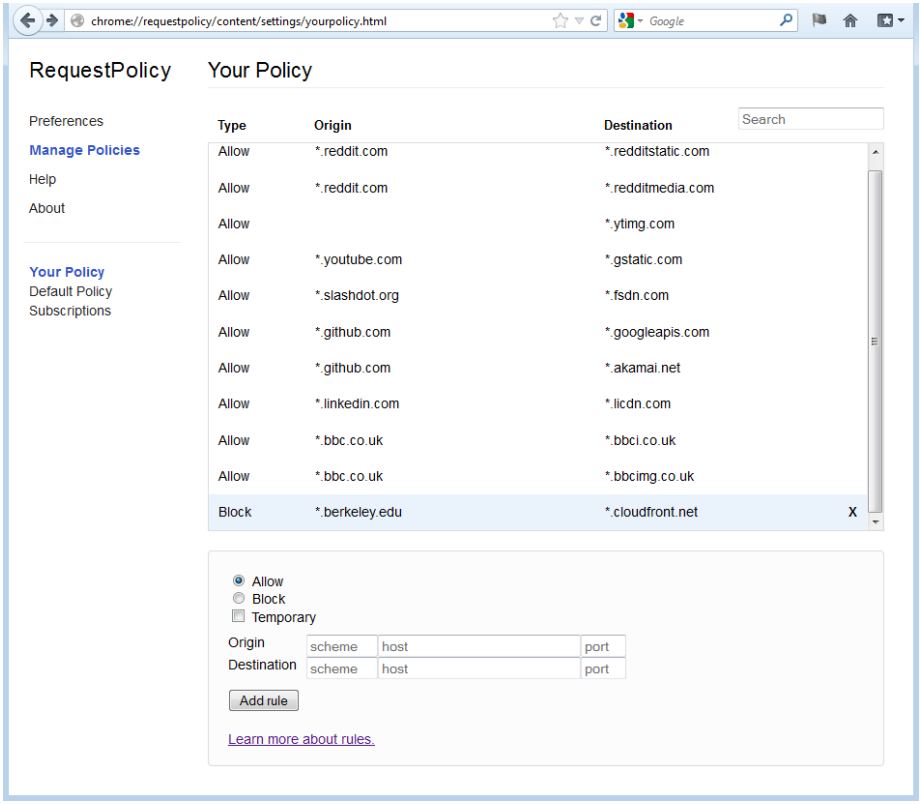



Figure 5.5: RequestPolicy 1.0 preferences window showing user policy management.

# Chapter 6

# Future Work

In order to evaluate the effectiveness of our new design in RequestPolicy 1.0, we will need to gather telemetry from users of the new version as well as perform usability studies. This could also give us insight into how useful the inferences from our telemetry of RequestPolicy 0.5 appear to have been. Additionally, we could integrate a survey into the new RequestPolicy to directly get feedback from users.

The changes we have made for RequestPolicy 1.0 are significant but still leave much to be desired. First and foremost, the subscription policy system we have implemented is only one piece of what is needed for subscriptions to be highly useful. The next major step for subscriptions will be to implement tools that enable an engaged subset of RequestPolicy users to help us improve and maintain subscriptions policies. These tools could include a website where users can discuss our subscriptions as well as curate their own. Additionally, we intend to investigate methods that can enable all users to contribute to the quality of subscription policies by sharing information such as which websites they have found to be broken (e.g. through a button in the menu). It is possible that telemetry could be a useful tool for automatically identifying websites that RequestPolicy "breaks," though the telemetry required would likely need to reveal user-visited URLs. For example, the fact that a user opens the menu on a particular web page is likely a strong indication that the page is broken. Relatedly, it would be highly useful to identify privacy-preserving ways for users to share the contents of their own policies.

The new menu format creates many new possibilities for ways to provide information to

users and help them make whitelisting and blacklisting decisions. For example, a common form of website breakage occurs when requests for stylesheets have been blocked, usually resulting in a page's HTML being rendered using the browser's default styles (white background, large serif font, bulleted lists, and significant whitespace). If stylesheets have been blocked, RequestPolicy could inform the user and give them an option to add any rules necessary to enable the stylesheet requests the site is making. The same is true for images, videos, and even scripts. A difficulty here is in deciding which options should be made available such that we avoid overloading the user with choices and complicating the menu.

The extensible rule format introduced in RequestPolicy 1.0 will allow us to implement additional, interesting rule criteria. Most significantly, we plan to enable rules to specify URL paths and content type (image, stylesheet, video, etc.).

Though we believe the first-run window of RequestPolicy is significantly improved, we are not certain that having a first-run window at all is the best approach. For example, the menu could offer options to read a tutorial or perform advanced configuration. Thus, our primary post-install objective would be to make the user aware of the existence of the RequestPolicy icon that was added to their toolbar.

Recent developments in the Google Chrome browser have opened up the possibility of porting RequestPolicy to Chrome. Specifically, Chrome has recently added an API that allows blocking requests [6]. We may also consider adding support for Firefox Mobile if its market share becomes significant.

It is worth noting that the feedback from users of RequestPolicy 1.0 will likely influence our future development priorities. Over the past four and a half years, RequestPolicy users have been the source of many great suggestions that may have eluded us or that we would not have realized the importance of. This is especially true given that RequestPolicy 1.0 will be usable by an entirely new group of users due to its less strict default behavior.

# Chapter 7

# Conclusion

Our telemetry study is a starting point for understanding the usage of and improving policy-based privacy and security tools. Prior to our study, we had only anecdotal evidence of how RequestPolicy is used. Our lack of real-world usage data for RequestPolicy limited our understanding of how users other than ourselves interact with the extension.

Through our study, we've begun to see usage patterns among RequestPolicy users, including differences in the types of rules users prefer to create. These differences may be due to many factors, some of which are intuitive and some of which we may not be aware of. For example, users may have differences in their levels of privacy and security concern, different threats they are concerned about, as well as differing levels of patience for policy creation and website breakage.

From our perspective as both developers and researchers, the use of telemetry to understand real-world RequestPolicy usage has been extremely valuable. Had telemetry been integrated in RequestPolicy from the beginning, we would be much further along in understanding its usage.

We are only now beginning to understand policy interaction in RequestPolicy beyond anecdotal evidence, our own experiences, and intuition. We believe that our redesign of RequestPolicy has made it both easier to use for existing users as well as usable for a broader set of potential users. However, until we perform usage and usability studies of the new version, we are still relying heavily on intuition to make design decisions.

# Appendix A

# IRB Application

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Amendment Application * * *

### Amendment Application

1. **Summarize the amendment (or proposed changes) you wish to make to your study.**

We are starting and ending this study later than stated in the original protocol. The original protocol said we would end the study in June 2012. We are now planning to begin the study at the earliest in May 2012 and will finish the study by December 2012.

2. **Explain the reason(s) for the proposed amendment(s).**

We have not yet begun this study.

3. **Indicate how the change(s) impact the level of risk to subjects:**

| | |
|---|---|
| | Increase |
| Y | No Change |
| | Decrease |

4. **Describe any effects the change(s) will have regarding risk(s) to the subjects:**

None. The updates to the protocol have only been to change specified study dates.

5. **Will this amendment require the re-consent of any currently enrolled subjects?** N

**If YES, please explain.**

6. **Is this modification consistent with the scope of research activities as described in the proposal(s) for the grant(s) funding the research? (Check N/A if you have no external funding)** Y

7. **Proceed to the appropriate section(s) and make your changes. The list of sections that have been changed or modified will appear below:**

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details. |

---

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Personnel Information * * *

Enter all UC Berkeley study personnel (if not previously entered) and relevant training information. Please read Personnel Titles and Responsibilities: Roles in eProtocol before completing this section.

Note: The Principal Investigator or Faculty Sponsor, Co-Principal Investigator, Student or Postdoctoral Investigator, Administrative Contact, and Other Contact can EDIT and SUBMIT. Other Personnel can only VIEW the protocol.

