



Making Secure Systems Easy for the Public to Use

Lorrie Faith Cranor

lorrie.cranor.org

@lorrietweet





Security

Human error is the root cause of most data breaches

Financial damage of data leaks must be considered by firms

Markel Direct



ENDPOINT / MOBILE SECURITY

The Weakest Link: The Role of Human Error in Cybersecurity



CEOs in the News

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

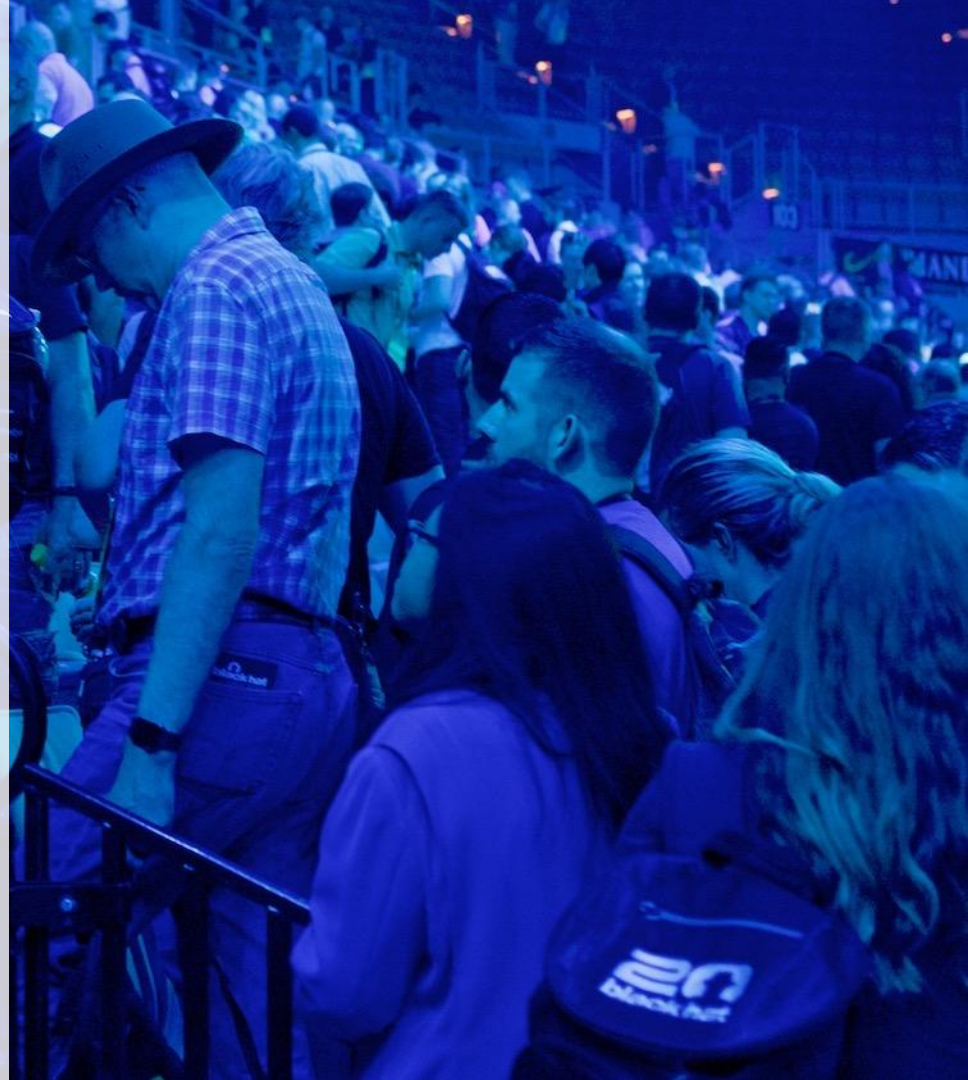
By **Ross Kelly** - March 3, 2017



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

The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations



SOCIAL MEDIA, SECURITY

Twitter's New Privacy Policy Means You Need to Change Your Settings



By Nancy Messieh / May 23, 2017 / 3 minutes

Advertisement

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:

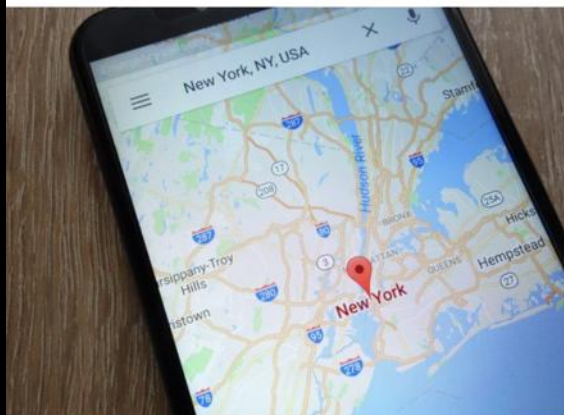


ENTERPRISE

Google clarifies its location tracking help page for confused users

by Ellen Tannam

17 AUG 2018 260 VIEWS



Google Maps on mobile device. Image: Piotr Swat/Shutterstock



BUSINESS



Facebook to make privacy settings less difficult to use

By Nicolas Vega

March 28, 2018 | 11:16am



AFP/Getty Images

Facebook said Wednesday it will finally simplify the notoriously confusing maze of privacy settings on its site.

The embattled social network — which previously sent users to more than a dozen different pages when they wanted to adjust the amount of data they shared, or see what third-party apps had access to their information — announced plans to consolidate those settings onto one central page.

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**



USENIX Security 1999

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
*School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu*


J. D. Tygar¹
*EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu*

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

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct



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



MISCONCEPTION

Adding ! to the end makes it secure

Password!

iloveyou!

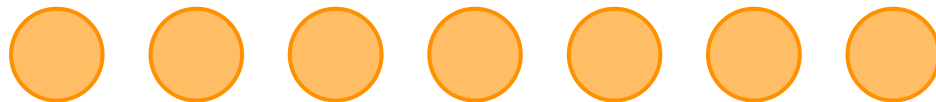
monkey!

Password perceptions study

iloveyou88

ieatkale88

iloveyou88
much more
secure



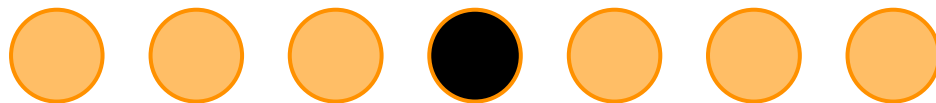
ieatkale88
much more
secure

Password perceptions study

i1oveyou88

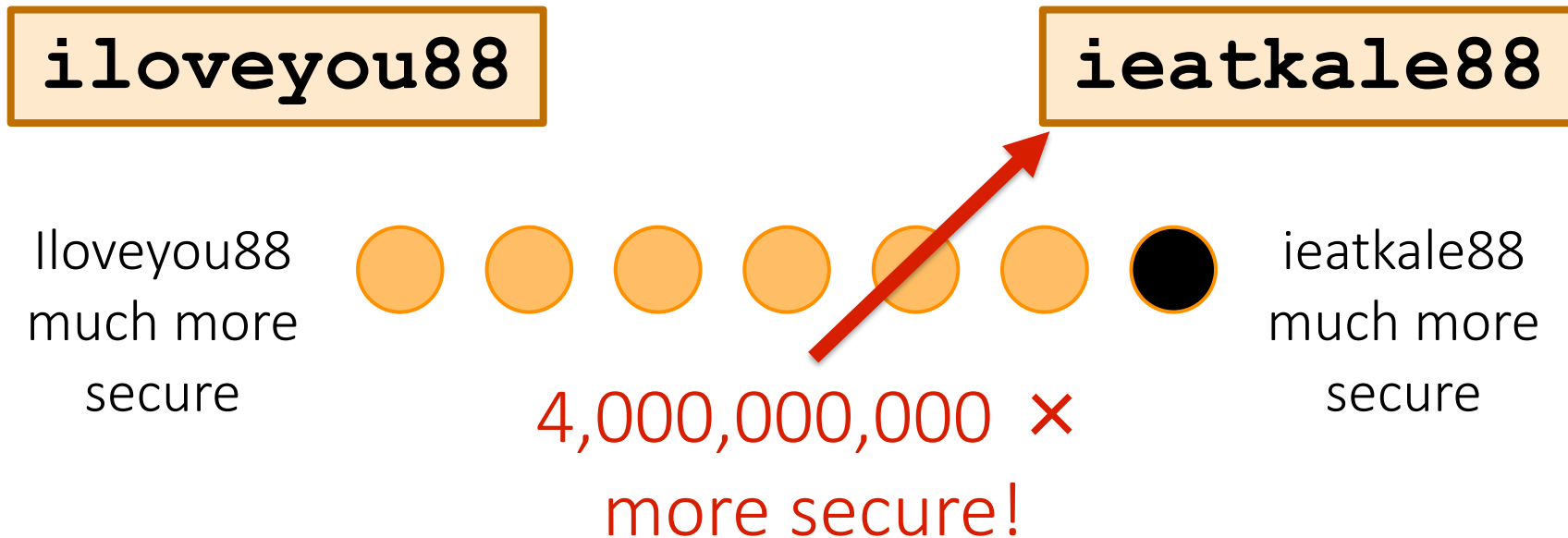
ieatkale88

lloveyou88
much more
secure



ieatkale88
much more
secure

Password perceptions study





Most password meters don't help much

Change your password

Strengthen the security of your account with a new password.

☐ show password

Continue

Cancel

Your password is weak,
create a stronger password.

Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback ☒

Confirm Password

Continue

Your password could be better.

