Making Secure Systems Easy for the Public to Use

Lorrie Faith Cranor
lorrie.cranor.org
@lorrietweet
Human error is the root cause of most data breaches

Financial damage of data leaks must be considered by firms

The Weakest Link: The Role of Human Error in Cybersecurity

Almost 90% of Cyber Attacks are Caused by Human Error or Behavior

By Ross Kelly - March 3, 2017

Few store managers would respond to revelations that a junior assistant had been stealing from the cash register by investing thousands of dollars in new security cameras. It could be far cheaper for them to instill hiring practices that ensure employees are honest from the start.
The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations
Twitter recently introduced an updated privacy policy announcing changes to how they collect user data and deliver advertising into your timeline. So what does the update mean and what should you do about it?

If you haven't logged in to Twitter since the changes were announced, you'll see this message:
Privacy is complicated
Better together

Examining **security/privacy** and **usability** together is often critical for achieving either.

Don’t assume you always have to tradeoff security for usability, sometimes you can achieve both!
Security and privacy are secondary tasks
Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may contribute to security failures, and the user test demonstrated that when our test participants were given 90 minutes in which to sign and encrypt a message using PGP 5.0, the majority of them were unable to do so successfully.

We conclude that PGP 5.0 is not usable enough to provide effective security for most computer users, despite its attractive graphical user interface, supporting our hypothesis that user interface design for effective security remains an open problem. We close with a brief description of our continuing work on the development and application of user interface design principles and techniques for security.

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct network protocols, and bug-free code will not provide security if users do not use them correctly. Yet, average citizens are now increasingly encouraged to make use of networked computers for private transactions, and the need to make security manageable for even untrained users has become critical. This is inescapably a user interface design problem. Legal remedies, increased automation, and user training provide only limited solutions. Individual users may not have the resources to pursue an attacker legally, and may not even realize that an attack took place. Automation may work for securing a communications channel, but not for setting access control policy when a user wants to share some files and not others. Employees can be required to attend training sessions, but home computer users cannot.
22 years later
Johnny still can't encrypt...
We still rely on users to do security tasks that they aren’t good at

Creating unique and memorable passwords
Users have many misconceptions about passwords
MISCONCEPTION

Keyboard patterns are secure

1qazxsw2

B. Ur, F. Noma, J. Bees, S. Segreti, R. Shay, L. Bauer, N. Christin, L Cranor."I Added '!' At The End To Make It Secure": Observing Password Creation in the Lab. SOUPS 2015
MISCONCEPTION

Adding ! to the end makes it secure

Password!

iloveyou!

monkey!
Password perceptions study

Password perceptions study

Password perceptions study

iloveryou88

much more secure

4,000,000,000 ×

more secure!

ieatkale88

much more secure

Most password meters don’t help much
Change your password

Strengthen the security of your account with a new password.

Your password is weak, create a stronger password.

Confirm new password

show password

Continue

Cancel
Demo: cups.cs.cmu.edu/meter

Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements

Joshua Tan, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor
Carnegie Mellon University
{jstan,lbauer,nicolasc,lorrie}@cmu.edu

ABSTRACT
Multiple mechanisms exist to encourage users to create stronger passwords, including minimum-length and character-class requirements, prohibiting blocklisted passwords, and giving feedback on the strength of candidate passwords. Despite much research, there is little definitive, scientific guidance on how these mechanisms should be combined and configured to best effect. Through two online experiments, we evaluated combinations of minimum-length and character-class requirements, blocklists, and a minimum-strength requirement that requires passwords to exceed a strength threshold according to neural-network-driven password-strength estimates.

Our results lead to concrete recommendations for policy configurations that produce a good balance of security and usability. In particular, for high-value user accounts we recommend policies that combine minimum-strength and minimum-length requirements. While we offer recommendations for organizations required to use blocklists, using blocklists does not provide further gains. Interestingly, we also find that against expert attackers, character-class requirements, traditionally associated with producing stronger passwords, in practice may provide very little improvement and may even reduce effective security.

1 INTRODUCTION
To help users create stronger passwords, system administrators often require passwords to exceed a certain length, contain at least a specific number of character classes, or not appear on a blocklist [19]. Users are also often nudged to create stronger passwords by password meters that give feedback on the strength of candidate passwords and suggestions about how to improve them.