### Principal Investigator or Faculty Sponsor

| Name of Principal Investigator | Degree (e.g., MS/PhD) | Title |
|---|---|---|
| Vern Paxson | PhD | Professor |
| **y** | **Phone** | **y** |
| vern@eecs.berkeley | | |
| **Department Name** | **Mailing Address** | |
| Computer Science | vern@eecs.berkeley | |

UCB status (select all that apply

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| X | y | | Postdoc | | Grad | | Undergrad | | Other |

ALL PIs and Ky RSONNy
equivalent. ALL STUDy
Training and y

If applicable, please insert date (mm/dd/y ) of completion in appropriate box(es) below:

| CITI | NIH | Other Training (title & date completed) |
|---|---|---|
| | | |

### Student or Postdoctoral Investigator

NOTy aculty
researcher." If NOT a student or postdoc project, enter student(s) and/ or postdoc(s) under Other Personnel below.

| Name of Student/Postdoc Investigator | Degree | Title |
|---|---|---|
| Justin C. Samuel | | |
| **y** | **Phone** | **y** |
| jsamuel@cs.berkeley | | |

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

**Department Name** **Mailing Address**

Computer Science

UCB status (select all that apply):

| | Faculty | | Postdoc | X | Grad | | Undergrad | | Other | |
|---|---|---|---|---|---|---|---|---|---|---|

ALL PIs and KEY PERSONNEL on an NIH award are required to complete NIH Training or an accepted equivalent. ALL STUDENTS engaged in human subjects research are required to complete CITI training. See Training and Education for more information.

If applicable, please insert date (mm/dd/yy) of completion in appropriate box(es) below:

| CITI | NIH | Other Training (title & date completed) |
|---|---|---|
| 10/21/11 | | |



---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Vulnerable Subject Checklist * * *

### Vulnerable Subject Checklist

| Yes | No | |
|---|---|---|
| | N | Children/Minors |
| | N | Prisoners |
| | N | Pregnant Women |
| | N | Fetuses |
| | N | Neonates |
| | N | Educationally Disadvantaged |
| | N | Economically Disadvantaged |
| | N | Cognitively Impaired |
| | N | Other (i.e., any vulnerable subject population(s) not specified above) |



---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Study Sites * * *

### Study Sites

Select All That Apply :

International

International Site(s) (specify country, region, and township or village)

Local

UC Berkeley

UC Davis

UC Irvine

UC Los Angeles

UC Merced

UC Riverside

UC San Diego

UC San Francisco

UC Santa Barbara

UC Santa Cruz

Lawrence Berkeley National Laboratory

Alameda Unified School District (specify schools below)

Berkeley Unified School District (specify schools below)

Oakland Unified School District (specify schools below)

X Other (Specify other Study Sites)

Software running in user's web browser. No restrictions on user nationality or location.

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

## * * * General Checklist * * *

### General Checklist

| Yes | No | |
|---|---|---|
| Y | | Is the research receiving any federal funding (e.g., NIH, NSF, DOD, etc.) |
| | N | Is another UC campus relying on UC Berkeley for IRB review by means of the UC System Memorandum of Understanding (MOU)? |
| | N | Is another institution relying on UC Berkeley for IRB review by means of an Inter-institutional IRB Authorization Agreement? |
| | N | Will subjects be paid for participation? |
| | N | Is this protocol administratively supported by Research Enterprise Services (RES)? |

---

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details. |

---

## * * * Funding * * *

### Funding Checklist

If the research is not funded, check the "Not Funded" box below. If the research is funded, add the funding source to the appropriate table below.

NOTE: Only the Principal Investigator (PI) of the grant or subcontract can add his or her own SPO Funding information in this section. The PI of the grant must also be listed in the Personnel Information section of the protocol in one of the following roles: Principal Investigator or Faculty Sponsor, Student or Postdoctoral Investigator, Co-Principal Investigator, Administrative Contact, or Other Contact. Training Grants can be added by anyone in one of the aforementioned roles. For step-by-step instructions, see Add SPO Funding Quick Guide

Not Funded

### SPO - Funding

### Funding - Other

| | |
|---|---|
| **Funding Type** | **Other**<br>Graduate Fellowship |
| **Sponsor/Provider** | NSF |
| **#** | 2010110910 |
| **Title** | GRFP |
| **Amount** | |
| **Begin** | 08/13/2010 |
| **End** | 08/12/2012 |
| **Narrative Desctiption** | |
| **Lead PI**<br>**(If different from Protocol PI)** | Justin Samuel |

---

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details. |

---

## * * * Expedited Paragraphs * * *

Request for Expedited Review

An expedited review procedure consists of a review of research involving human subjects by the IRB Chair, or by one or more experienced reviewers designated by the Chairperson from among the members of the committees.

In order to be eligible for expedited review, ALL aspects of the research must include activities that (1) present no more than minimal risk to human subjects, and (2) involve only procedures included in one or more of the specific categories listed below.

If requesting Expedited Review, select one or more of the applicable paragraph(s) below.
(DO NOT select any paragraph(s) if your protocol does not qualify for expedited review. Protocols that do not qualify for expedited review will be reviewed by the full (convened) Committee.)

1. Clinical studies of drugs and medical devices only when conditions (a) and (b) are met.

   a) Research on drugs for which an investigational new drug application (21 CFR Part 312) is not required. (Note: Research on marketed drugs that significantly increases the risks or decreases the acceptability of the risks associated with the use of the product is not eligible for expedited review.)

   b) Research on medical devices for which

   i) an investigational device exemption application (21 CFR Part 812) is not required; or

   ii) the medical device is cleared/approved for marketing and the medical device is being used in accordance with its cleared/approved labeling.

2. Collection of blood samples by finger stick, heel stick, ear stick, or venipuncture as follows:

   a) From healthy, non-pregnant adults who weigh at least 110 pounds. For these subjects, the amounts drawn may not exceed 550 ml in an 8 week period and collection may not occur more frequently than 2 times per week; or

   b) From other adults and children, considering the age, weight, and health of the subjects, the collection procedure, the amount of blood to be collected, and the frequency with which it will be collected. For these subjects, the amount drawn may not exceed the lesser

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

of 50 ml or 3 ml per kg in an 8 week period and collection may not occur more frequently than 2 times per week.

3. Prospective collection of biological specimen for research purposes by non-invasive means.
   Examples:
   a) hair and nail clippings in a non-disfiguring manner;
   b) deciduous teeth at time of exfoliation or if routine patient care indicates a need for extraction;
   c) permanent teeth if routine patient care indicates a need for extraction;
   d) excreta and external secretions (including sweat);
   e) uncannulated saliva collected either in an unstimulated fashion or stimulated by chewing gumbase or wax or by applying a dilute citric solution to the tongue;
   f) placenta removed at delivery;
   g) amniotic fluid obtained at the time of rupture of the membrane prior to or during labor;
   h) supra- and subgingival dental plaque and calculus, provided the collection procedure is not more invasive than routine prophylactic scaling of the teeth and the process is accomplished in accordance with accepted prophylactic techniques;
   i) mucosal and skin cells collected by buccal scraping or swab, skin swab, or mouth
   j) sputum collected after saline mist nebulization.

4. Collection of data through non-invasive procedures (not involving general anesthesia or sedation) routinely employed in clinical practice, excluding procedures involving x rays or microwaves. Where medical devices are employed, they must be cleared/approved for marketing. (Studies intended to evaluate the safety and effectiveness of the medical device are not generally eligible for expedited review, including studies of cleared medical devices for new indications.)