- Don't use dictionary words (**Unicorn**) or words used on Wikipedia (**Crypto**) [\(Why?\)](#)
- Consider inserting digits into the middle, not just at the end [\(Why?\)](#)
- Consider making your password longer than 14 characters [\(Why?\)](#)

A better choice: **C3**ryptoUni**C**orn**@**

[How to make strong passwords](#)

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

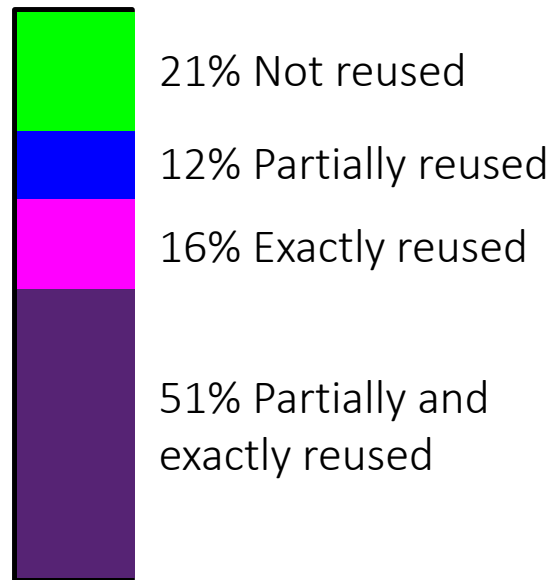
On average, participants had

- 26 different accounts
- 10 distinct passwords

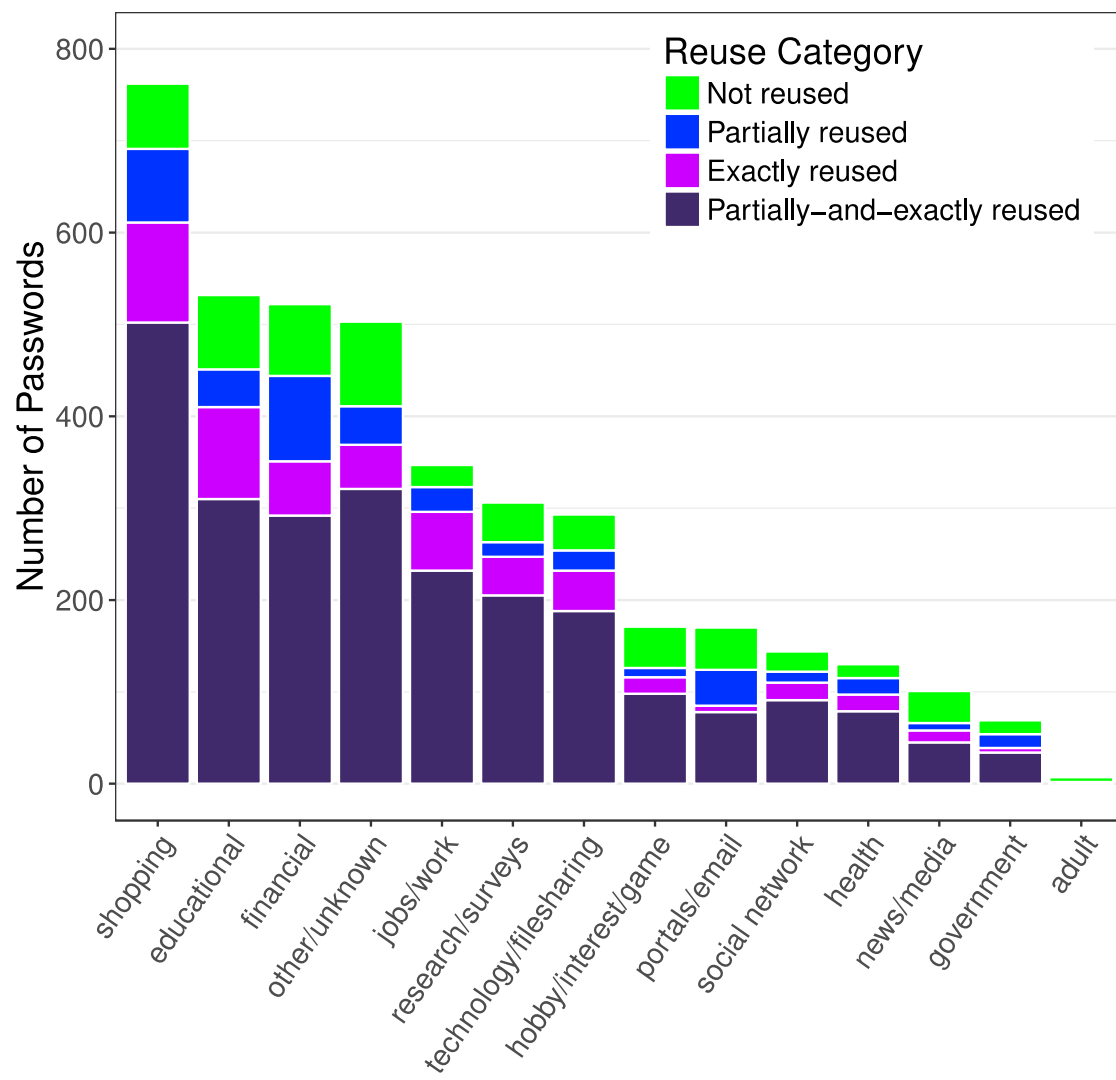
People reuse their passwords a lot

On average, participants had

- 26 different accounts
- 10 distinct passwords



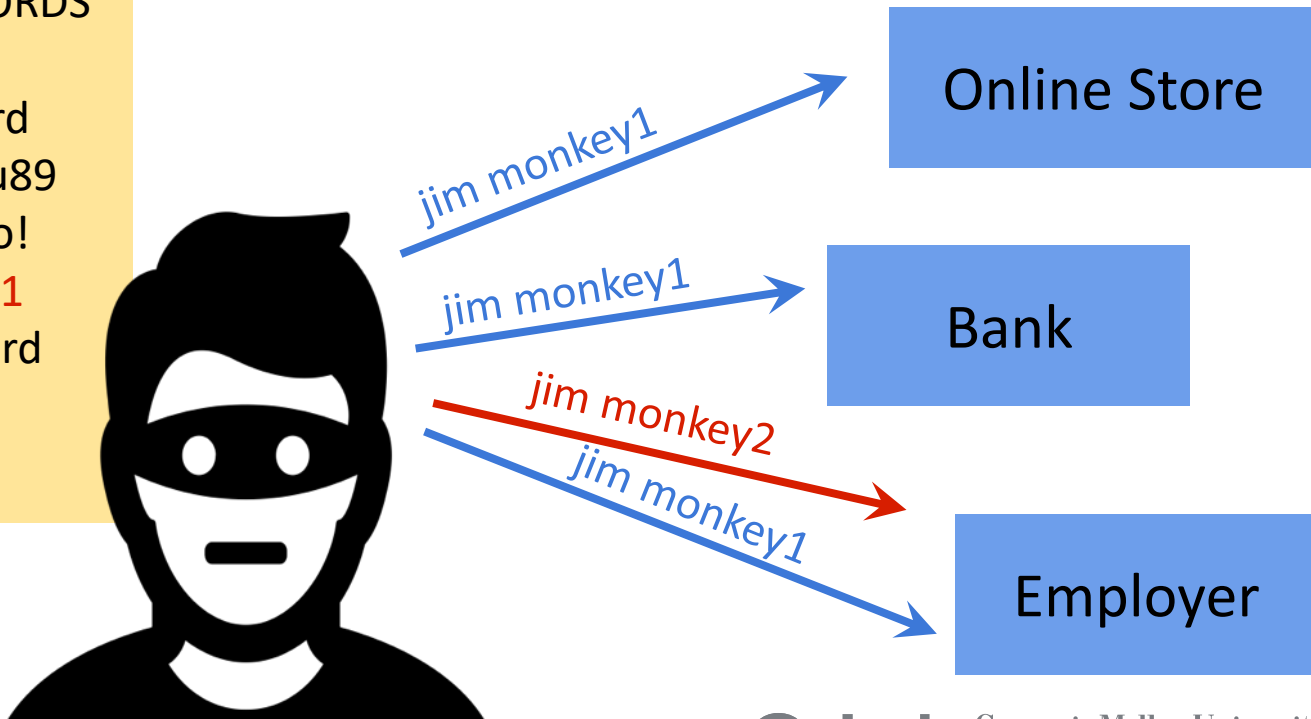
Lots of reuse
across almost all
categories of
websites



Attackers exploit password reuse

CRACKED PASSWORDS

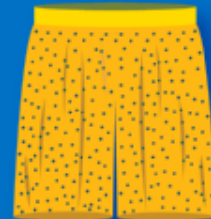
UserID	Password
jane	iloveyou89
jami	godoggo!
jim	monkey1
kar	pa\$\$word
katie	princ3ss2





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.

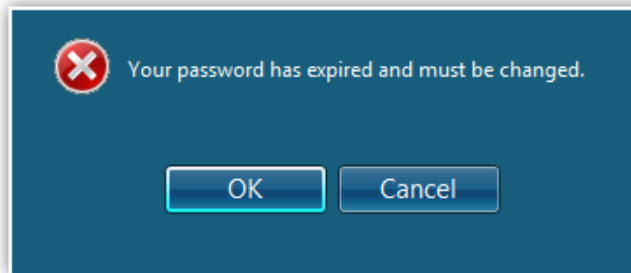
Why require password changes?

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: `tarheels#1` → `tArheels#1`

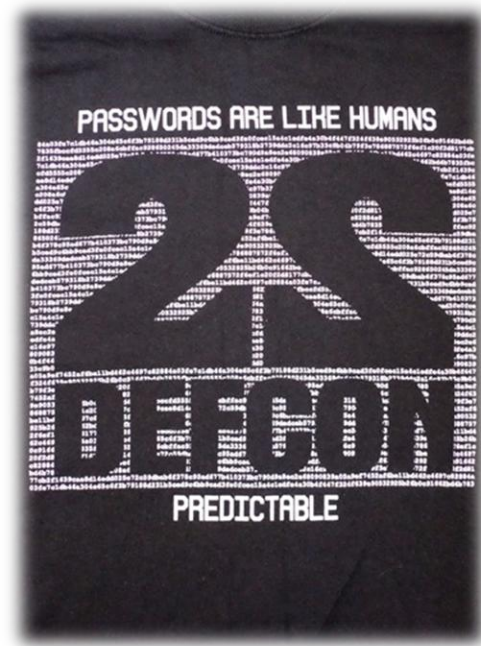
Substitution: `tarheels#1` → `tarheels#2`

Keyboard transform: `tarheels#1` → `tarheels#!`

Date: `tarheel#0510` → `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





Time to rethink mandatory password changes

TAGS: [Authentication](#) | [Human-computer interaction](#) | [Passwords](#) | [Research](#)

Research (6)

[Home](#) > [About Us](#) > [IA Matters](#)

The problems with forcing regular password expiry

Version: 1

Created: 11 April 2016

Updated: 15 April 2016

Topics: [Passwords](#), [Best Practice](#)

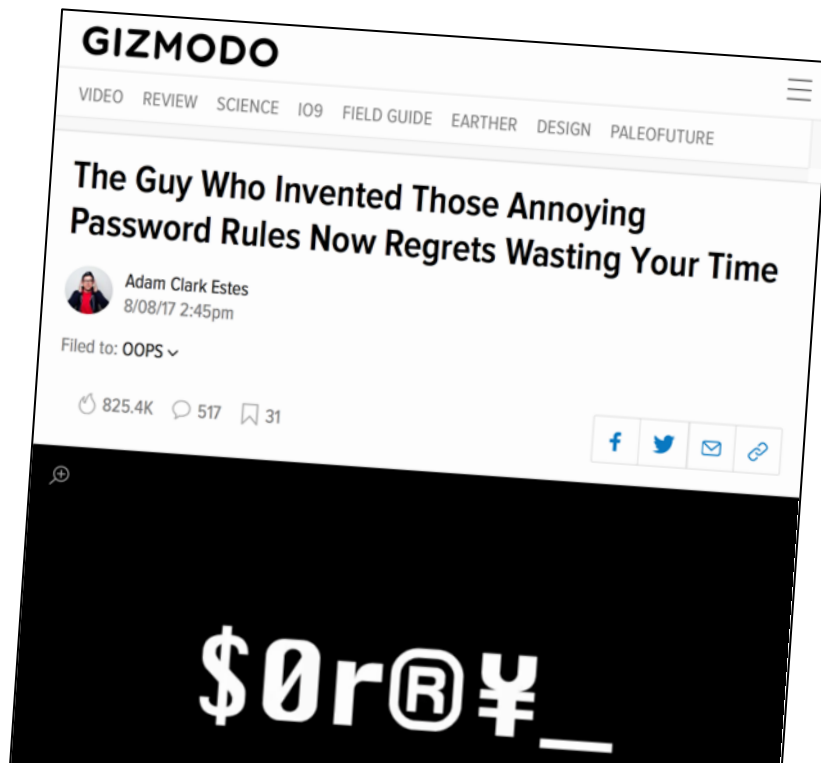
Share this page


 [LinkedIn](#)  [Facebook](#)  [Twitter](#)  [Google+](#)