Early guidance for how to deploy these approaches relied mostly on common sense and experts’ opinions [17, 18]. Over the past decade, a scientific basis has emerged for what requirements are most effective at encouraging users to create passwords that are strong but still memorable. For example, research has shown that increasing minimum length may increase password strength more than relying just on character class requirements [26]; that password meters can very effectively nudge users to create stronger passwords [28]; and that carefully configured blocklists can help prevent users from picking easily guessed passwords [8].

These early efforts shed light on which password requirements were more or less effective, but stopped short of providing empirically evaluated, definitive guidance for how to combine requirements. In this paper, we seek to address this. Building on
Users cope with lots of passwords by reusing them
Security Behavior Observatory

- Network of instrumented home Windows computers
- ~200 active participants
- Natural observation + surveys and interviews
- Data includes hashed passwords
People reuse their passwords a lot

On average, participants had

• 26 different accounts
• 10 distinct passwords
People reuse their passwords a lot

On average, participants had

- 26 different accounts
- 10 distinct passwords

21% Not reused
12% Partially reused
16% Exactly reused
51% Partially and exactly reused

Lots of reuse across almost all categories of websites.
Attackers exploit password reuse

CRACKED PASSWORDS

UserID       Password
jane         iloveyou89
jami         godoggo!
jim          monkey1
kar           pa$$word
katieprinc3ss2

Online Store
Bank
Employer
Users encouraged or required to change their passwords frequently
PASSWORDS ARE LIKE UNDERPANTS

Change them often, keep them private and never share them with anyone.
Why require password changes?

Lock out attackers who have learned users’ passwords
Testing this theory at UNC

- Mandatory password change every 3 months
- Researchers obtained and cracked hashed defunct passwords to 7,700+ accounts
Knowing old password can we predict new one?

Researchers tried to guess new passwords by making small changes to old passwords.
Predictable transformations
Predictable transformations

**Capitalization:** \( \text{tarheels}\#1 \rightarrow \text{tArheels}\#1 \)

**Substitution:** \( \text{tarheels}\#1 \rightarrow \text{tarheels}\#2 \)

**Keyboard transform:** \( \text{tarheels}\#1 \rightarrow \text{tarheels}\#! \)

**Date:** \( \text{tarheel}\#0510 \rightarrow \text{tarheel}\#0810 \)
Knowing prior passwords helps predict next one

- Online attack
  - 17% of accounts cracked within 5 guesses
- Offline attack
  - 41% of accounts cracked within 3 seconds on a 2.67GHz processor

Zhang, Monrose, and Reiter, CCS 2010
Time to rethink mandatory password changes

By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

TAGS: Authentication | Human-computer interaction | Passwords | Research

Data security is a process that evolves over time as new threats emerge and new countermeasures are developed. The FTC's longstanding advice to companies has been to conduct risk assessments, taking into account factors such as the sensitivity of information they collect and the availability of low-cost measures to mitigate risks. The FTC has also advised companies to keep abreast of new technologies and trends to identify and mitigate emerging threats.
The problems with forcing regular password expiry

Version: 1
Created: 11 April 2016
Updated: 15 April 2016
Topics: Passwords, Best Practice

Why CESG decided to advise against this long-established security guideline

Related Content
June 2017: NIST recommends against regular password expiry
2FA and password managers can improve password security, but adoption is low
Carnegie Mellon University

Web Login

AndrewID
Password
Login

Device: Mobile 1+3 (XXX-XXX-8412)

Choose an authentication method

- Duo Push RECOMMENDED
- Passcode

Send Me a Push
Enter a Passcode

Remember me for 30 days

What is this? Need help?
Collected data on 2FA rollout at CMU

- Surveyed ~1,200 people 1-3 weeks before mandatory adoption deadline
- Surveyed ~800 people 3 months after deadline
- Helpdesk and access log data

Students perceive 2FA more negatively than faculty and staff

“Remember me” feature doesn’t work in labs
New users need convincing

Why should I?
“Nothing a CMU student can access on the network is private or important enough to warrant this inane policy.”

My friends hate it
“I have heard it is a complete hassle and people regret doing it.”
But it turns out to be not so bad

“I previously assumed it would be more of a pain than it was worth. It's not actually that horrible.”
YOU NEED A PASSWORD MANAGER. HERE ARE SOME GOOD FREE ONES
Why are password manager (and generator) adoption rates so low?