   Examples:
   a) physical sensors that are applied either to the surface of the body or at a distance and do not involve input of significant amounts of energy into the subject of an invasion of the subject's privacy;
   b) weighing or testing sensory acuity;
   c) magnetic resonance imaging;
   d) electrocardiography, electroencephalography, thermography, detection of naturally occurring radioactivity, electroretinography, ultrasound, diagnostic infrared imaging, doppler blood flow, and echocardiography;
   e) moderate exercise, muscular strength testing, body composition assessment, and flexibility testing where appropriate given the age, weight, and health of the individual.

5. Research involving materials (data, documents, records, or specimens) that have been collected or will be collected solely for non-research purposes (such as medical treatment or diagnosis). (NOTE:

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details. |

---

Some research in this paragraph may be exempt from the HHS regulations for the protection of human subjects. 45 CFR 46.101(b)(4). This listing refers only to research that is not exempt.)

6. Collection of data from voice, video, digital, or image recordings made for research purposes.

X 7. Research on individual or group characteristics or behavior (including, but not limited to, research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies. (NOTE: Some research in this category may be exempt.)

8. Continuing review of research previously approved by the convened IRB as follows:

   a) Where (i) the research is permanently closed to the enrollment of new subjects; (ii) all subjects have completed all research-related interventions; and (iii) the research remains active only for long-term follow-up of subjects; or

   b) Where no subjects have been enrolled and no additional risks have been identified; or

   c) Where the remaining research activities are limited to data analysis.

9. Continuing review of research, not conducted under an investigational new drug application or investigational device exemption where categories two (2) through eight (8) do not apply but the IRB has determined and documented at a convened meeting that the research involves no greater than minimal risk and no additional risks have been identified.

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

## * * * Purpose, Background, Collaborative Research * * *

Old CPHS # (for Protocols approved before eProtocol)

**Study Title**

Understanding Usage of Web Policy Controls through Telemetry

**Complete each section. When a question is not applicable, enter "N/A". Do not leave any sections blank.**

### 1. Purpose

**Provide a brief explanation of the proposed research, including specific study hypothesis, objectives, and rationale.**

An important area of research into privacy and security issues with web browsing focuses on cross-site requests. The term "request" refers to the browser's use of network communication to contact a website in order to retrieve specific content from that website. Frequently, a web page from one website will instruct the browser to request additional content from other websites. These cross-site requests are invisible to the user as the browser's address bar only indicates the domain name of the website that provided the initial HTML document. Various tools have been developed to give users rule-based control over these requests. However, there is little understanding of how these tools are used once deployed.

In this study, we will gain insight into how people use one of these tools, how requests blocked by the tool impact the user's browsing, and how such tools can be improved to meet the needs of users. Our objective is not to test a specific hypothesis but rather to inform future design decisions for tools that provide controls over browser behavior such as cross-site requests. There are many usage questions we intend to answer. For example, how often do users interact with the the user interfaces (UIs) through which policy rules are managed? What types of rules do users create? How long does it take the user to decide which rule to create or modify? Do users have many "stale" rules from websites they visited only once? Do users primarily choose permissive or restrictive rules? If certain types of rules were enabled by default (e.g. preventing secure HTTPS pages from including scripts obtained over insecure HTTP), how frequently would these cause requests to be blocked?

RequestPolicy is one such tool that gives users control over cross-site requests. RequestPolicy has approximately 20,000 active users and is developed by Justin Samuel, the Student Investigator (SI) on this proposal. Our study will measure various aspects of RequestPolicy's usage through a technique known as telemetry: instrumenting software to perform measurements and automatically transmitting that measurement information back to the developer. We will only collect data from users who opt in to the study.

### 2. Background

**Give relevant background (e.g., summarize previous/current related studies) on condition, procedure,**

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

**product, etc. under investigation, including citations if applicable (attach bibliography in Attachments section).**

Very generally, a web page is an HTML document that often contains only a small portion of the information a web browser needs in order to display the page to the user. The additional information a web page wants to include may range from images to videos to entirely separate web pages (other HTML documents). An HTML document uses URLs to describe how this additional content can be obtained. Frequently, these additional URLs describe content that resides on websites other than the one which provided the HTML document. Browsers automatically request the additional content from these other websites. In doing so, the other websites learn information about the user such as what web page the user is viewing.

It has become common practice for websites that provide additional content to other websites to use this vantage point for tracking the online behavior of large numbers of people. For example, when a user visits <http://berkeley.edu/>, this web page instructs the browser to request additional content from <google-analytics.com>, a website that collects data about user browsing habits. As many sites besides <berkeley.edu> instruct browsers to make requests to this same third-party site, <google-analytics.com> learns a great amount about each individual user. This creates a privacy concern for many people who browse the web.

In response to the growing privacy concern over cross-site requests, various tools have been developed to give users control over these requests. RequestPolicy, developed by the SI, is one such tool. RequestPolicy is an extension for the Mozilla Firefox web browser which enforces a default-deny policy on cross-site requests and provides a UI through which users can manage rules that selectively allow cross-site requests [Samuel 2008]. Browser extensions like RequestPolicy use APIs (Application Programming Interfaces) that the browser provides specifically for the purpose of changing browser functionality. When RequestPolicy blocks cross-site requests, sometimes the website's functionality is degraded. When this happens, users interact with the UI to modify their cross-site request rules in order to “unbreak” the website.

The SI’s previous published work on RequestPolicy identified the difficulty of choosing appropriate default behavior and UIs for the extension [Samuel and Zhang 2009]. There are many different types of users with widely varying expectations, goals, technical understanding, and levels of patience. At the time of RequestPolicy's initial development, many of these design decisions were based on intuition. Now that RequestPolicy has a substantial user base (more than 80,000 current installations, approximately 20,000 daily users [Mozilla 2011]), the potential exists to gain understanding of how RequestPolicy is used and leverage this information to improve RequestPolicy and similar tools.

The procedure we will be using for collecting usage data is to automatically gather measurement data within the user's browser and then automatically transmit this information back to our data collection server. This practice of telemetry is common in many software applications, including popular web browsers such as Chrome and Firefox [Fette 2008, Glek 2011]. Without telemetry, software vendors must rely on users to manually report information about how they are using a product. Manual reporting increases the burden on users who want to assist the software developer by providing this information and, as a result of the inconvenience, the software developers receive much less data.

**3. Collaborative Research**

**a) If any non-UCB institutions or individuals are engaged in the research, explain here.**

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

N/A

b) If any non-UCB institutions or individuals are collaborating in the research, complete the table below and attach any relevant IRB approvals in the Attachments section.

Non-UCB institutions

4. Qualifications of Study Personnel

a) Explain expertise of Principal Investigator, Student/Postdoc Investigator, Faculty Sponsor (if applicable), any Co-Investigators or other key personnel listed in the application, and how it relates to their specific roles in the study team.

Principal Investigator: Prof. Vern Paxson is a faculty member in the UCB Dept. of Electrical Engineering and Computer Sciences and a senior scientist at the International Computer Science Institute. Prof. Paxson has expertise in network measurement and empirical analysis and will be providing guidance to the SI with respect to data collection and analysis.

Student Investigator: Justin Samuel is a UCB Computer Science Ph.D. student studying privacy and security. Justin is the author of RequestPolicy and will be performing data analysis as well as all implementation of data collection. In addition to developing and maintaining RequestPolicy since 2008, Justin has interned with Mozilla's security team where he worked on Firefox privacy and security issues related to cross-site requests.

b) In case of International research, describe the expertise you have, or have access to, which prepares you to conduct research in this location and/or with this subject population, including specific qualifications (e.g., relevant coursework, background, experience, training). Also, explain your knowledge of local community attitudes and cultural norms, and cultural sensitivities necessary to carry out the research. See <a href='http://cphs.berkeley.edu/international.pdf' target='_blank'>CPHS Guidelines on Research in an International Setting

RequestPolicy has a diverse international user base. The SI has developed and maintained RequestPolicy for three years, frequently interacting with users through a variety of support channels. Through this interaction as well as through studying and researching online privacy issues, the SI understands the diversity of views and concerns of RequestPolicy users.