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

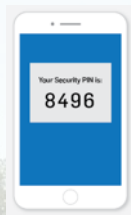
Related Content

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



**Carnegie
Mellon
University**

[What is this?](#)

[Need help?](#)

Device: Mobile 1+3 (XXX-XXX-8412) ▼

Choose an authentication method



DUO Push RECOMMENDED

Send Me a Push

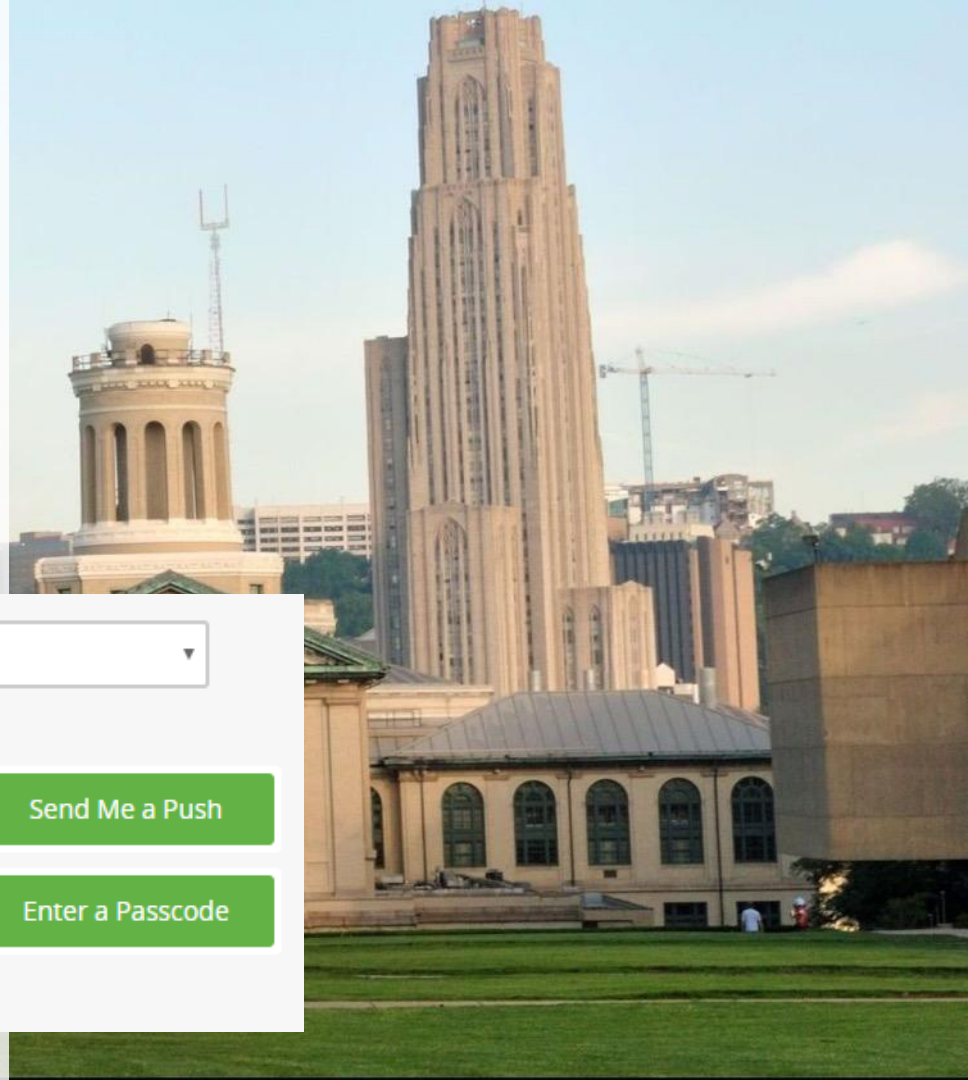


Passcode

Enter a Passcode



Remember me for 30 days



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



VS



“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.”



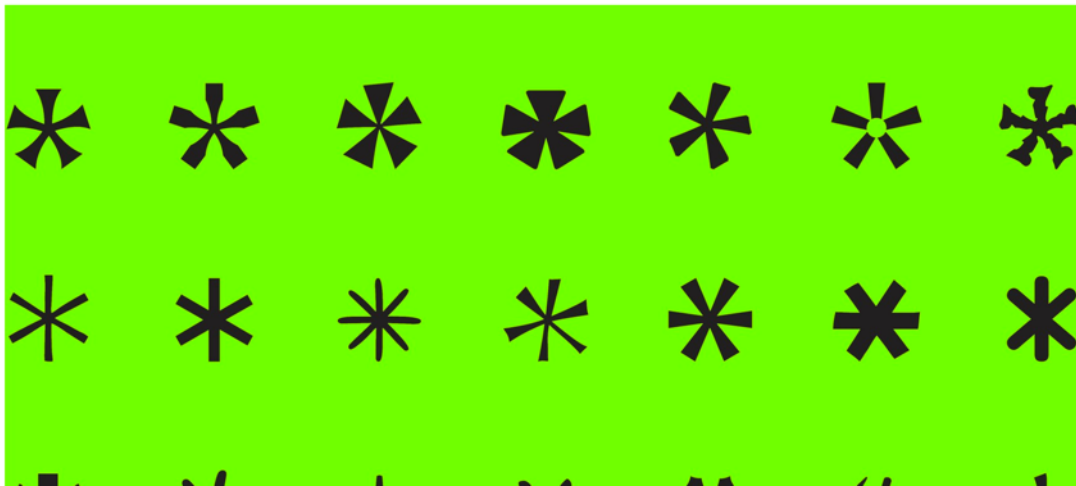
But it turns out to be not so bad

“I previously assumed it would be more of a pain than it was worth. It's not actually that horrible.”



APRIL GLASER GEAR 01.24.16 7:00 AM

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



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

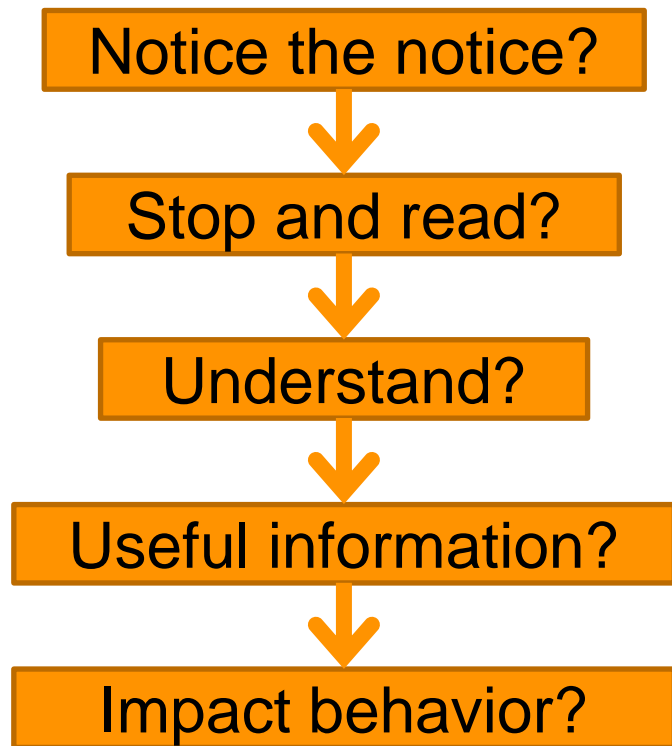


How can we put people in control over their personal information?

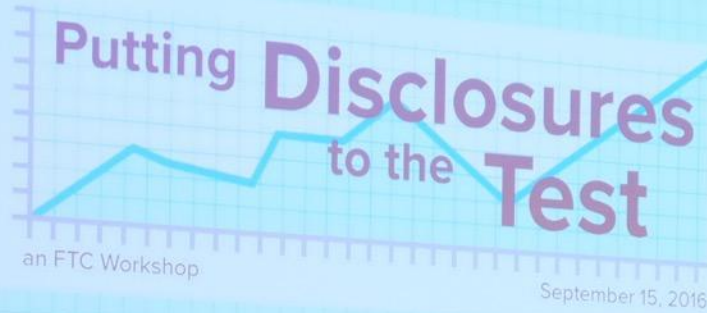
And how do we know
when we have
succeeded?



By what criteria should we measure effectiveness?



ftc.gov/testingdisclosures



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

Privacy Facts

Privacy Facts

information we collect

ways we use your information

information sharing

	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out		opt out	opt in
cookies		opt out	opt out			
demographic information		opt out	opt out			
financial information						
health information		opt out	opt out			
preferences		opt out	opt out			opt in
purchasing information		opt out	opt out			opt in
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

cups.cs.cmu.edu/privacyLabel/

P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder. A “Nutrition Label” for Privacy. SOUPS 2009.

P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CHI2010.

FACTS	WHAT DOES BANK OF AMERICA DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Under federal law, that means personally identifiable 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 carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none"> • 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; the reasons Bank of America chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Bank of America share?	Can you limit this sharing?
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	Yes	No
For our marketing purposes — with service providers we use to offer our products and services to you (please see below to limit the ways we contact you)	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes — Information about your transactions and experiences	Yes	Yes
For our affiliates' everyday business purposes — Information about your creditworthiness	Yes	Yes
For nonaffiliates to market to you — for all credit card accounts	Yes	Yes
For nonaffiliates to market to you — for accounts and services endorsed by another organization (e.g., debit card co-branded with a baseball team) *Sponsored Accounts*	Yes	Yes
For nonaffiliates to market to you — for accounts other than credit card accounts and Sponsored Accounts, such as insurance, investments, deposit and lending	No	We don't share

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 carefully to understand what we do.
What?	The types of personal information we collect and share depends on the product or service you have with us. This information can include: <ul style="list-style-type: none"> • 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 this sharing.

Reasons we can share your personal information	Does CIT share?	Can you limit this sharing?
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	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions? Call: 1-800-681-0740 or go to: <http://www.cit.com/utility/privacy-policy/index.htm>

cups.cs.cmu.edu/bankprivacy/

BANK PRIVACY

We've collected 6,326 banks' privacy notices. See how your bank stacks up...

Look up a bank

...or find banks in your ZIP code...