- Lack of awareness
- Underestimate risk of password reuse
- Overestimate risk of password manager compromise
- Confusing prompts
- Usability and reliability problems

Users of built-in password managers may be driven more by convenience, while users of separately installed tools appear more driven by security

Privacy and transparency

- Privacy policies and nutrition labels
- Online tracking icons
- Cookie consent banners
Privacy and transparency

- Privacy policies and nutrition labels
- Online tracking icons
- Cookie consent banners
About Our Privacy Policy

Whenever you do something like buy one of our products, watch a video, or enter information is created. Because we know your privacy is important to you, we have created this Privacy Policy to explain how we collect, use and protect that information. There is more information available in the FAQ format (https://privacy_policy/terms). We want to simplify, make informed choices about your privacy, and then spend the rest of our time focusing on products and services.

Effective July 24, 2016

A Quick Summary of Our Privacy Policy

Our Privacy Policy applies to your use of all products, services, and our AT&T affiliates, such as DIRECTV, unless they have their own separate privacy policy. Because some apps, including some AT&T and DIRECTV branded apps, store or collect information, or use information in different ways, they may have their own privacy policies and/or terms and conditions. These apps may also ask you to provide additional information related to your personal information.

Back to Top

Our privacy commitments

- We don’t sell your Personal Information to anyone for any reason.
- We keep your Personal Information in our business records until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.
244 HOURS PER YEAR

“ONLY IN SOME FANTASY WORLD do users actually read these notices and understand their implications before clicking to indicate their consent”

— United States President’s Council of Advisors on Science and Technology, Big Data and Privacy, May 2014
How can we put people in control over their personal information?

And how do we know when we have succeeded?
By what criteria should we measure effectiveness?

Notice the notice?

Stop and read?

Understand?

Useful information?

Impact behavior?
Important to test, even on low budget
Test comprehension in context
Towards a privacy “nutrition label”

- Standardized format
  - People learn where info is
  - Facilitates policy comparisons
- Standardized language
  - People learn terminology
- Brief
  - People find info quickly
- Linked to extended view
  - Get more details if needed
### cups.cs.cmu.edu/privacyLabel/


<table>
<thead>
<tr>
<th><strong>information we collect</strong></th>
<th><strong>ways we use your information</strong></th>
<th><strong>information sharing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>provide service and maintain site</td>
<td>marketing</td>
</tr>
<tr>
<td>contact information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>cookies</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>demographic information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>financial information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>health information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>preferences</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>purchasing information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>social security number &amp; gov't ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>your activity on this site</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>your location</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Facts
#### What Does Bank of America Do with Your Personal Information?

**Why?**
Financial companies choose how they share your personal information. Under federal law, financial companies, like Bank of America, are required to tell you how we collect, share, and protect your personal information. Please read this notice to understand what we do.

**What?**
The types of personal information we collect and share depend on the products or services you have with us. The information can include:
- Social security number and employment information
- Account balances, transaction history and credit information
- Assets and investment experience

**How?**
All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information.

#### Reasons We Can Share Your Personal Information

<table>
<thead>
<tr>
<th>Reasons We Can Share Your Personal Information</th>
<th>Does Bank of America Share?</th>
<th>Can You Limit This Sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus</td>
<td>Yes, No</td>
<td>No</td>
</tr>
<tr>
<td>For our marketing purposes — with service providers we use to offer our products and services to you (please see below to limit when we contact you)</td>
<td>Yes, No</td>
<td>No</td>
</tr>
<tr>
<td>For joint marketing with other financial companies</td>
<td>Yes, No</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes — Information about your transactions and experiences</td>
<td>Yes, Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes — Information about your creditworthiness</td>
<td>Yes, Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>For nonaffiliates to market to you — for accounts and services offered by other organization (e.g., retail bank or credit card)</td>
<td>No, Yes</td>
<td>No, We don't share</td>
</tr>
<tr>
<td>For nonaffiliates to market to you — for accounts other than credit card accounts and sponsored accounts, such as insurance, investments, deposits and loans</td>
<td>No, Yes</td>
<td>No, We don't share</td>
</tr>
</tbody>
</table>

#### Questions?
Call 1-800-381-0740 or go to: http://www.cit.com/utility/privacy-policy/index.html

---

### Facts
#### What Does CIT Group Inc. ("CIT") Do with Your Personal Information?

**Why?**
Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice to understand what we do.

**What?**
The types of personal information we collect and share depend on the products or services you have with us. This information can include:
- Social Security Number and income
- Account balances and transaction history
- Credit history and credit scores

When you are no longer our customer, we continue to share your information as described in this notice.