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Subject Population * * *

### 5. Subject Population

**a) Describe proposed subject population, stating age range, gender, race, ethnicity, language and literacy.**

The subject population consists of users of RequestPolicy who are age 18 or older that opt in to participation in the study. The only demographic information we have on RequestPolicy users are approximate numbers of users' primary languages. Of the approximately 20,000 active users, the primary languages are as follows:

English: 13,000
German: 3,500
Japanese: 2,500
French: 800

There are around 20 other primary languages among RequestPolicy users, including some for which there are less than 10 users. The RequestPolicy user interface is only fully translated into 8 languages, excluding English.

Prior unrelated interaction with a small subset of RequestPolicy users through provided support channels indicates that there is a wide variety of users with respect to their technical knowledge. Some are experts in privacy and security while others have extremely limited understanding of the privacy and security threats that RequestPolicy mitigates.

**b) State total (maximum) number of subjects planned for the study and how many must be recruited to obtain this sample size. Explain how number of subjects needed to answer the research question was determined.**

The upper bound on the number of subjects in this study is the number of RequestPolicy users. RequestPolicy currently has approximately 20,000 active users. It is difficult to estimate what percentage of users will choose to participate in this study. All users will be welcome to participate.

**c) If any proposed subjects are children/minors, prisoners, pregnant women, those with physical or cognitive impairments, or others who are considered vulnerable to coercion or undue influence, state rationale for their involvement.**

Minors will be excluded from the study by the consent form which indicates that participation is limited to users who are age 18 or older. Beyond the exclusion of minors, we will have no way of knowing whether any of the subjects of this study are considered to be part of vulnerable populations. Among 20,000 active users, it is likely that some are members of vulnerable populations. As all users will see the same invitation to the study, there is no intentional bias towards any vulnerable population.

### 6. Recruitment

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

a) **Explain how, where, when, and by whom prospective subjects will be identified/selected and approached for study participation. If researcher is subject's instructor, physician, or job supervisor, or if vulnerable subject groups will be recruited, explain what precautions will be taken to minimize potential coercion or undue influence to participate. See CPHS Guidelines on Recruitment for more information.**

We will inform RequestPolicy users of the existence of the study through a new option we will add to the RequestPolicy UI (see attachment "option to participate"). When a user selects this option, a new browser tab will open that shows the consent form. The consent form will explain the purpose and details of the study. Users can begin participating in the study by pressing the "accept" button at the bottom of the consent form.

b) **Describe any recruitment materials (e.g., letters, flyers, advertisements [note type of media/where posted], scripts for verbal recruitment, etc.) and letter of permission/cooperation from institutions, agencies or organizations where off-site subject recruitment will take place (e.g., another UC campus, clinic, school district). Attach these documents in Attachments section.**

There will be no "off site" recruitment. Only users of RequestPolicy will have the option to participate in the study.

c) **Will anyone who will be recruiting or enrolling human subjects for this research receive compensation for each subject enrolled into this protocol? If yes, please identify the individual(s) and the amount of payment (per subject and total).**

No.



## 7. Screening

a) **Provide criteria for subject inclusion and exclusion. If any inclusion/exclusion criteria are based on gender, race, or ethnicity, explain rationale for restrictions.**

There will be no criteria for inclusion other than being a user of RequestPolicy.

b) **If prospective subjects will be screened via tests, interviews, etc., prior to entry into the "main" study, explain how, where, when, and by whom screening will be done. NOTE: Consent must be obtained for screening procedures as well as "main" study procedures. As appropriate, either: 1) create a separate "Screening Consent Form;" or 2) include screening information within the consent form for the main study.**

There will be no screening. All RequestPolicy users will have the option to participate in the study.

## 8. Compensation and Costs

a)

Describe plan for compensation of subjects. If no compensation will be provided, this should be stated. If subjects will be compensated for their participation, explain in detail about the amount and methods/ terms of payment.

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

Include any provisions for partial payment if subject withdraws before study is complete.

When subjects are required to provide Social Security Number in order to be paid, this data must be collected separately from consent documentation. If applicable, describe security measures that will be used to protect subject confidentiality.

**If non-monetary compensation (e.g., course credit, services) will be offered, explain how**

There will be no compensation to users who participate in the study. The only potential benefit to users for participating in the study will be an indirect one: enabling us to improve RequestPolicy.

b) **Discuss reasoning behind amount/method/terms of compensation, including appropriateness of compensation for the study population and avoiding undue influence to participate.**

It is common practice for software to allow users to provide usage information in order to help the developers improve the software. For example, the popular web browsers Chrome and Firefox collect some data by default and other data by user opt-in [Fette 2008, Glek 2011]. When users provide such usage data to software developers, they are not compensated.

c) **Costs to Subjects. If applicable, describe any costs/charges which subjects or their insurance carriers will be expected to pay. (If there are no costs to subjects or their insurers, this should be stated.)**

There will be no costs to users.

---

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.** |

---

## * * * Study Procedures, Alternatives to Participation * * *

### 9. Study Procedures

**a) Describe in chronological order of events how the research will be conducted, providing information about all study procedures (e.g., all interventions/interactions with subjects, data collection procedures etc.), including follow-up procedures.**

1) A user either installs RequestPolicy or upgrades their current version to one which includes the study.
2) When the user opens the RequestPolicy UI, one of the options the user sees invites the user to participate in the study (a screenshot showing placement and wording is shown in attachment "option to participate").
3) If the user chooses the option to participate in the study, a new tab opens with the consent form.
4) If the user presses the "accept" button on the consent form, the tab containing the consent form will close. Otherwise, if the user does not accept (i.e. by closing the consent form without accepting) or never opens the consent form in the first place, none of the following steps will occur.
5) The option in the RequestPolicy UI which invited the user to participate now has different text which gives the user the option to stop participating (a screenshot showing placement and wording is shown in attachment "option to end participation"). If selected, further data collection from this user stops immediately and the menu option once again invites the user to participate. We may also display a notification to the user which tells them that they have stopped participating in the study. Below we continue describing what happens before a user chooses to stop participating in the study.
6) While the user browses the web and interacts with RequestPolicy, RequestPolicy performs measurements and collects study data. This data will include information such as the number of policy rules the user has created (but not what the individual rules are), counts of how many requests were blocked and allowed (but not what the URLs or domains of the requests are), the number of times the user has interacted with the policy management UI, how much time the user spent interacting with the policy management UI, and how many requests would have been blocked or allowed if certain additional rules were part of the user's policy.
7) Occasionally (e.g. once an hour), these statistics are transmitted over an encrypted communication channel to our server. When submitted, an opaque identifier generated by the user's browser will be included with the data. As we collect no other identifying information, this identifier allows us to correlate multiple data submissions from the same user.
8) We analyze the collected data.
9) If we find errors in the our data collection implementation or additional data points we need to collect, we will release software updates which address these errors.
10) When we terminate the study, we will do so through an updated version of RequestPolicy which terminates this study's data collection and indicates to users who were participating in the study that the study has ended.

**b) Explain who will conduct the procedures, where and when they will take place. Indicate frequency and duration of visits/sessions, as well as total time commitment for the study.**

Once a user has opted in to participating in our study, there will be no further required user interaction. Data from opted-in users will be automatically transmitted to our server approximately once an hour. There will be no time requirement on the part of the user. There will be no direct interaction between participants

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

and researchers. The study will end by December 2012.

c) Identify any research procedures that are experimental/investigational. Experimental or investigational procedures are treatments or interventions that do not conform to commonly accepted clinical or research practice as may occur in medical, psychological, or educational settings. Note: if the study only involves standard research or clinical procedures, enter "N/A" here.

All aspects of this study would be considered standard practices in industry or research.

d) If any type of deception or incomplete disclosure will be used, explain what it will entail, why it is justified, and what the plans are to debrief subjects. See CPHS Guidelines on Deception and Incomplete Disclosure for more information. Any debriefing materials should be included in the Attachments section.