Enter ZIP code

...or search for a privacy-protective bank.

Characteristic: **ANY**

Specialization: **ANY**

Size: **ANY**

Headquarters: **ANY**

Search for such a bank

Own marketing: **ANY**

Joint marketing: **ANY**

Affiliates (transactions): **ANY**

Affiliates (creditworthiness): **ANY**

Affiliates' marketing: **ANY**

Nonaffiliates' marketing: **ANY**

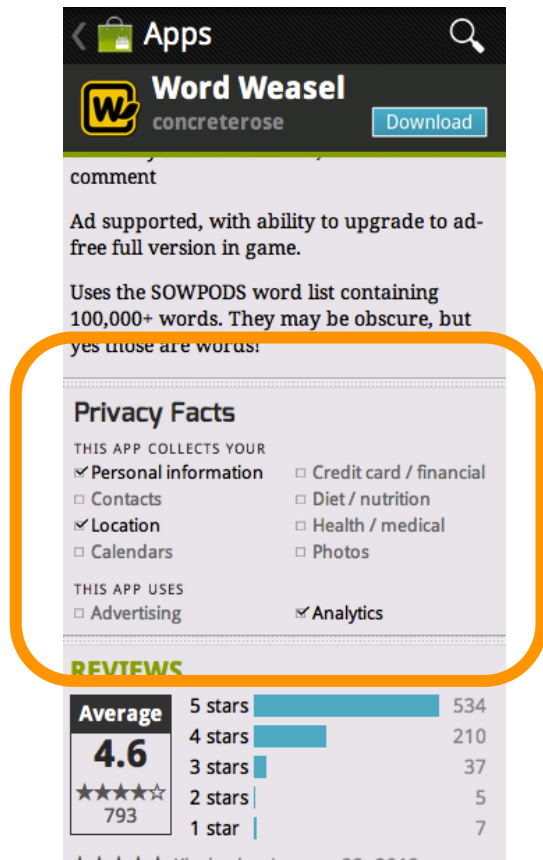
Bank Privacy: About

The following 96 banks meet your criteria:

Institution	Location	Everyday business	Our marketing	Joint marketing	Affiliates: trans...	Affiliates: credit...	Affiliates: mark
Pacific Coast Bankers Bank	Walnut Creek, CA						
1st Capital Bank	Monterey, CA						
Community 1st Bank	Auburn, CA						
Golden State Bank	Upland, CA						
Pacific Coast Bankers Bancshares	Walnut Creek, CA						
American Continental Bank	City Of Industry, CA						
Uniti Bank	Buena Park, CA						
Orange County Business Bank	Irvine, CA						
Presidio Bank	San Francisco, CA						
1st Enterprise Bank	Los Angeles, CA						
Security First Bank	Fresno, CA						
Uniti Financial Corporation	Buena Park, CA						
California Center Credit Union	Ontario, CA						
EH National Bank	Beverly Hills, CA						
Commerciwest Bank	Newport Beach, CA						
Heritage Oaks Bank	Paso Robles, CA						
Open Bank	Los Angeles, CA						
49er Credit Union	Placerville, CA						
Royal Business Bank	Los Angeles, CA						
FNB Bancorp	South San Francisco, CA						
Folsom Lake Bank	Folsom, CA						

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

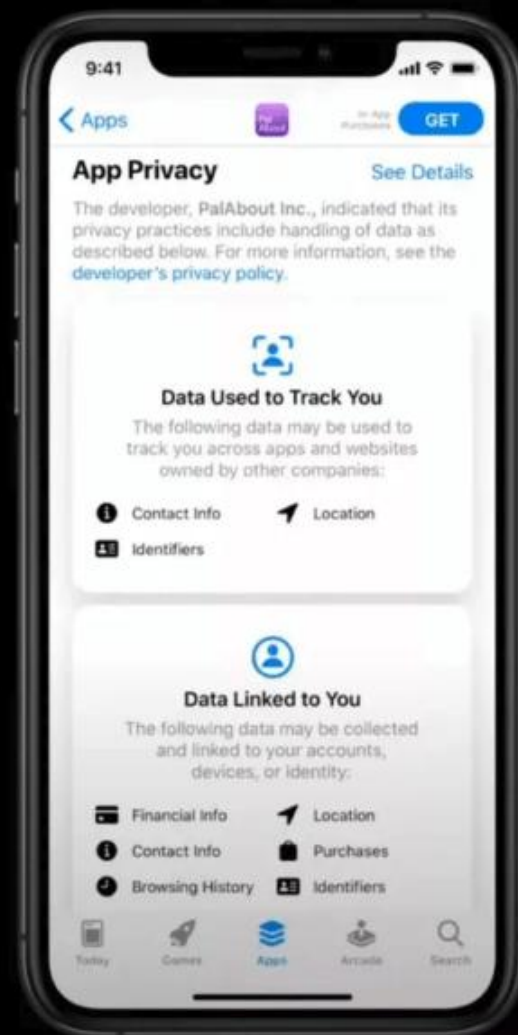


Apple will require apps to add privacy 'nutrition labels' starting December 8th

The labels explain what data is collected at a glance

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

f t  SHARE



Privacy & Security Facts

Security Camera S200

Smart++, incorporated in United States 2017
Firmware version 3.1.6 (updated June 12, 2018)

CR Consumer Reports

55

Overall score out of 100



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: ★★☆☆☆

MORE INFORMATION

Tip(s): Register your device to receive updates

Scan QR code for manufacturer's privacy and security information



P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. CHI 2019.


















Security & Privacy Overview

Smart Device Co.

Smart Video Doorbell NS200

Firmware version: 2.5.1 - updated on: 11/12/2020

The device was manufactured in: China

	Security Mechanisms	<table><tr><td>Security updates</td><td>Automatic - Available until at least 1/1/2022</td></tr><tr><td>Access control</td><td>Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed</td></tr></table>	Security updates	Automatic - Available until at least 1/1/2022	Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed																																									
Security updates	Automatic - Available until at least 1/1/2022																																														
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed																																														
	Data Practices	<table><tr><td>Sensor data collection</td><td> Visual</td><td> Audio</td><td> Physiological</td><td> Location</td></tr><tr><td>Sensor type</td><td></td><td>Microphone</td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td><td></td></tr><tr><td>Data stored on device</td><td></td><td></td><td></td><td></td></tr><tr><td>Data stored on cloud</td><td></td><td>Identified - Option to delete</td><td></td><td></td></tr><tr><td>Shared with</td><td></td><td>Manufacturer</td><td></td><td></td></tr><tr><td>Sold to</td><td>Not disclosed</td><td>Not sold</td><td></td><td></td></tr><tr><td>Other collected data</td><td colspan="4">Motion, Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr><tr><td>Privacy policy</td><td colspan="4">www.NS200.smartdeviceco.com/policy</td></tr></table>	Sensor data collection	 Visual	 Audio	 Physiological	 Location	Sensor type		Microphone			Purpose					Data stored on device					Data stored on cloud		Identified - Option to delete			Shared with		Manufacturer			Sold to	Not disclosed	Not sold			Other collected data	Motion, Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info				Privacy policy	www.NS200.smartdeviceco.com/policy			
Sensor data collection	 Visual	 Audio	 Physiological	 Location																																											
Sensor type		Microphone																																													
Purpose																																															
Data stored on device																																															
Data stored on cloud		Identified - Option to delete																																													
Shared with		Manufacturer																																													
Sold to	Not disclosed	Not sold																																													
Other collected data	Motion, Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info																																														
Privacy policy	www.NS200.smartdeviceco.com/policy																																														
	More Information	<p>Detailed Security & Privacy Label:</p> <p>www.iotsecurityprivacy.org/featured/external/manufacture/Smart/Video-Doorbell</p> 																																													
CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org																																															
																																															















Security & Privacy Details

Smart Device Co.