**How?**
All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons CIT chooses to share; and whether you can limit the sharing.

#### Reasons We Can Share Your Personal Information

<table>
<thead>
<tr>
<th>Reasons We Can Share Your Personal Information</th>
<th>Does CIT Share?</th>
<th>Can You Limit This Sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our marketing purposes — to offer our products and services to you</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For joint marketing with other financial companies</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes — Information about your transactions and experiences</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For our affiliates' everyday business purposes — Information about your creditworthiness</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>For nonaffiliates to market to you</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Questions? Call 1-800-381-0740 or go to: http://www.cit.com/utility/privacy-policy/index.html
Android Privacy Facts

• Task: select apps for friend with new smartphone
  • Choose from 2 similar apps w/ different permission requests
• Participants who saw Privacy Facts more likely to select apps with fewer permissions
  • Brand and rating reduce effect

P.G. Kelley, L.F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. CHI 2013.
Apple will require apps to add privacy 'nutrition labels' starting December 8th

The labels explain what data is collected at a glance

By Ian Carlos Campbell | @soupsthename | Nov 5, 2020, 8:42pm EST
Privacy & Security Facts

<table>
<thead>
<tr>
<th>Security Camera S200</th>
<th>Smart++, Incorporated in United States 2017</th>
<th>Firmware version 3.1.6 (updated June 12, 2016)</th>
</tr>
</thead>
</table>

**PRIVACY**

- **Collected data:** Video, device configuration, login info
- **Purpose:** Security, maintenance, advertisement
- **Retention time:** Forever
- **Shared with:** Manufacturer
- **Choices:** None
- **Independent Privacy Lab Rating:** ★★★★★
- **Level of detail for the data that is being used:** Identifiable
- **Level of detail for the data that is being collected:** Identifiable

**SECURITY**

- **Automatic updates:** No
- **Updates lifetime:** Until January 1, 2020
- **Choices:** Configurable updates, purchase extended updates
- **Encrypted communication:** Yes
- **Authentication method:** Fingerprint
- **Internet connectivity:** Required
- **Independent IT Security Institute Rating:** ★★★★★

---

Privacy and transparency

- Privacy policies and nutrition labels
- Online tracking icons
- Cookie consent banners
LAWRENCEVILLE, GA—Expressing her growing unease at repeatedly spotting the same picture and text lurking in the corners of her favorite webpages, local woman Laura Spelman confirmed Monday that she has been stalked across eight different sites by an obsessed Nine West shoe advertisement. “When I first saw the ad for the black ballet flats in my Facebook news feed, it seemed harmless enough, but then I went to check the forecast on Weather.com and it was waiting there for me—it’s really kind of disturbing,” said Spelman, adding that she has taken to scrolling away from the fanatical ad as fast as possible whenever she catches sight of it. “I hope they get the message that I have no interest in the product.”
Merrell Encore Mid Boot Q2 Women's Boots

$149.95

UGG Niels Women's Boots

$194.95

Rieker Z6784 Women's Dress Boots

$120

Born Kristina Women's Pull-on Boots

$135
Do people recognize the AdChoices icon?

1,505-participant online survey

Varied icon and taglines

- Why did I get this ad?
- Interest based ads
- AdChoices
- Sponsor ads
- Learn about your ad choices
- Configure ad preferences
- ‘No tagline’
What would happen if you clicked on the icon?

AdChoices

56%  More ads will pop up

45%  Will take you to a page where you can buy advertisements on this website

27%  Will take you to a page where you can opt out of tailored ads

% who agreed with each statement; some participants agreed with multiple statements
What would happen if you clicked on the icon?