There will be no deception.

e) State if audio or video taping will occur. Describe what will become of the tapes after the project (e.g., shown at scientific meetings, erased) and final disposition of the tapes.

No.

10. Alternatives to Participation

Describe appropriate alternative resources, procedures, courses of treatment, if any, that are available to prospective subjects. If there are no appropriate alternatives to study participation, this should be stated. If the study does not involve treatment/intervention, enter "N/A" here.

N/A

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Risks and Discomforts * * *

### 11. Risks and Discomforts

**a) Describe all known risks and discomforts associated with study procedures, whether physical, psychological, economic or social (e.g., pain, stress, invasion of privacy, breach of confidentiality), noting the likelihood and degree of potential harm.**

1) Over-collection of data.

A bug in our data collection could result in us collecting data which we did not intend to collect. The likelihood of an over-collection bug involving sensitive or personal information is low though the harm of such a bug could be quite severe for some users. For example, a nearly worst-case over-collection might include information which reveals specific websites a user has visited. For users engaged in illegal activities, this type of over-collection could result in our data set including information which could cause harm to the user if exposed.

2) Public disclosure of collected data.

If our data collection server is misconfigured or gets compromised by an attacker, the data we have collected from users may become public or may be obtained by an attacker. The likelihood of a disclosure bug is low as the risk of disclosure would be limited to server compromise or improper data handling by the investigators. If a public disclosure occurred, the impact would be very low as the collected data does not contain identifying information.

3) Software bugs in data collection interfering with normal web browsing.

A bug in our extension could cause the browser to crash or otherwise negatively impact the user's browsing experience. The likelihood of a bug in data collection interfering with normal browsing is low.

**b) Discuss measures that will be taken to minimize risks and discomforts to subjects.**

1) Over-collection of data.

We mitigate the risk of over-collection by only collecting the specific data we are interested in. We do not, for example, collect browser configuration files which might contain unexpected personal data. The SI will perform both manual and automated analysis of collected data in order to identify whether data over-collection has occurred.

2) Public disclosure of collected data.

We mitigate the risk of public disclosure of data by running a fully patched Linux server that has been configured with attention to security (e.g. unnecessary services disabled, internally used services firewalled off, etc.). Further, the investigators handling and analyzing the data after it has been downloaded

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

from the data collection server are experienced with computer security. Also worth noting is that the data we are collecting has little value to others as it contains general information about the behavior of RequestPolicy and how users interact with it but does not include identifying information. Thus, it is not an inherently attractive target for attackers.

3) Software bugs in data collection interfering with normal web browsing.

This type of risk is mitigated by the fact that we have over 100 beta testers (users who choose to run beta versions of RequestPolicy) who help us test new versions before they are released. Further, as RequestPolicy is implemented entirely in a memory-safe language (JavaScript) and uses only browser APIs which are intended for use by extensions, it is not common to crash the browser through an extension bug.

c) **Discuss plans for reporting unanticipated problems involving risks to subjects or others, or serious adverse events, to CPHS. (This applies to all types of research.) See <a href='http://cphs.berkeley.edu/reviewtypes.html#adverse' target='_blank'>Adverse Event and Unanticipated Problem Reporting.**

An initial report will be made by fax, mail/delivery, phone, email, to the Director, Research Subject Protection as soon as possible, but within no more than one week (7 calendar days) of the Principal Investigator learning of the incident. The initial report will be followed by a formal written report within no more than two weeks (14 calendar days) of the Principal Investigator learning of the incident.

d) **Describe plans for provision of treatment for study-related injuries, and how costs of injury treatment will be covered. If the study involves more than minimal risk, indicate that the researchers are familiar with and will follow University of California policy in this regard, and will use recommended wording on any consent forms (see <a href='http://cphs.berkeley.edu/informedconsent.html' target='_blank'>CPHS Informed Consent Guidelines).**

We will fix any bugs we discover in our data collection software. Through a combination of manual and automated methods, we will audit our collected data to look for over-collection and delete any over-collected data. The researchers are familiar with and will follow University of California policy and will use recommended wording on consent forms where applicable.

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Benefits, Confidentiality * * *

### 12. Benefits

**Describe any potential benefits to the individual subject, group of subjects, and/or society. If subjects will not benefit directly from study procedures, this should be stated.**

**NOTE: Do not include compensation/payment of subjects in this section, as remuneration is not considered a "benefit" of participation in research.**

Subjects will not receive any direct benefit from participation in our study. The RequestPolicy software will benefit by understanding how users interact with the software which in turn provides a basis for making various design decisions. Society will benefit from an increased understanding of how privacy and security software is used by real users and potentially how the usability of such software can be improved.

### 13. Confidentiality

NOTE: See CPHS Data Security Policy before completing this section.

a) **Explain how subject privacy will be protected and how confidentiality of subject information will be maintained. Discuss who will have access to study records/specimens and how the records will be secured.**

The data we collect will not contain identifying information. We will not collect data about which domains or URLs a user visits, nor will we collect personal information such as names or email addresses. We will see a participant's IP address on our server when measurement data is sent to our server, however we will not record the IP address.

The data collected from each participant will include an opaque identifier which will allow us to correlate multiple data submissions from the same participant. This opaque identifier is used specifically because we are not collecting any other information which would allow us to recognize separate data submissions as having come from the same participant.

We will use best practices to keep our data collection server secure. All data will be transmitted to and from our server using industry-standard encryption. The data collection server will be kept fully patched and properly configured. Only the SI and PI will have access to the raw collected data. In the future, after the study is over, we may bring on additional RequestPolicy developers. Though we have no plans to add developers, future developers would also be given access to the study data.

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

b) **Will subjects be asked to give permission for release of identifiable data (e.g., information, videotapes), now or in future? If so, explain here and include appropriate statements in consent materials.**

Even though the information we collect will not contain identifying information, we will not release our raw data.

c) **Will data be collected anonymously (i.e., no identifying information from subjects will be collected/ recorded that can be linked to the study data) (NOTE: Data is not anonymous if there is a code linking it to personally identifiable information. Also, audio and video recordings are generally not considered to be anonymous.)**

No, data will not be collected anonymously. The primary reasons for this are that a) the collected data is transmitted back to our server directly by the user's browser which means the user's IP address is visible to our server, and b) data transmitted to our server will include an identifier which will allow us to correlate separate data submissions from the same user. The identifier will be a random identifier generated by our software running in the user's browser at the time the user consents to participation in the study. We will not have any way to map this identifier to identifying information other than the user's IP address. Further, we will not be collecting the IP address as part of the research data set and we will disable IP address logging by the data collection server.

d) **If using existing data/biological specimens, will the researchers have access to a code linking the data to personally identifiable information?**

N/A

e) **If identifying information will be collected and linked to data/specimens, explain at what stage identifiers will be removed from the data/specimens. If identifiers will be retained, explain why this is necessary and how confidentiality will be protected.**

The participant identifier will not be linkable to any other collected data. The identifier will never be removed from the data set.

f) **If the data is coded, explain where the key to identifiers will be stored, how it will be protected, and who will have access to it.**

The participant identifier we use is not coded and we will not intentionally collect or record additional data which could map the identifier to other personal information.

g) **Indicate whether research data/specimens will be destroyed at the end of the study. If data will not be destroyed, explain why, where, in what format, how long it will be retained and who will have access to it.**

Any IP address data collected due to server misconfiguration will be destroyed. Due to the lack of collection of sensitive information and thus the minimal risk to users, the collected research data may never be destroyed. This study will continue through December 2012. Only the SI and PI will have access to the raw collected data. In the future, after the study is over, we may bring on additional RequestPolicy developers. Though we have no plans to add developers, future developers would also be given access to the study data.