Smart Video Doorbell NS200

Firmware version: 2.5.1 - updated on: 11/12/2020

The device was manufactured in: China

	Security Mechanisms	<table><tr><td>Security updates</td><td>Automatic - Available until at least 1/1/2022</td></tr><tr><td>Access control</td><td>Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed</td></tr><tr><td>Security oversight</td><td>No security audits</td></tr><tr><td>Ports and protocols</td><td>www.NS200.smartdeviceco.com/ports</td></tr><tr><td>Hardware safety</td><td>Not disclosed</td></tr><tr><td>Software safety</td><td>www.NS200.smartdeviceco.com/sw_safety</td></tr><tr><td>Personal safety</td><td>www.NS200.smartdeviceco.com/user_safety</td></tr><tr><td>Vulnerability disclosure and management</td><td>www.NS200.smartdeviceco.com/vul_report</td></tr><tr><td>Software and hardware composition list</td><td>www.NS200.smartdeviceco.com/BOM</td></tr><tr><td>Encryption and key management</td><td>www.NS200.smartdeviceco.com/encryption</td></tr></table>	Security updates	Automatic - Available until at least 1/1/2022	Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed	Security oversight	No security audits	Ports and protocols	www.NS200.smartdeviceco.com/ports	Hardware safety	Not disclosed	Software safety	www.NS200.smartdeviceco.com/sw_safety	Personal safety	www.NS200.smartdeviceco.com/user_safety	Vulnerability disclosure and management	www.NS200.smartdeviceco.com/vul_report	Software and hardware composition list	www.NS200.smartdeviceco.com/BOM	Encryption and key management	www.NS200.smartdeviceco.com/encryption																																																													
Security updates	Automatic - Available until at least 1/1/2022																																																																																		
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed																																																																																		
Security oversight	No security audits																																																																																		
Ports and protocols	www.NS200.smartdeviceco.com/ports																																																																																		
Hardware safety	Not disclosed																																																																																		
Software safety	www.NS200.smartdeviceco.com/sw_safety																																																																																		
Personal safety	www.NS200.smartdeviceco.com/user_safety																																																																																		
Vulnerability disclosure and management	www.NS200.smartdeviceco.com/vul_report																																																																																		
Software and hardware composition list	www.NS200.smartdeviceco.com/BOM																																																																																		
Encryption and key management	www.NS200.smartdeviceco.com/encryption																																																																																		
	Data Practices	<table><tr><td>Sensor data collection</td><td><table><tr><td>Visual</td><td><ul style="list-style-type: none">CameraContinuous - Option to opt outProviding device functions</td><td><table><tr><td>Audio</td><td><ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research</td><td><table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table></td></tr><tr><td>Collection frequency</td><td></td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td></tr><tr><td>Data stored on the device</td><td>Identified</td><td>No device storage</td><td>Pseudonymized</td></tr><tr><td>Local data retention time</td><td>Up to a year</td><td>No retention</td><td>Up to a month</td></tr><tr><td>Data stored in the cloud</td><td>Identified - Data subject access request</td><td>Identified - Option to delete</td><td>No cloud storage</td></tr><tr><td>Cloud data retention time</td><td>Up to 10 years</td><td>Up to two months</td><td>No cloud storage</td></tr><tr><td>Data shared with</td><td>Manufacturers, Government</td><td>Manufacturer</td><td>Manufacturer, Third parties</td></tr><tr><td>Data sharing frequency</td><td>Periodic</td><td>Periodic - Adjustable</td><td>Periodic - Adjustable</td></tr><tr><td>Data sold to</td><td>Not disclosed</td><td>Not sold</td><td>Third parties</td></tr><tr><td>Other collected data</td><td colspan="3">Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr></table></td></tr><tr><td></td><td>More Information</td><td><table><tr><td>Data linkage</td><td>Data will not be linked with other data sources</td></tr><tr><td>What will be inferred from user's data</td><td>Not disclosed</td></tr><tr><td>Special data handling practices for children</td><td>No</td></tr><tr><td>In compliance with</td><td>GDPR</td></tr><tr><td>Privacy policy</td><td>www.NS200.smartdeviceco.com/policy</td></tr><tr><td>Call Smart Device Co. with your questions at</td><td>1 000-000-0000</td></tr><tr><td>Email Smart Device Co. with your questions at</td><td>info@smartdeviceco.com</td></tr><tr><td>Functionality when offline</td><td>Limited functionality</td></tr><tr><td>Functionality with no data processing</td><td>Limited functionality</td></tr><tr><td>Physical actuations and triggers</td><td>Device blinks when motion is detected</td></tr><tr><td>Compatible platforms</td><td>Amazon Alexa</td></tr></table></td></tr><tr><td colspan="3">CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org</td></tr><tr><td colspan="3"></td></tr></table></td></tr></table>	Sensor data collection	<table><tr><td>Visual</td><td><ul style="list-style-type: none">CameraContinuous - Option to opt outProviding device functions</td><td><table><tr><td>Audio</td><td><ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research</td><td><table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table></td></tr><tr><td>Collection frequency</td><td></td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td></tr><tr><td>Data stored on the device</td><td>Identified</td><td>No device storage</td><td>Pseudonymized</td></tr><tr><td>Local data retention time</td><td>Up to a year</td><td>No retention</td><td>Up to a month</td></tr><tr><td>Data stored in the cloud</td><td>Identified - Data subject access request</td><td>Identified - Option to delete</td><td>No cloud storage</td></tr><tr><td>Cloud data retention time</td><td>Up to 10 years</td><td>Up to two months</td><td>No cloud storage</td></tr><tr><td>Data shared with</td><td>Manufacturers, Government</td><td>Manufacturer</td><td>Manufacturer, Third parties</td></tr><tr><td>Data sharing frequency</td><td>Periodic</td><td>Periodic - Adjustable</td><td>Periodic - Adjustable</td></tr><tr><td>Data sold to</td><td>Not disclosed</td><td>Not sold</td><td>Third parties</td></tr><tr><td>Other collected data</td><td colspan="3">Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr></table></td></tr><tr><td></td><td>More Information</td><td><table><tr><td>Data linkage</td><td>Data will not be linked with other data sources</td></tr><tr><td>What will be inferred from user's data</td><td>Not disclosed</td></tr><tr><td>Special data handling practices for children</td><td>No</td></tr><tr><td>In compliance with</td><td>GDPR</td></tr><tr><td>Privacy policy</td><td>www.NS200.smartdeviceco.com/policy</td></tr><tr><td>Call Smart Device Co. with your questions at</td><td>1 000-000-0000</td></tr><tr><td>Email Smart Device Co. with your questions at</td><td>info@smartdeviceco.com</td></tr><tr><td>Functionality when offline</td><td>Limited functionality</td></tr><tr><td>Functionality with no data processing</td><td>Limited functionality</td></tr><tr><td>Physical actuations and triggers</td><td>Device blinks when motion is detected</td></tr><tr><td>Compatible platforms</td><td>Amazon Alexa</td></tr></table></td></tr><tr><td colspan="3">CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org</td></tr><tr><td colspan="3"></td></tr></table>	Visual	<ul style="list-style-type: none">CameraContinuous - Option to opt outProviding device functions	<table><tr><td>Audio</td><td><ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research</td><td><table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table></td></tr><tr><td>Collection frequency</td><td></td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td></tr><tr><td>Data stored on the device</td><td>Identified</td><td>No device storage</td><td>Pseudonymized</td></tr><tr><td>Local data retention time</td><td>Up to a year</td><td>No retention</td><td>Up to a month</td></tr><tr><td>Data stored in the cloud</td><td>Identified - Data subject access request</td><td>Identified - Option to delete</td><td>No cloud storage</td></tr><tr><td>Cloud data retention time</td><td>Up to 10 years</td><td>Up to two months</td><td>No cloud storage</td></tr><tr><td>Data shared with</td><td>Manufacturers, Government</td><td>Manufacturer</td><td>Manufacturer, Third parties</td></tr><tr><td>Data sharing frequency</td><td>Periodic</td><td>Periodic - Adjustable</td><td>Periodic - Adjustable</td></tr><tr><td>Data sold to</td><td>Not disclosed</td><td>Not sold</td><td>Third parties</td></tr><tr><td>Other collected data</td><td colspan="3">Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr></table>	Audio	<ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research	<table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table>	Motion	<ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research	Collection frequency				Purpose				Data stored on the device	Identified	No device storage	Pseudonymized	Local data retention time	Up to a year	No retention	Up to a month	Data stored in the cloud	Identified - Data subject access request	Identified - Option to delete	No cloud storage	Cloud data retention time	Up to 10 years	Up to two months	No cloud storage	Data shared with	Manufacturers, Government	Manufacturer	Manufacturer, Third parties	Data sharing frequency	Periodic	Periodic - Adjustable	Periodic - Adjustable	Data sold to	Not disclosed	Not sold	Third parties	Other collected data	Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info				More Information	<table><tr><td>Data linkage</td><td>Data will not be linked with other data sources</td></tr><tr><td>What will be inferred from user's data</td><td>Not disclosed</td></tr><tr><td>Special data handling practices for children</td><td>No</td></tr><tr><td>In compliance with</td><td>GDPR</td></tr><tr><td>Privacy policy</td><td>www.NS200.smartdeviceco.com/policy</td></tr><tr><td>Call Smart Device Co. with your questions at</td><td>1 000-000-0000</td></tr><tr><td>Email Smart Device Co. with your questions at</td><td>info@smartdeviceco.com</td></tr><tr><td>Functionality when offline</td><td>Limited functionality</td></tr><tr><td>Functionality with no data processing</td><td>Limited functionality</td></tr><tr><td>Physical actuations and triggers</td><td>Device blinks when motion is detected</td></tr><tr><td>Compatible platforms</td><td>Amazon Alexa</td></tr></table>	Data linkage	Data will not be linked with other data sources	What will be inferred from user's data	Not disclosed	Special data handling practices for children	No	In compliance with	GDPR	Privacy policy	www.NS200.smartdeviceco.com/policy	Call Smart Device Co. with your questions at	1 000-000-0000	Email Smart Device Co. with your questions at	info@smartdeviceco.com	Functionality when offline	Limited functionality	Functionality with no data processing	Limited functionality	Physical actuations and triggers	Device blinks when motion is detected	Compatible platforms	Amazon Alexa	CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org					
Sensor data collection	<table><tr><td>Visual</td><td><ul style="list-style-type: none">CameraContinuous - Option to opt outProviding device functions</td><td><table><tr><td>Audio</td><td><ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research</td><td><table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table></td></tr><tr><td>Collection frequency</td><td></td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td></tr><tr><td>Data stored on the device</td><td>Identified</td><td>No device storage</td><td>Pseudonymized</td></tr><tr><td>Local data retention time</td><td>Up to a year</td><td>No retention</td><td>Up to a month</td></tr><tr><td>Data stored in the cloud</td><td>Identified - Data subject access request</td><td>Identified - Option to delete</td><td>No cloud storage</td></tr><tr><td>Cloud data retention time</td><td>Up to 10 years</td><td>Up to two months</td><td>No cloud storage</td></tr><tr><td>Data shared with</td><td>Manufacturers, Government</td><td>Manufacturer</td><td>Manufacturer, Third parties</td></tr><tr><td>Data sharing frequency</td><td>Periodic</td><td>Periodic - Adjustable</td><td>Periodic - Adjustable</td></tr><tr><td>Data sold to</td><td>Not disclosed</td><td>Not sold</td><td>Third parties</td></tr><tr><td>Other collected data</td><td colspan="3">Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr></table></td></tr><tr><td></td><td>More Information</td><td><table><tr><td>Data linkage</td><td>Data will not be linked with other data sources</td></tr><tr><td>What will be inferred from user's data</td><td>Not disclosed</td></tr><tr><td>Special data handling practices for children</td><td>No</td></tr><tr><td>In compliance with</td><td>GDPR</td></tr><tr><td>Privacy policy</td><td>www.NS200.smartdeviceco.com/policy</td></tr><tr><td>Call Smart Device Co. with your questions at</td><td>1 000-000-0000</td></tr><tr><td>Email Smart Device Co. with your questions at</td><td>info@smartdeviceco.com</td></tr><tr><td>Functionality when offline</td><td>Limited functionality</td></tr><tr><td>Functionality with no data processing</td><td>Limited functionality</td></tr><tr><td>Physical actuations and triggers</td><td>Device blinks when motion is detected</td></tr><tr><td>Compatible platforms</td><td>Amazon Alexa</td></tr></table></td></tr><tr><td colspan="3">CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org</td></tr><tr><td colspan="3"></td></tr></table>	Visual	<ul style="list-style-type: none">CameraContinuous - Option to opt outProviding device functions	<table><tr><td>Audio</td><td><ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research</td><td><table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table></td></tr><tr><td>Collection frequency</td><td></td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td></tr><tr><td>Data stored on the device</td><td>Identified</td><td>No device storage</td><td>Pseudonymized</td></tr><tr><td>Local data retention time</td><td>Up to a year</td><td>No retention</td><td>Up to a month</td></tr><tr><td>Data stored in the cloud</td><td>Identified - Data subject access request</td><td>Identified - Option to delete</td><td>No cloud storage</td></tr><tr><td>Cloud data retention time</td><td>Up to 10 years</td><td>Up to two months</td><td>No cloud storage</td></tr><tr><td>Data shared with</td><td>Manufacturers, Government</td><td>Manufacturer</td><td>Manufacturer, Third parties</td></tr><tr><td>Data sharing frequency</td><td>Periodic</td><td>Periodic - Adjustable</td><td>Periodic - Adjustable</td></tr><tr><td>Data sold to</td><td>Not disclosed</td><td>Not sold</td><td>Third parties</td></tr><tr><td>Other collected data</td><td colspan="3">Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr></table>	Audio	<ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research	<table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table>	Motion	<ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research	Collection frequency				Purpose				Data stored on the device	Identified	No device storage	Pseudonymized	Local data retention time	Up to a year	No retention	Up to a month	Data stored in the cloud	Identified - Data subject access request	Identified - Option to delete	No cloud storage	Cloud data retention time	Up to 10 years	Up to two months	No cloud storage	Data shared with	Manufacturers, Government	Manufacturer	Manufacturer, Third parties	Data sharing frequency	Periodic	Periodic - Adjustable	Periodic - Adjustable	Data sold to	Not disclosed	Not sold	Third parties	Other collected data	Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info				More Information	<table><tr><td>Data linkage</td><td>Data will not be linked with other data sources</td></tr><tr><td>What will be inferred from user's data</td><td>Not disclosed</td></tr><tr><td>Special data handling practices for children</td><td>No</td></tr><tr><td>In compliance with</td><td>GDPR</td></tr><tr><td>Privacy policy</td><td>www.NS200.smartdeviceco.com/policy</td></tr><tr><td>Call Smart Device Co. with your questions at</td><td>1 000-000-0000</td></tr><tr><td>Email Smart Device Co. with your questions at</td><td>info@smartdeviceco.com</td></tr><tr><td>Functionality when offline</td><td>Limited functionality</td></tr><tr><td>Functionality with no data processing</td><td>Limited functionality</td></tr><tr><td>Physical actuations and triggers</td><td>Device blinks when motion is detected</td></tr><tr><td>Compatible platforms</td><td>Amazon Alexa</td></tr></table>	Data linkage	Data will not be linked with other data sources	What will be inferred from user's data	Not disclosed	Special data handling practices for children	No	In compliance with	GDPR	Privacy policy	www.NS200.smartdeviceco.com/policy	Call Smart Device Co. with your questions at	1 000-000-0000	Email Smart Device Co. with your questions at	info@smartdeviceco.com	Functionality when offline	Limited functionality	Functionality with no data processing	Limited functionality	Physical actuations and triggers	Device blinks when motion is detected	Compatible platforms	Amazon Alexa	CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org								
Visual	<ul style="list-style-type: none">CameraContinuous - Option to opt outProviding device functions	<table><tr><td>Audio</td><td><ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research</td><td><table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table></td></tr><tr><td>Collection frequency</td><td></td><td></td><td></td></tr><tr><td>Purpose</td><td></td><td></td><td></td></tr><tr><td>Data stored on the device</td><td>Identified</td><td>No device storage</td><td>Pseudonymized</td></tr><tr><td>Local data retention time</td><td>Up to a year</td><td>No retention</td><td>Up to a month</td></tr><tr><td>Data stored in the cloud</td><td>Identified - Data subject access request</td><td>Identified - Option to delete</td><td>No cloud storage</td></tr><tr><td>Cloud data retention time</td><td>Up to 10 years</td><td>Up to two months</td><td>No cloud storage</td></tr><tr><td>Data shared with</td><td>Manufacturers, Government</td><td>Manufacturer</td><td>Manufacturer, Third parties</td></tr><tr><td>Data sharing frequency</td><td>Periodic</td><td>Periodic - Adjustable</td><td>Periodic - Adjustable</td></tr><tr><td>Data sold to</td><td>Not disclosed</td><td>Not sold</td><td>Third parties</td></tr><tr><td>Other collected data</td><td colspan="3">Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info</td></tr></table>	Audio	<ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research	<table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table>	Motion	<ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research	Collection frequency				Purpose				Data stored on the device	Identified	No device storage	Pseudonymized	Local data retention time	Up to a year	No retention	Up to a month	Data stored in the cloud	Identified - Data subject access request	Identified - Option to delete	No cloud storage	Cloud data retention time	Up to 10 years	Up to two months	No cloud storage	Data shared with	Manufacturers, Government	Manufacturer	Manufacturer, Third parties	Data sharing frequency	Periodic	Periodic - Adjustable	Periodic - Adjustable	Data sold to	Not disclosed	Not sold	Third parties	Other collected data	Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info																																						
Audio	<ul style="list-style-type: none">MicrophoneContinuous - Option to opt outProviding device functions, Research	<table><tr><td>Motion</td><td><ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research</td></tr></table>	Motion	<ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research																																																																															
Motion	<ul style="list-style-type: none">Motion sensorContinuous - Option to opt outProviding device functions, Research																																																																																		
Collection frequency																																																																																			
Purpose																																																																																			
Data stored on the device	Identified	No device storage	Pseudonymized																																																																																
Local data retention time	Up to a year	No retention	Up to a month																																																																																
Data stored in the cloud	Identified - Data subject access request	Identified - Option to delete	No cloud storage																																																																																
Cloud data retention time	Up to 10 years	Up to two months	No cloud storage																																																																																
Data shared with	Manufacturers, Government	Manufacturer	Manufacturer, Third parties																																																																																
Data sharing frequency	Periodic	Periodic - Adjustable	Periodic - Adjustable																																																																																
Data sold to	Not disclosed	Not sold	Third parties																																																																																
Other collected data	Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info																																																																																		
	More Information	<table><tr><td>Data linkage</td><td>Data will not be linked with other data sources</td></tr><tr><td>What will be inferred from user's data</td><td>Not disclosed</td></tr><tr><td>Special data handling practices for children</td><td>No</td></tr><tr><td>In compliance with</td><td>GDPR</td></tr><tr><td>Privacy policy</td><td>www.NS200.smartdeviceco.com/policy</td></tr><tr><td>Call Smart Device Co. with your questions at</td><td>1 000-000-0000</td></tr><tr><td>Email Smart Device Co. with your questions at</td><td>info@smartdeviceco.com</td></tr><tr><td>Functionality when offline</td><td>Limited functionality</td></tr><tr><td>Functionality with no data processing</td><td>Limited functionality</td></tr><tr><td>Physical actuations and triggers</td><td>Device blinks when motion is detected</td></tr><tr><td>Compatible platforms</td><td>Amazon Alexa</td></tr></table>	Data linkage	Data will not be linked with other data sources	What will be inferred from user's data	Not disclosed	Special data handling practices for children	No	In compliance with	GDPR	Privacy policy	www.NS200.smartdeviceco.com/policy	Call Smart Device Co. with your questions at	1 000-000-0000	Email Smart Device Co. with your questions at	info@smartdeviceco.com	Functionality when offline	Limited functionality	Functionality with no data processing	Limited functionality	Physical actuations and triggers	Device blinks when motion is detected	Compatible platforms	Amazon Alexa																																																											
Data linkage	Data will not be linked with other data sources																																																																																		
What will be inferred from user's data	Not disclosed																																																																																		
Special data handling practices for children	No																																																																																		
In compliance with	GDPR																																																																																		
Privacy policy	www.NS200.smartdeviceco.com/policy																																																																																		
Call Smart Device Co. with your questions at	1 000-000-0000																																																																																		
Email Smart Device Co. with your questions at	info@smartdeviceco.com																																																																																		
Functionality when offline	Limited functionality																																																																																		
Functionality with no data processing	Limited functionality																																																																																		
Physical actuations and triggers	Device blinks when motion is detected																																																																																		
Compatible platforms	Amazon Alexa																																																																																		
CMU IoT Security and Privacy Label CISPL 1.0 iotsecurityprivacy.org																																																																																			
																																																																																			