**Configure Ad Preferences**

- More ads will pop up (56%)
- Will take you to a page where you can buy advertisements on this website (45%)
- Will take you to a page where you can opt out of tailored ads (27%)

% who agreed with each statement; some participants agreed with multiple statements
CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

PROPOSED TEXT OF REGULATIONS

§ 999.315. Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form.

(e) Opt-Out Button or Logo

(1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]
Choice/consent

Opting out

Do not sell (personal info)

DAA Privacy Rights
Refined icons for evaluation

ID-Card  Slash-Dollar  Stop-Dollar  Toggle  DAA
Combo testing

• Mturk study with 1,416 participants
• Tested 3 icons + no icon
  ✔️ ✗ ☹️ ➕
• Tested 5 taglines + no tagline
  • Do not sell my personal information
  • Do not sell my info
  • Privacy choices
  • Privacy options
  • Personal info choices
• 23 combinations tested
OAG’s revised proposed regulations

(1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.

(2) When the opt-out button is used, it shall appear to the left of the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link, as demonstrated below, and shall be approximately the same size as other buttons on the business’s webpage. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]

- Do Not Sell My Personal Information
- Do Not Sell My Info
So we ran another study

- Insignificant difference between icons with the big and small X
- But big differences between the CalAG icon and our stylized toggle
- CalAG icon more likely to be misinterpreted as actual toggle
- Small differences based on color
- Some small changes can sometimes make a big difference and you won’t know unless you test with users
Then the OAG removed the button

- Button completely removed from regulation
- OAG will design a uniform and recognizable opt-out button in the future

Former subsection (f), regarding the proposed opt-out button, has been deleted in response to the various comments received during the public comment period. The OAG has removed this subsection in order to further develop and evaluate a uniform opt-out logo or button for use by all businesses to promote consumer awareness of how to easily opt-out of the sale of personal information.
Then the OAG asked us to test more icons!

- Which of these icons, paired with the “Do Not Sell My Personal Information” link text performs best
  - standing out to users on a website?
  - communicating the presence of a do-not-sell choice?
  - motivating users to click?
- ... and only recruit participants from CA
Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act

Monday, March 15, 2021
Contact: (916) 210-6000, agpressoffice@doj.ca.gov

Includes new Privacy Options icon that businesses are encouraged to use to help build consumer awareness of Californians’ privacy rights

SACRAMENTO – California Attorney General Xavier Becerra today announced additional regulations approved by the Office of Administrative Law that advance protections for Californians seeking to control the sale of their personal information. The California Consumer Privacy Act (CCPA) gives consumers new tools and rights for protecting their data privacy. These newly-approved rules strengthen the language of the CCPA regulations approved by OAL in August 2020, including protecting consumers from unlawful business practices that may be deceptive or misleading.

Read more at cups.cs.cmu.edu/optout
Privacy and transparency

- Privacy policies and nutrition labels
- Online tracking icons
- Cookie consent banners
What makes a consent interface useable?

• Addresses user needs
• Requires minimal user effort
• Makes users aware of what choices exist and where to find them
• Conveys choices and their implications so users understand them easily (comprehension)
• Users are satisfied with interface and choice options, trust their choices will be honored (sentiment)
• Allows users to change their decision due to errors or changing their mind (decision reversal)
• Doesn’t nudge users towards less privacy-protective options
Common usability problems with cookie banners

- Nudge users to accept all cookies by presenting that option as a big button
- Require extra steps to make other choices – first you have to click through to cookie settings
- It’s not even clear what the other choices are without clicking through

Cookie consent

We use our own and third-party cookies to show you more relevant content based on your browsing and navigation history. Please accept or manage your cookie settings below. Here’s our cookie policy.
Hana Habib, Megan Li, Ellie Young, Lorrie Faith Cranor

Paper to be presented at CHI 2022

“Okay, whatever”: An Evaluation of Cookie Consent Interfaces
Evaluating the impact of design parameters on the usability of cookie consent interfaces

• Inspection evaluation
  • Reviewed ~200 cookie consent banners from 5 CMPs
  • Checked for dark patterns and found them on 88% of banners (most common: easiest option is to accept all cookies)
  • Identified key design parameters

• User study
  • Tested 12 cookie consent design variants with users, evaluating 6 usability factors
Recruited 1,316 crowd workers from Prolific