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

h) Explain how data collection instruments, audiotapes, videotapes, photographs, etc., will be stored and who will have access to them. Indicate at what point they will be transcribed and/or destroyed (if ever).

Data will be stored in a database on our data collection server. Additional copies of the data may be stored on the investigators' computers. Some or all of the data may never be destroyed.

---

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.**<br>**Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.** |

---

## * * * Potential Financial Conflict of Interest * * *

**14. Potential Financial Conflict of Interest**

Individuals who have independent roles in projects and who are responsible for the design, analysis, conduct, or reporting of the results of research performed (or to be performed) under a human subjects protocol must disclose whether or not they have a financial interest in or association with the sponsor or the company supplying materials, drugs, or devices for the project. This checklist pertains to the entire project team working under the protocol. Any individual who has a conflict must comply with University regulations and procedures for disclosure of financial conflict of interest.

See Conflict of Interest Committee Website for more information.



Please answer the following questions:

Does any member of the project team (defined as UCB or non-UCB personnel working under the protocol) with substantive responsibility for the design, conduct, or reporting of activities under the protocol, or any member of their immediate family (defined as spouse, dependent child, or registered domestic partner) have any of the following relationships with the non-UC entity financing the research to be done under the protocol or the non-UC entity supplying materials, drugs or devices being tested under the protocol:

| | | |
|---|---|---|
| 1. | N | **Positions of management (e.g., board member, scientific advisor, director, officer, partner, trustee, employee, consultant).** |
| 2. | N | **Equity interest (e.g., stock, stock options, investment, or other ownership).** |
| 3. | Y | **Rights to a pending patent application or issued patent to any invention(s), or license rights or copyright for software that has a direct relationship to the project proposed.** |

If the answer to any of the above is Yes, then each individual with any "Yes" response(s) must submit a Human Subjects Financial Conflict of Interest Form DIRECTLY to the Conflict of Interest (COI) Committee for a separate review.

NOTE: When review by the COI Committee is required, CPHS approval or exemption of protocols will be contingent upon the disclosure and resolution of all financial conflicts of interest, as determined by the COI Committee.

---

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.** |

---

## * * * Informed Consent * * *

### 15. Informed Consent

**Add the consent documents and/or waivers needed for this research using the table at the bottom of the page. Any foreign language versions should also be added. You will be asked to provide relevant background information for each consent document or waiver. The various consent/waiver options are described below.**

**Note: DO NOT include child assent documents, parent permission documents or waivers here (these are addressed in the next section).**

Altered and Unsigned Consent - A consent document that has omitted required information and does not include a place for a participant's signature. This means that CPHS is being asked to waive one or more elements of consent in addition to the requirement for documented consent.

Altered Consent Form - A consent form that has omitted required information. This means that the CPHS is asked to waive one or more required elements of informed consent. For example, if the purpose of the study will not be disclosed to participants in order to avoid bias, this option should be selected because disclosure of the "purpose" is a required element of informed consent. The form must include a signature line and date line for the individual to sign if he or she agrees to participate.

Consent Form - A standard consent document that embodies all of the required information (elements of informed consent) designed to help an individual make an informed decision about whether or not to participate in the research. The form must include a signature line and date line for the individual to sign if he or she agrees to participate. The Consent Form can also be presented as a "short form" document stating that the required elements of informed consent have been presented orally to the participant. When the short form method is used, a "summary" of the information that is presented to the participant must also be provided for CPHS approval and there must be an impartial witness to the oral presentation. The witness must sign the summary as well as the short form and the participant must sign the summary. The "short form" method may be used in circumstances where oral presentation of consent is preferable or necessary, e.g., subjects are illiterate in English or their native language.

Consent Waiver - No consent will be sought at all. This means that the CPHS is asked to waive the requirement for informed consent. This option is often appropriate for research that involves use of existing data or samples

Unsigned Consent - A document that embodies all of the required information (elements of informed consent), but does not include a place for a participant to indicate with a signature that he or she agrees to take part in the research. This means that the CPHS is asked to waive the requirement for documented (signed) consent. For example, if consent will be obtained verbally or using a button on the web, this option should be selected.

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

•Informed Consent Guidelines, Templates and Sample Forms

•Informed Consent Policies and Procedures

•Consent Builder: Online Tool for Creating Consent Forms

## Informed Consent

| | | | |
|---|---|---|---|
| Consent/Waiver Description (e.g. Consent for Group A, Waiver for Group B, Surrogate Consent for Group C) | Consent form | | |
| Consent Type | Unsigned Consent | | |
| Attach Consent Document (in PDF format) | X | Consent Document | 2011-10-3676_Samuel_requestpolicy_consent_form |

Explain how, where, when, and by whom informed consent will be obtained. If any vulnerable subject groups are involved, discuss relevant considerations. Note: If attaching multiple consent forms and consent process has already been described for another consent form, simply refer to the other form (e.g., "consent process is the same as for Group A").

Consent will be obtained through RequestPolicy's user interface before usage data will be collected by us. Consent will involve clicking an "Accept" button at the bottom of the consent form. No additional information will be required or collected in order to complete the consent form. Specifically, we will not ask for the user's name, signature, or other personal information. There will be a single consent form which will be the same for all users. We will not know if any individual user is a member of a vulnerable population.

For CPHS to approve a waiver of the requirement for documented (signed) consent, either criterion A or B must be met. Select the applicable criterion and provide justification in the box below.

**A.** The only record linking the subject and the research would be the consent document AND the principal risk of the research would be potential harm resulting from a breach of confidentiality.

Y **B.** The research presents no more than minimal risk of harm to subjects AND involves no procedures for which written consent is normally required outside of the research context.

The primary risk of harm to subjects is that of disclosure of sensitive information, especially with respect to their browsing history. With the way we have designed our study, the risk of harm to subjects is no more than minimal. We will not be collecting personally identifiable information or browsing history. The only identifying information we will have access to are the IP addresses of users when measurement data is submitted to us. We will not be recording IP addresses and this information will therefore not be part of our data set. The practices we are using for obtaining consent are standard for this type of data when collected in industry.

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.**
**Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

## * * * Child Assent & Parent Permission * * *

### 16. Child Assent and Parent/Guardian Permission

Add each assent document, parent/guardian permission document, and/or waiver needed for this research using the table at the bottom of the page. Any foreign language versions should also be added. You will be asked to provide relevant background information for each assent, permission, or waiver. The various assent, permission, and waiver options are described below.

Altered and Unsigned Parent/Guardian Permission Form - A parent permission document that has omitted required information (elements) and does not include a place for a parent to indicate with a signature that he or she agrees to permit the child's participation. This means that CPHS is being asked to waive one or more elements of consent in addition to the requirement for documented consent.

Altered Parent/Guardian Permission Form - A permission form that has omitted required information (elements). This means that the CPHS is asked to waive one or more required elements of informed consent. However, the form must include signature and date lines for the parent(s)/guardian(s) to sign if the child is permitted to take part in the research.

Assent Document - A form or script of the information that will be conveyed to the child about the study. In general, researchers must obtain the affirmative agreement of children ages seven years and older for their participation. Assent forms should be written at a level understandable to the child. If the study includes a broad age range of children, more than one assent form may be needed (i.e., an assent form suitable for a 15 year old is not usually suitable for a 7 year old child).

Assent Waiver - No child assent will be sought at all. This means that CPHS is asked to waive the requirement for child assent. Among other circumstances, this option is appropriate when the capability of the child to understand the research is too limited or when the research holds out a prospect of direct benefit that is important to the health or well being of the child.

Parent/Guardian Permission Form - A document that embodies all of the required information (elements of informed consent) designed to help the parent/guardian of a child make an informed decision about whether or not to permit the child's participation in the research. The form must include signature and date lines for the parent(s)/guardian(s) to sign if the child is permitted to take part in the research.