iotsecurityprivacy.org

Privacy and transparency

Privacy policies and nutrition labels

Online tracking icons

Cookie consent banners

Woman Stalked Across 8 Websites By Obsessed Shoe Advertisement

NEWS IN BRIEF

October 12, 2015

VOL 51 ISSUE 41

News · Technology ·
Advertising · Fashion



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



Merrell Encore Mid Boot Q2
Women's Boots

\$149.95

-40%



UGG Niels Women's Boots

\$194.95



Rieker Z6784 Women's Dress
Boots

\$120



Born Kristina Women's Pull-on
Boots

\$135



Zappos
com





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?



- 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
~~AdChoices~~



~~42%~~ ~~56%~~ More ads will pop up

~~15%~~ ~~45%~~ Will take you to a page where you can buy advertisements on this website

~~50%~~ ~~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

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

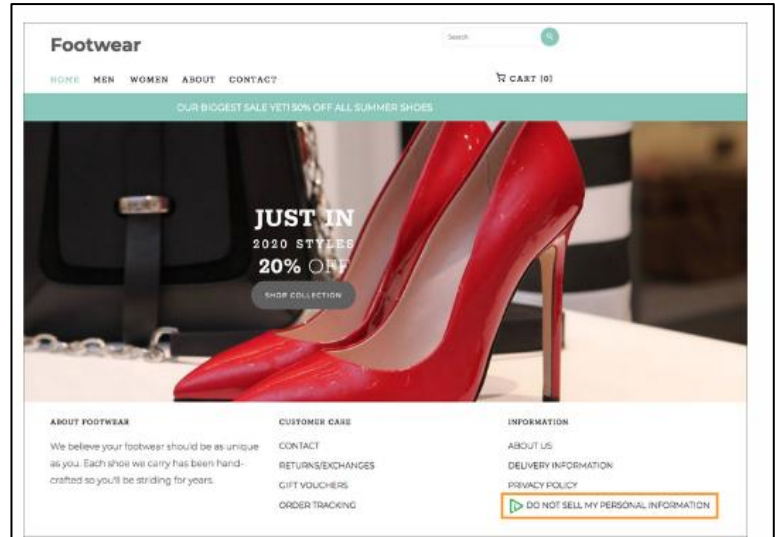


Combo testing

- 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



Close up of highlighted area:



What do you think would happen if you clicked on the symbol and link in the highlighted area on this web page?

Our
recommended
icon



iOS toggle
switch



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

Stylized toggle



CalAG toggle



CalAG-X toggle



+ swapped colors

- 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





XAVIER BECERRA
Attorney General

Search

Translate Website | Traducir Sitio Web

HOME ABOUT MEDIA CAREERS REGULATIONS RESOURCES PROGRAMS CONTACT

Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act

Press Release / Attorney General Becerra Announces Approval of Additional Re...

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.

CCPA PRIVACY OPTIONS ICON



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 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](#).