- Participants assigned website shopping task
  - Select item and put it in your shopping cart
- Exposed to 1 of 12 consent interface variants
- Asked to fill out survey
- Asked to review consent interface again and answer more survey questions
- Median completion time ~16 min, compensation $5.00
- Analyzed interactions and survey responses from 1,109 participants
  - Where they clicked, consent choices made, time spent, etc.
“Best-practices” variant

This website uses cookies

- Why we use cookies: To enhance site performance, personalize your experience, and deliver interest-based ads
- Your choices: Some cookies are optional. Click ‘Allow all cookies’ to accept all cookies, or edit your cookie preferences below and select ‘Allow
- Updating preferences: Click on the ‘Cookie Preferences’ button on the bottom right corner of this website
- More information: Please see our Privacy Policy

![Cookie Preferences interface]

- Reversal through persistent “cookie preferences” button
- Fully-blocking design
- Detailed button text
- Single-layer “Cookie Preferences” interface

Bulleted text
In-line options available
This website uses cookies

- **Why we use cookies:** To enhance site performance, personalize your experience, and deliver interest-based ads.
- **Your choices:** Some cookies are optional. Click 'Allow all cookies' to accept all cookies, or edit your cookie preferences below and select 'Allow'.
- **Updating preferences:** Click on the 'Cookie Preferences' button on the bottom right corner of this website.
- **More information:** Please see our Privacy Policy.

**Allow selected cookies**  **Allow all cookies**

- Strictly necessary
- Performance
- Functional
- Targeting

Show details
“Worst-practices” variant

Banner design at bottom of page

Loss aversion text

This website uses cookies
We use cookies to make the website work properly, enhance performance, create personalized functionality, and deliver targeted ads. Note that if you do not accept optional cookies, your experience may be affected. By continuing to use this site you agree to the use of cookies as shown in your cookie preferences. You may update your cookie preferences at any time. For more information, please see our Privacy Policy.

Okay

Embedded link to multi-layer interface

Generic button text

Decision reversal not mentioned

Paragraph text
“Corner button” variant

Cookie preferences

Single-layer “Cookie Preferences” interface
ALL OF THE CUPS.

Our biggest restock ever.
Use code SUMMER21 for 21% off all cold cups.
Some variables impacted consent decisions, others not so much

Changes to paragraph or button text didn’t have much impact

Participants more likely to consent to all cookies without inline options

Inline options led users to restrict cookies

Non blocking interfaces led many users to skip making a consent decision!
Absence of fully-blocking or banner notice led to poor awareness

- No participants interacted with the Cookie Preferences button
- Less awareness of a privacy decision & available cookie options compared to best-practices
Absence of in-line options led to lower investment in decision-making

More likely to choose “easiest option” and “not at all carefully” on survey compared to *best-practices*
But... absence of in-line options led to higher focused comprehension scores

Perhaps because participants who had in-line options available didn’t drill down to cookie preferences screens with definitions.
Persistent “Cookie Preferences” button enabled decision reversal

- **82%** of *best-practices* participants said they would use the button to change their decision
  - Only **45%** of participants who saw a link to cookie policy but no button said they would visit the cookie policy to change their decision
- No significant impact due to absence of reversal instruction text
Standard cookie categories cause confusion

• Performance cookies
  • Cookies that help measure and improve website features
  • Only 48% of participants selected correct definition

• Functional cookies
  • Cookies that help personalize the website’s services for you
  • Only 16% of participants selected correct definition

*Categories used by OneTrust and other CMPs are from ICC UK Cookie Guide*

The burden of user consent

• Considerable cost to reading cookie consent interfaces, comprehending available options, and making a decision at large numbers of websites

• Potential long-term solution: browser-based consent management
• Don’t assume you have to tradeoff security/privacy and usability
• Don’t ask people to do security tasks they aren’t good at
• Is it usable? Test with the people who will be using it
• Look for automated and standardized solutions that don’t rely on user effort
  • Standard icon and notice formats
  • Machine-readable notices and tools to search them and present useful information to users
  • Password managers so users can create random passwords and don’t have to remember them

Research discussed in this talk was funded in part by Carnegie Corporation of New York, Carnegie Mellon CyLab, DARPA, Facebook, Google, IBM, Microsoft Research, Innovators Network Foundation, NSA, NSF, PNC Center for Financial Services Innovation, and The Privacy Projects.