Permission Waiver - No parent/guardian permission will be sought at all. This means that the CPHS is asked to waive the requirement for parent/guardian permission. This option, for example, is often appropriate for research designed to study conditions in children or a study population for which parental permission is not a reasonable requirement to protect the children (e.g., neglected or abused children).

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

Unsigned Parent/Guardian Permission Form - A parent permission document that embodies all of the required information (elements of informed consent), but does not include a place for a parent to indicate with a signature that he or she agrees to permit the child's participation. This means that the CPHS is asked to waive the requirement for documented (signed) consent.

•<a href='http://cphs.berkeley.edu/informedconsent.html' target='_blank'> Child Assent and Parent Permission Guidelines, Templates, and Sample Forms

•Policies and Procedures on Child Assent and Parent Permission

Documents and Waivers

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

## * * * Attachments * * *

### 17. Attachments

Add appropriate attachments (e.g., advertisements, data collection instruments, IRB approvals from collaborating institutions, etc.) in this section. Attachments MUST be in PDF format.

| | |
|---|---|
| **Document Type** | **Other** |
| | option_to_participate |
| **Document Name** | option_to_participate |
| **Document Type** | **Other** |
| | option_to_end_participation |
| **Document Name** | option_to_end_participation |
| **Document Type** | **References** |
| | bibliography |
| **Document Name** | bibliography |
| **Document Type** | **CITI Certificate(s)** |
| | citi_completion_report_Justin_Samuel |
| **Document Name** | citi_completion_report_Justin_Samuel |



---

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.<br>Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details. |

---

## * * * Assurance * * *

**Assurance**

**As Faculty Sponsor, I understand that I am responsible for overseeing the protection of the rights and welfare of the human subjects, and adherence to CPHS requirements, federal regulations, and state statutes for human subjects research.**

**I hereby assure the following:**

1. I have read the protocol.
2. I have discussed with the Student/Postdoc Investigator how to comply with his or her assurances.
3. I will be available throughout the course of the study to provide guidance and consultation.

X **I have read and agree to the above assurances.**

**As Student/Postdoctoral Investigator, I am responsible for the performance of this study, the protection of the rights and welfare of the human subjects, and strict adherence by all co-investigators and research personnel to CPHS requirements, federal regulations, and state statutes for human subjects research.**

**I hereby assure the following:**

1. The information provided in this application is accurate to the best of my knowledge.
2. All experiments and procedures involving human subjects will be performed under my supervision or that of another qualified professional listed on this protocol.
3. This protocol covers the human subjects research activities described in the grant proposal(s) supporting this research and any such activities that are not covered have been/will be covered by a CPHS approved protocol.

| | |
|---|---|
| **Protocol Title:** | Understanding Usage of Web Policy Controls through Telemetry |
| **Protocol Type:** | Soc-Behav-Ed Non-Exempt |
| **Date Submitted:** | 04/25/2012 |
| **Approval Period:** | 04/28/2012-02/20/2013 |
| **Important Note:** | **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.**<br>**Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.** |

---

4. The legally effective informed consent of all human subjects or their legally authorized representative will be obtained (unless waived) using only the current, approved consent form(s).

5. If any study subject experiences an unanticipated problem involving risks to subjects or others, and/or a serious adverse event, the CPHS will be informed promptly within no more than one week (7 calendar days), and receive a written report within no more than two weeks (14 calendar days), of recognition/ notification of the event.

6. No change in the design, conduct, or key personnel of this research will be implemented without prior CPHS review and approval, unless the changes are necessary to eliminate an apparent immediate hazard to subjects. Changes made to eliminate hazards to subjects will be reported to OPHS/CPHS via the AE/UP reporting process.

7. Applications for continuation review will be submitted in a timely manner prior to the expiration date to allow sufficient time for the renewal process. I understand that if approval expires, all research activity (including data analysis) must cease until I receive notice of re-approval by the CPHS.

8. Participants' complaints or requests for information about the study will be addressed appropriately.

9. I will promptly and completely comply with a CPHS decision to suspend or withdraw its approval for the project.

10. I will submit a study closure form at the conclusion of this project.

X **I have read and agree to the above assurances.**

---

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.

---

*** * * Attached Document * * ***

| Document Name | Created Date |
|---|---|
| 2011-10-3676_Samuel_requestpolicy_consent_form.pdf | 04/25/2012 |

University of California at Berkeley
Consent to Participate in Research

# Understanding Usage of RequestPolicy through Telemetry

*In order to participate, you must be at least 18 years old and click "Accept" at the bottom of this page.*

## Introduction and Purpose

My name is Justin Samuel. I'm the author of RequestPolicy. I'm also a graduate student at the University of California, Berkeley working with Professor Vern Paxson in the Department of Electrical Engineering and Computer Sciences. I would like to invite you to take part in my research study of the usage of RequestPolicy.

## Procedures

If you agree to participate in my research, RequestPolicy will collect and transmit back to us some data about how you use RequestPolicy. We will not collect information about specific websites you visit. The type of information we're collecting involves how you use RequestPolicy and how RequestPolicy impacts your browsing. For example, we will collect information on how often you add and remove items from your whitelist (but not what those items are), whether you use certain features, which toolbar you have the RequestPolicy button placed in, how long RequestPolicy takes to load your whitelist when the browser starts, and how many items you have in your whitelist.

## Benefits

There is no direct benefit to you from taking part in this study. We hope that the research will improve the usability of RequestPolicy as well as other privacy and security software.

## Risks

As with all research, there is a chance that confidentiality could be compromised. However, we are taking precautions to minimize this risk.

## Confidentiality

Your study data will be handled as confidentially as possible. If results of this study are published or presented, personally identifiable information will not be used. We will not record your IP address on our server when we collect study data. To further decrease risks to confidentiality, RequestPolicy will use SSL encryption when it transmits study data back to our server. Of course, we'll also do our best to keep our server secure.

When the research is completed, I may save the data for use in future research done by myself or others. The data may also be used by future RequestPolicy developers other than myself. We will not make public the data that we collect.

## Compensation

You will not be paid for taking part in this study.

## Rights

Participation in research is completely voluntary. You have the right to decline to participate or to withdraw at any point in this study without penalty or loss of benefits to which you are otherwise entitled.

## Questions

If you have any questions about this research, please feel free to contact me. I can be reached at support@requestpolicy.com. If you have any questions about your rights or treatment as a research participant in this study, please contact the University of California at Berkeley's Committee for Protection of Human Subjects at 510-642-7461, or e-mail subjects@berkeley.edu. If you agree to take part in the research, please click the "Accept" button below.

**I certify that I am 18 years or older. I have read this consent form and I agree to take part in this research.**

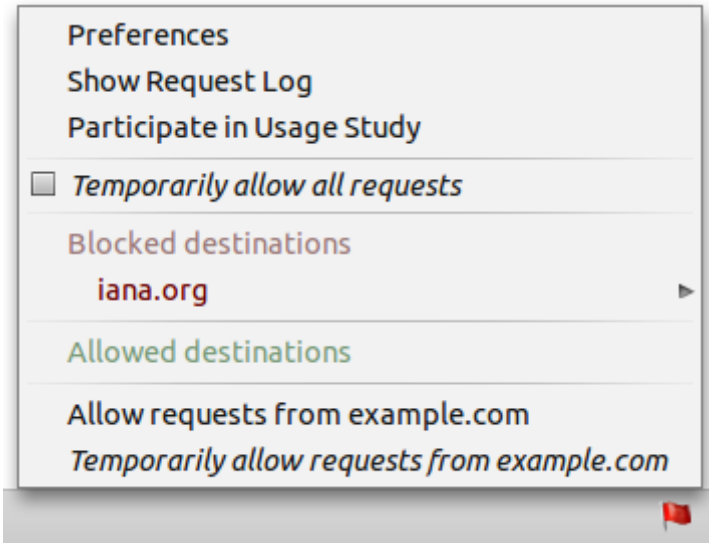
Accept

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

*** * * Attached Document * * ***

| Document Name | Created Date |
|---|---|
| option_to_participate.pdf | 04/25/2012 |