[Cookie settings](#)

Accept all cookies



Hana Habib, Megan Li, Ellie Young, Lorrie Faith Cranor

Paper to be presented at CHI 2022

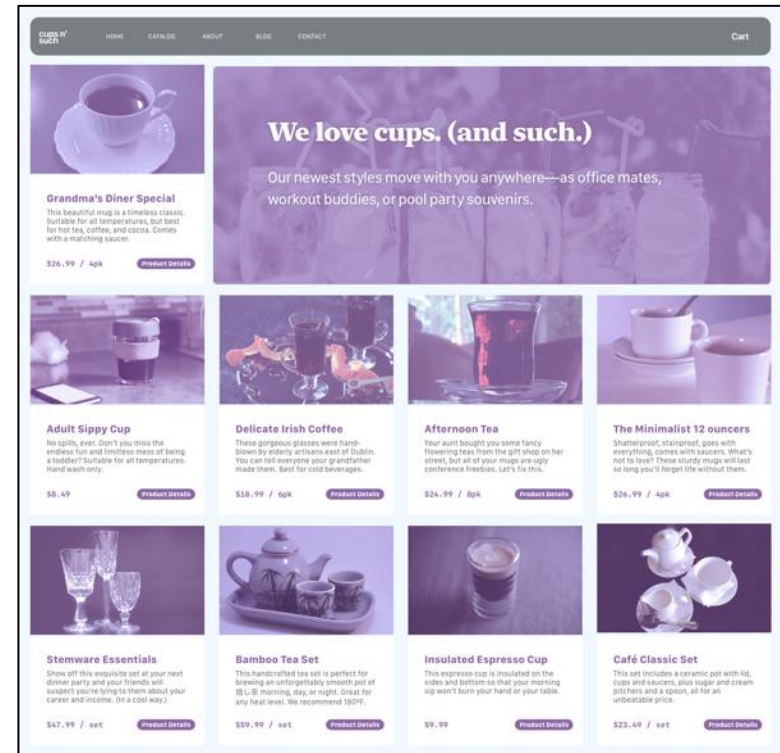
“Okay, whatever”: An Evaluation of Cookie Consent Interfaces

Evaluating the impact of design parameters on the usability of cookie consent interfaces

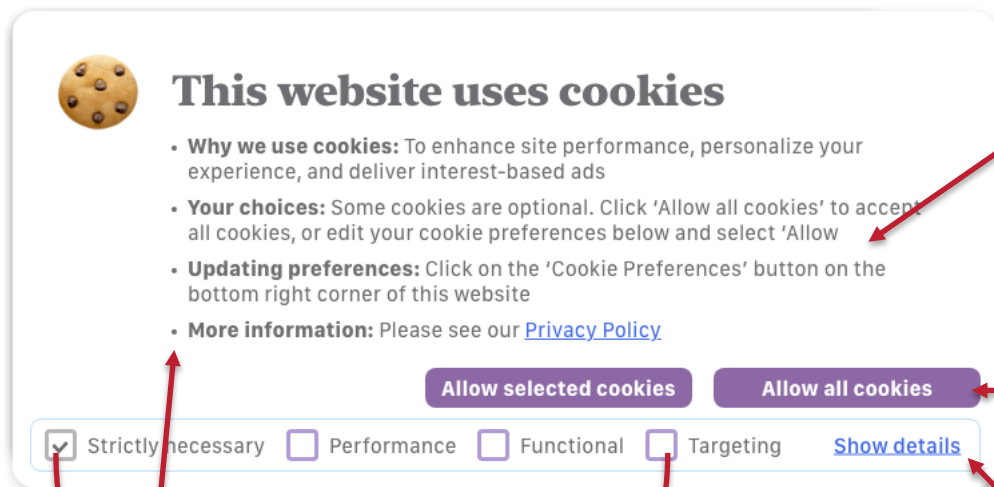
- Inspection evaluation
 - Reviewed ~200 cookie consent banners from 5 CMPs
 - Checked for dark patterns and found them on 88% of banners (most common: easiest option is to accept all cookies)
 - Identified key design parameters
- User study
 - Tested 12 cookie consent design variants with users, evaluating 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](#)

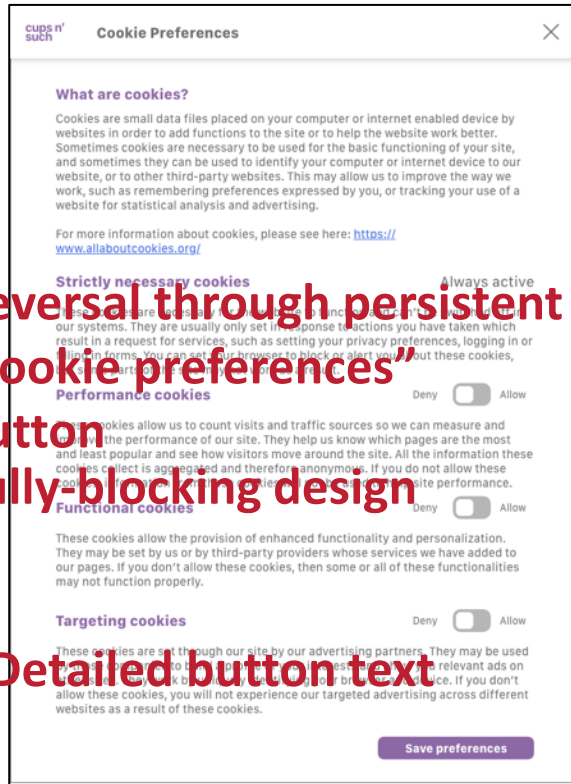
☒ Strictly necessary ☐ Performance ☐ Functional ☐ Targeting [Show details](#)

[Allow selected cookies](#) [Allow all cookies](#)

Reversal through persistent
“cookie preferences”
button
Fully-blocking design

Detailed button text

Single-layer “Cookie
Preferences” interface



Cookie Preferences

What are cookies?

Cookies are small data files placed on your computer or internet enabled device by websites in order to add functions to the site or to help the website work better. Sometimes cookies are necessary to be used for the basic functioning of your site, and sometimes they can be used to identify your computer or internet device to our website, or to other third-party websites. This may allow us to improve the way we work, such as remembering preferences expressed by you, or tracking your use of a website for statistical analysis and advertising.

For more information about cookies, please see here: <https://www.allaboutcookies.org/>

Strictly necessary cookies Always active

These cookies are essential for the website to function properly. They are usually only set in response to actions you have taken which result in a request for services, such as setting your privacy preferences, logging in or using certain site features. You can disable these cookies by blocking all cookies, but this may affect the website's performance.

Performance cookies Deny ☐ Allow ☒

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us know which pages are the most and least popular and see how visitors move around the site. All the information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies, we will not be able to improve our website's performance.

Functional cookies Deny ☐ Allow ☒

These cookies allow the provision of enhanced functionality and personalization. They may be set by us or by third-party providers whose services we have added to our pages. If you don't allow these cookies, then some or all of these functionalities may not function properly.

Targeting cookies Deny ☐ Allow ☒

These cookies are set through our site by our advertising partners. They may be used to enhance your navigation of our site and to increase the effectiveness of our marketing efforts. If you don't allow these cookies, you will not experience our targeted advertising across different websites as a result of these cookies.

[Save preferences](#)

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](#)[Cookie preferences](#)

ABOUT US

The Earth... Is A Cup.
(Holds Things)
— ancient proverb

We sell things that hold things.
Especially liquid things.
Mostly cups but also other things
and such.

CUSTOMER CARE

Contact Us
Ordering & Payment
Shipping
Returns
FAQ

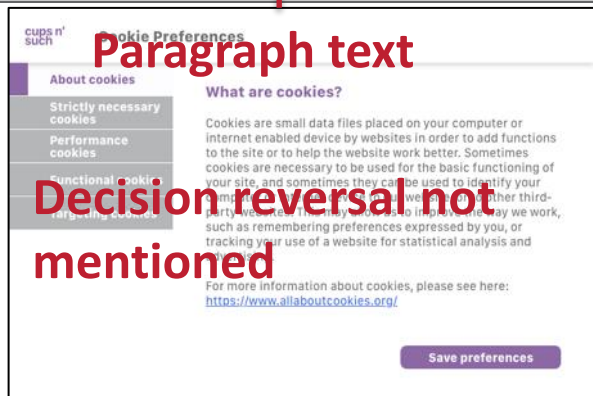
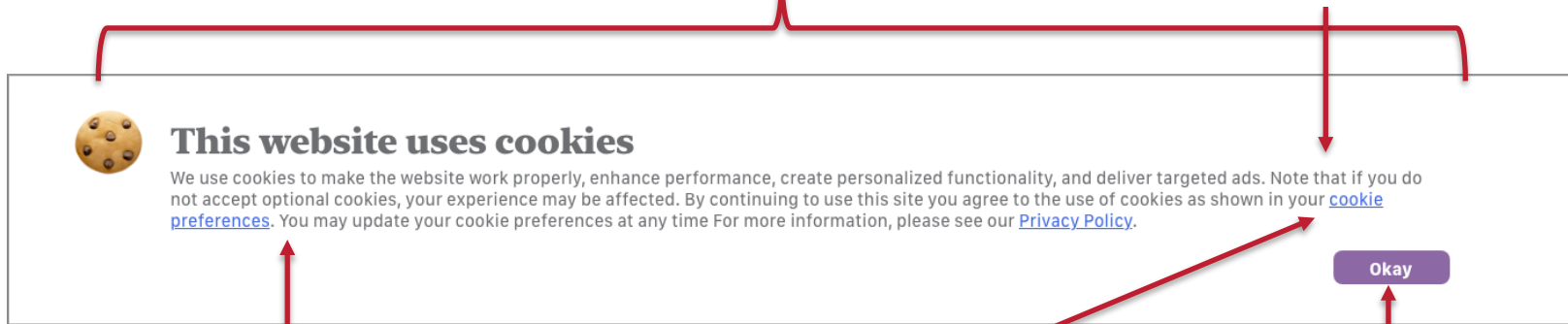
INFORMATION

Mission
Careers
Terms & Conditions
Privacy Policy
Cookie Policy



“Worst-practices” variant

Banner design at bottom of page
Loss aversion text



Embedded link to multi-layer interface

Generic button text

ALL OF THE CUPS.

Our biggest restock ever.
Use code SUMMER21 for 21% off all cold cups.

[SHOP COLLECTIONS](#)

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](#)

ABOUT US

The Earth... Is A Cup.
(Holds Things)
— ancient proverb

We sell things that hold things.
Especially liquid things.
Mostly cups but also other things
and such.

CUSTOMER CARE

Contact Us
Ordering & Payment
Shipping
Returns
FAQ

INFORMATION

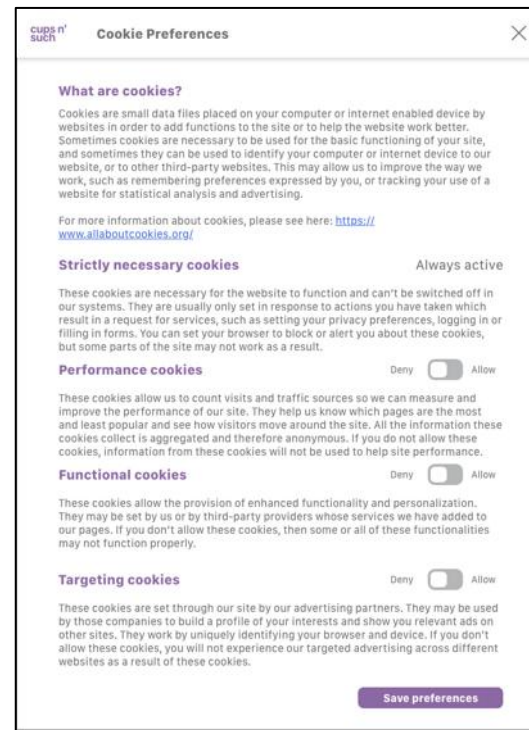
Mission
Careers
Terms & Conditions
Privacy Policy
Cookie Policy



“Corner button” variant

Cookie preferences

Single-layer “Cookie Preferences” interface



The screenshot shows a 'Cookie Preferences' dialog box with a close button (X) in the top right corner. The dialog is titled 'Cookie Preferences' and features the 'cups n' such' logo in the top left. It contains the following sections:

- What are cookies?**
Cookies are small data files placed on your computer or internet enabled device by websites in order to add functions to the site or to help the website work better. Sometimes cookies are necessary to be used for the basic functioning of your site, and sometimes they can be used to identify your computer or internet device to our website, or to other third-party websites. This may allow us to improve the way we work, such as remembering preferences expressed by you, or tracking your use of a website for statistical analysis and advertising.
For more information about cookies, please see here: <https://www.allaboutcookies.org/>
- Strictly necessary cookies** Always active
These cookies are necessary for the website to function and can't be switched off in our systems. They are usually only set in response to actions you have taken which result in a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site may not work as a result.
- Performance cookies** Deny ☐ Allow ☒
These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us know which pages are the most and least popular and see how visitors move around the site. All the information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies, information from these cookies will not be used to help site performance.
- Functional cookies** Deny ☐ Allow ☒
These cookies allow the provision of enhanced functionality and personalization. They may be set by us or by third-party providers whose services we have added to our pages. If you don't allow these cookies, then some or all of these functionalities may not function properly.
- Targeting cookies** Deny ☐ Allow ☒
These cookies are set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant ads on other sites. They work by uniquely identifying your browser and device. If you don't allow these cookies, you will not experience our targeted advertising across different websites as a result of these cookies.

A 'Save preferences' button is located at the bottom right of the dialog.

ALL OF THE CUPS.

Our biggest restock ever.
Use code SUMMER21 for 21% off all cold cups.

[SHOP COLLECTIONS](#)[Cookie preferences](#)

ABOUT US

*The Earth... is A Cup.
(Holds Things)
— ancient proverb*

We sell things that hold things.
Especially liquid things.
Mostly cups but also other things
and such.

CUSTOMER CARE

Contact Us
Ordering & Payment
Shipping
Returns
FAQ

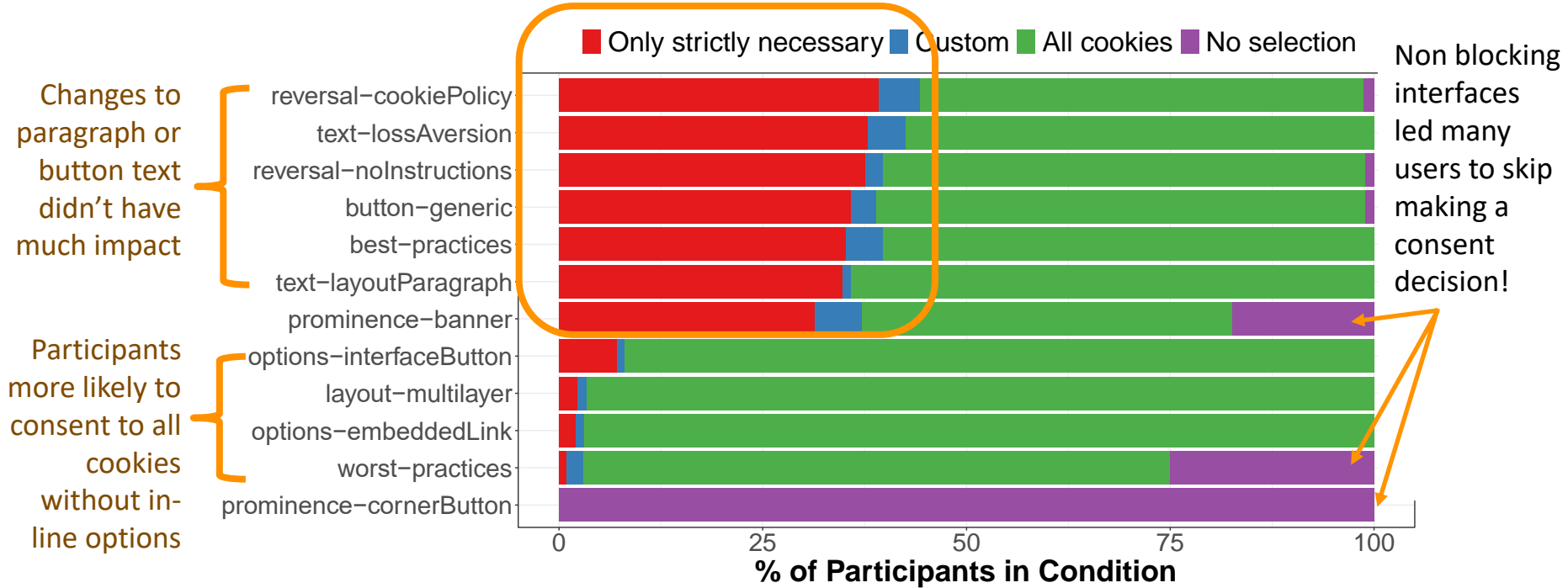
INFORMATION

Mission
Careers
Terms & Conditions
Privacy Policy
Cookie Policy

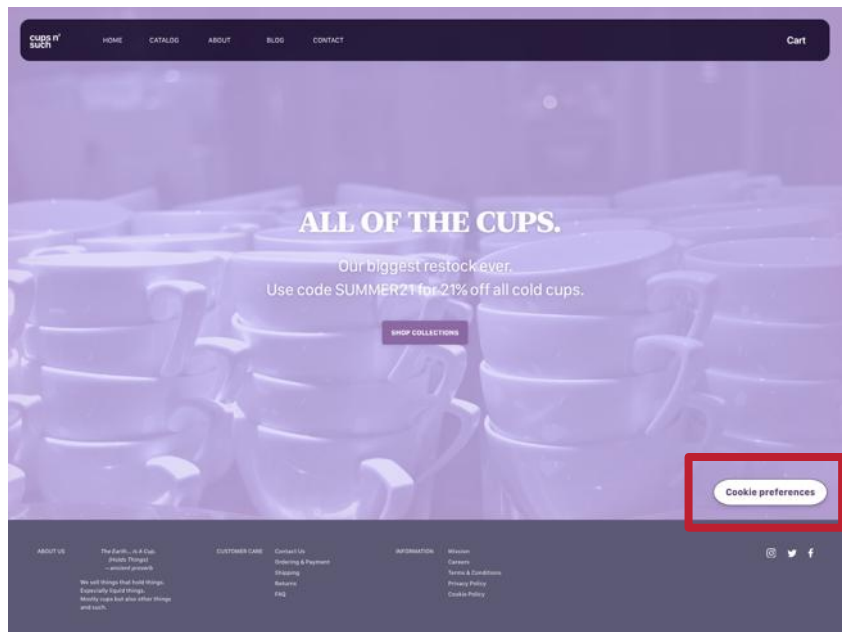


Some variables impacted consent decisions, others not so much

Inline options led users to restrict cookies

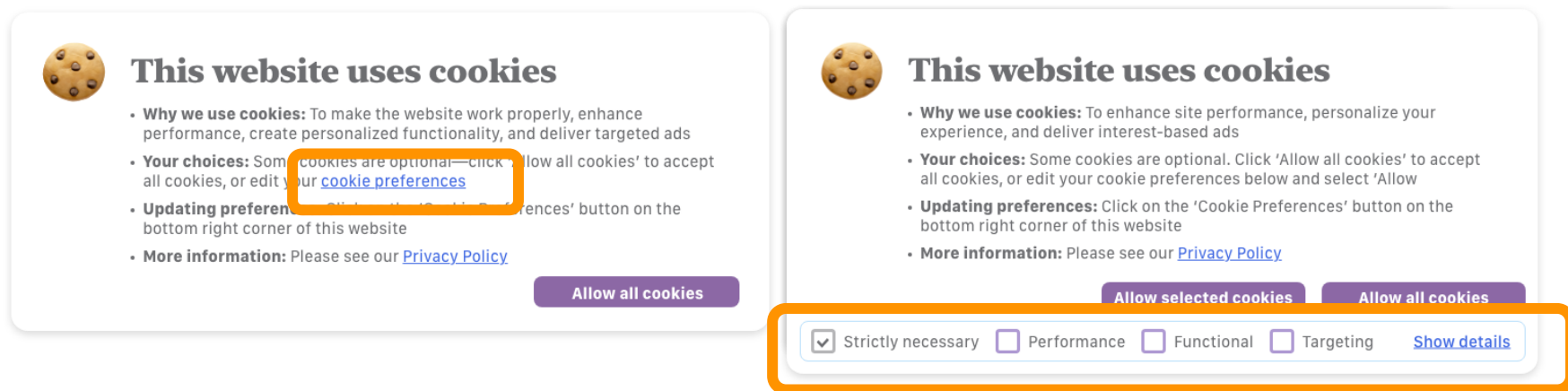


Absence of fully-blocking or banner notice led to poor awareness



- 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



This website uses cookies

- **Why we use cookies:** To make the website work properly, enhance performance, create personalized functionality, and deliver targeted ads
- **Your choices:** Some cookies are optional—click 'Allow all cookies' to accept all cookies, or edit your [cookie preferences](#)
- **Updating preferences:** Click on the 'Cookie Preferences' button on the bottom right corner of this website
- **More information:** Please see our [Privacy Policy](#)

Allow all cookies

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](#)

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

cups n' such Cookie Preferences

What are cookies?

Cookies are small data files placed on your computer or internet enabled device by websites in order to add functions to the site or to help the website work better. Sometimes cookies are necessary to be used for the basic functioning of your site, and sometimes they can be used to identify your computer or internet device to our website, or to other third-party websites. This may allow us to improve the way we work, such as remembering preferences expressed by you, or tracking your use of a website for statistical analysis and advertising.

For more information about cookies, please see here: <https://www.allaboutcookies.org/>

Strictly necessary cookies Always active

These cookies are necessary for the website to function and can't be switched off in our systems. They are usually only set in response to actions you have taken which result in a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site may not work as a result.

Performance cookies Deny ☐ Allow

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us know which pages are the most and least popular and see how visitors move around the site. All the information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies, information from these cookies will not be used to help site performance.

Functional cookies Deny ☐ Allow

These cookies allow the provision of enhanced functionality and personalization. They may be set by us or by third-party providers whose services we have added to our pages. If you don't allow these cookies, then some or all of these functionalities may not function properly.

Targeting cookies Deny ☐ Allow

These cookies are set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant ads on other sites. They work by uniquely identifying your browser and device. If you don't allow these cookies, you will not experience our targeted advertising across different websites as a result of these cookies.

Save preferences

cups n' such Cookie Preferences

- About cookies
- Strictly necessary cookies
- Performance cookies**
- Functional cookies
- Targeting cookies

Performance cookies Deny ☐ Allow

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us know which pages are the most and least popular and see how visitors move around the site. All the information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies, information from these cookies will not be used to help site performance.

Save preferences

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

https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf

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.

Lorrie Faith Cranor

lorrie.cranor.org

@lorrietweet

Papers: cups.cs.cmu.edu

**Privacy engineering masters
and certificate programs:**
privacy.cs.cmu.edu

Carnegie Mellon University
Security and Privacy Institute

CyLab