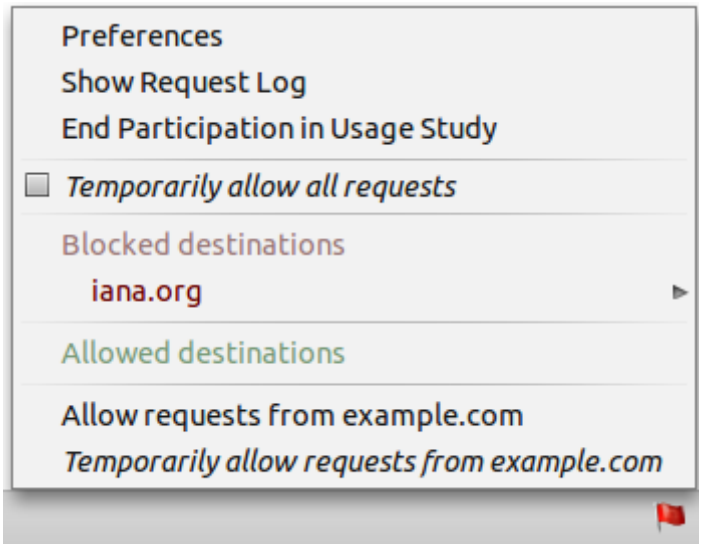

Preferences
Show Request Log
Participate in Usage Study
Temporarily allow all requests
Blocked destinations
iana.org
Allowed destinations
Allow requests from example.com
Temporarily allow requests from example.com

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

*** * * Attached Document * * ***

| Document Name | Created Date |
|---|---|
| option_to_end_participation.pdf | 04/25/2012 |


Preferences
Show Request Log
End Participation in Usage Study
Temporarily allow all requests
Blocked destinations
iana.org
Allowed destinations
Allow requests from example.com
Temporarily allow requests from example.com

**Protocol Title:** Understanding Usage of Web Policy Controls through Telemetry
**Protocol Type:** Soc-Behav-Ed Non-Exempt
**Date Submitted:** 04/25/2012
**Approval Period:** 04/28/2012-02/20/2013
**Important Note:** **This Print View may not reflect all comments and contingencies for approval. Please check the comments section of the online protocol.
Questions that appear to not have been answered may not have been required for this submission. Please see the system application for more details.**

---

*** * * Attached Document * * ***

| Document Name | Created Date |
|---|---|
| bibliography.pdf | 04/25/2012 |

## Bibliography

[Fette 2008] I. Fette. Chromium Blog: Google Chrome, Chromium, and Google. http://blog.chromium.org/2008/10/google-chrome-chromium-and-google.html. Oct. 2008.

[Glek 2011] T. Glek. Firefox 7: Telemetry. https://hacks.mozilla.org/2011/09/firefox-7-telemetry/. Sept. 2011.

[Mozilla 2011] Mozilla. Addons for Firefox - Statistics for RequestPolicy. https://addons.mozilla.org/en-US/firefox/addon/requestpolicy/statistics/. 2011.

[Samuel 2008] J. Samuel. RequestPolicy. https://www.requestpolicy.com/. 2008.

[Samuel and Zhang 2009] J. Samuel and B. Zhang. RequestPolicy: Increasing Web Browsing Privacy through Control of Cross-Site Requests. The 9th Privacy Enhancing Technologies Symposium (PETS 2009). https://www.eecs.berkeley.edu/~jsamuel/papers/requestpolicy-pets2009.pdf

# Bibliography

[1] R.D. Banker et al. “Software complexity and maintenance costs”. In: *Communications of the ACM* 36.11 (1993).

[2] D. Cancel and F. Shnir. *Ghostery :: Add-ons for Firefox*. https://addons.mozilla.org/en-US/firefox/addon/ghostery/.

[3] M. Chew. *Writing for the 98%*. http://monica-at-mozilla.blogspot.com/2013/02/writing-for-98.html.

[4] J. Clark, P. C. Van Oorschot, and C. Adams. “Usability of anonymous web browsing: an examination of Tor interfaces and deployability”. In: *Proceedings of the 3rd symposium on Usable privacy and security*. ACM. 2007, pp. 41–51.

[5] P. Eckersley. “How unique is your web browser?” In: *Privacy Enhancing Technologies*. 2010, pp. 1–18.

[6] Google Chrome Extensions. *chrome.experimental.webRequest*. https://code.google.com/chrome/extensions/experimental.webRequest.html.

[7] T. Glek. *Firefox 7: Telemetry*. https://blog.mozilla.org/tglek/2011/09/20/firefox-7-telemetry-faster-startup/.

[8] J. Gomez, T. Pinnick, and A. Soltani. *KnowPrivacy*. http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf. 2009.

[9] Google. *Google Chrome Privacy Notice*. http://www.google.com/chrome/intl/en/privacy.html.

[10] D. M. Hilbert and D. F. Redmiles. “Extracting usability information from user interface events”. In: *ACM Computing Surveys (CSUR)* 32.4 (2000), pp. 384–421.

[11] E. van Kempen. *BlockSite :: Add-ons for Firefox*. `https://addons.mozilla.org/en-US/firefox/addon/3145`.

[12] J.I. Kiger. "The depth/breadth trade-off in the design of menu-driven user interfaces". In: *International Journal of Man-Machine Studies* 20.2 (1984).

[13] B. Krishnamurthy, D. Malandrino, and C.E. Wills. "Measuring privacy loss and the impact of privacy protection in web browsing". In: *Symposium on Usable Privacy and Security*. 2007.

[14] B. Krishnamurthy, K. Naryshkin, and C. Wills. "Privacy leakage vs. protection measures: the growing disconnect". In: *Web 2.0 Security and Privacy Workshop*. 2011.

[15] B. Krishnamurthy and C. Wills. "Privacy diffusion on the web: A longitudinal perspective". In: *International Conference on the World Wide Web*. 2009.

[16] B. Krishnamurthy and C.E. Wills. "Generating a privacy footprint on the Internet". In: *ACM SIGCOMM Conference on Internet Measurement*. 2006.

[17] J.R. Mayer and J.C. Mitchell. "Third-party web tracking: Policy and technology". In: *IEEE Symposium on Security and Privacy*. IEEE. 2012, pp. 413–427.

[18] Microsoft Corporation. *Windows Internet Explorer 10 Developer Preview privacy statement*. `http://windows.microsoft.com/en-US/internet-explorer/ie10-developer-preview-privacy-statement`.

[19] Mozilla. *Privacy and Security :: Add-ons for Firefox*. `https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/?sort=users`.

[20] G. Norcie, K. Caine, and L. J. Camp. "Eliminating Stop-Points in the Installation and Use of Anonymity Systems: a Usability Evaluation of the Tor Browser Bundle". In: *HotPETS*. 2012.

[21] W. Palant. *Adblock Plus - for annoyance-free web surfing*. `https://adblockplus.org/`.

[22] A. Roosendaal. *Facebook Tracks and Traces Everyone: Like This!* Tech. rep. No. 03/2011. Tilburg Law School Legal Studies Research Paper Series.

[23] J. Samuel and B. Zhang. "RequestPolicy: Increasing Web Browsing Privacy through Control of Cross-Site Requests". In: *Privacy Enhancing Technologies*. 2009.

[24] Tails. *Tails - IceWeasel addon - RequestPolicy*. `https://tails.boum.org/todo/iceweasel_addon_-_RequestPolicy/`.

[25] The Tor Blog. *New Tor Browser Bundles for Windows*. `https://blog.torproject.org/blog/new-tor-browser-bundles-windows`.

[26] W3Schools. *OS Statistics*. `http://www.w3schools.com/browsers/browsers_os.asp`.