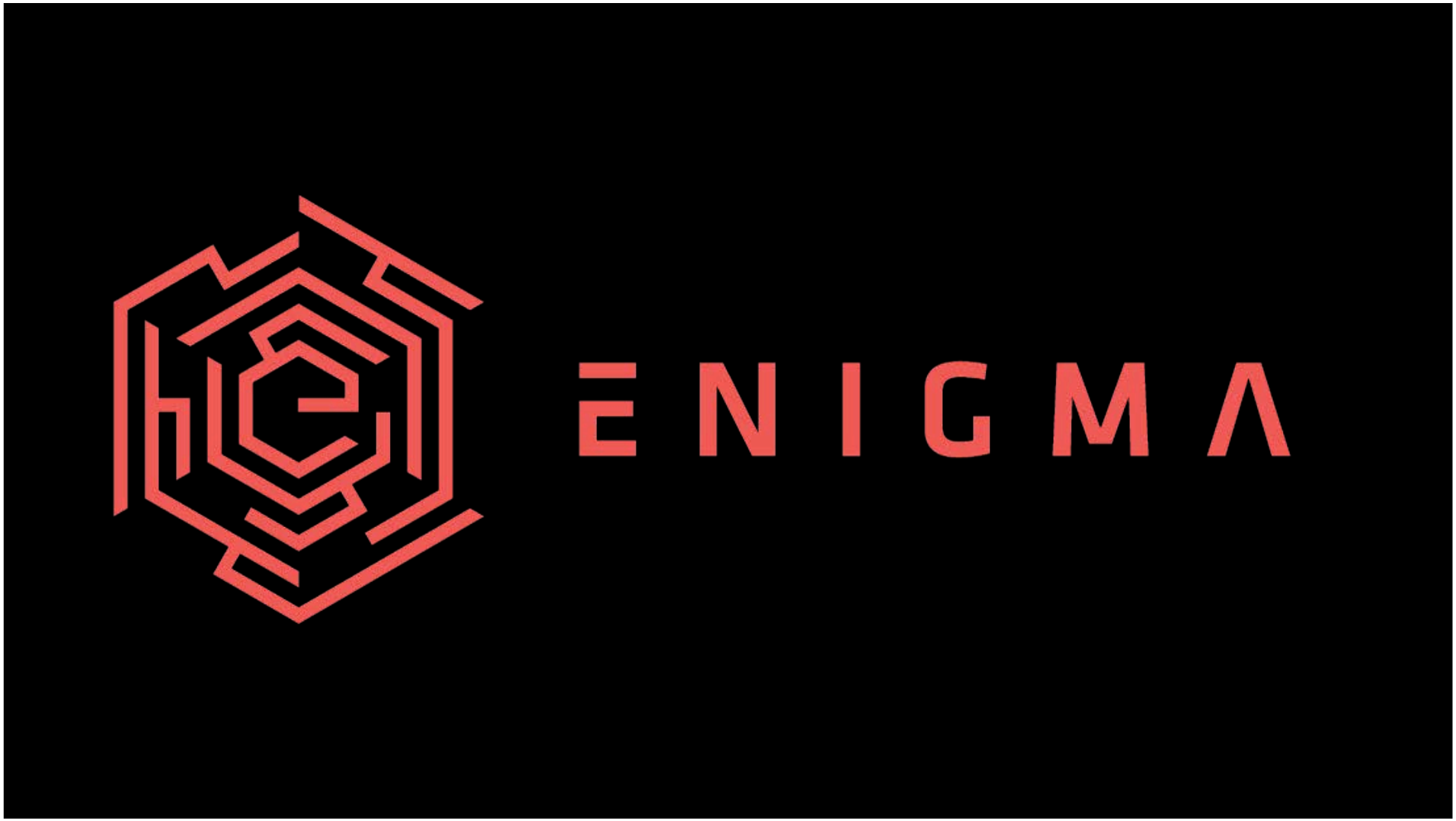

ENIGMA

Putting privacy notices to the test

Lorrie Faith Cranor

@lorrietweet

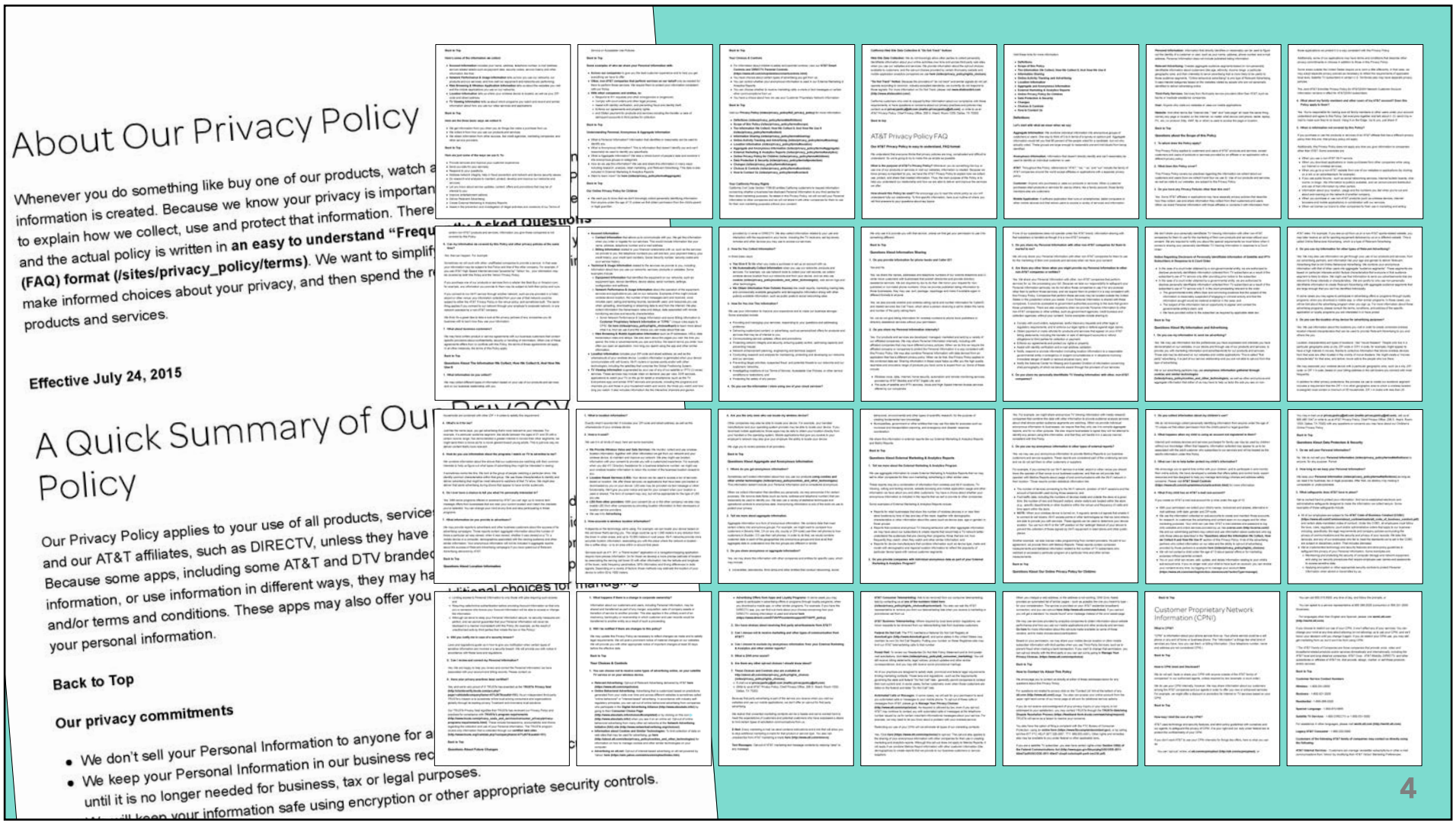


Carnegie Mellon University



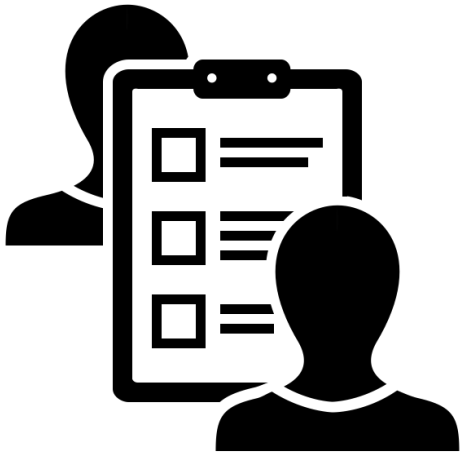
244 HOURS PER YEAR

A. McDonald & L. Cranor, The Cost of Reading Privacy Policies,
I/S: A Journal of Law and Policy for the Information Society, 2008.


About Our Privacy Policy
Whenever you do something like buy one of our products, watch a
information is created. Because we know your privacy is importan
to explain how we collect, use and protect that information. There
and the actual policy is written in an easy to understand "Frequ
(FAQ) format (/sites/privacy_policy/terms). We want to simplif
make informed choices about your privacy, and then spend the r
products and services.
Effective July 24, 2015
A Quick Summary of Our Privacy Policy
Our Privacy Policy applies to your use of all products, service
and our AT&T affiliates, such as DIRECTV, unless they have
Because some apps, including some AT&T and DTV branded
information, or use information in different ways, they may ha
and/or terms and conditions. These apps may also offer you
your personal information.
Back to Top
Our privacy commitments
We don't sell your Personal Information to anyone for a
We keep your Personal Information in our business rec
until it is no longer needed for business, tax or legal purposes.
information safe using encryption or other appropriate security controls.

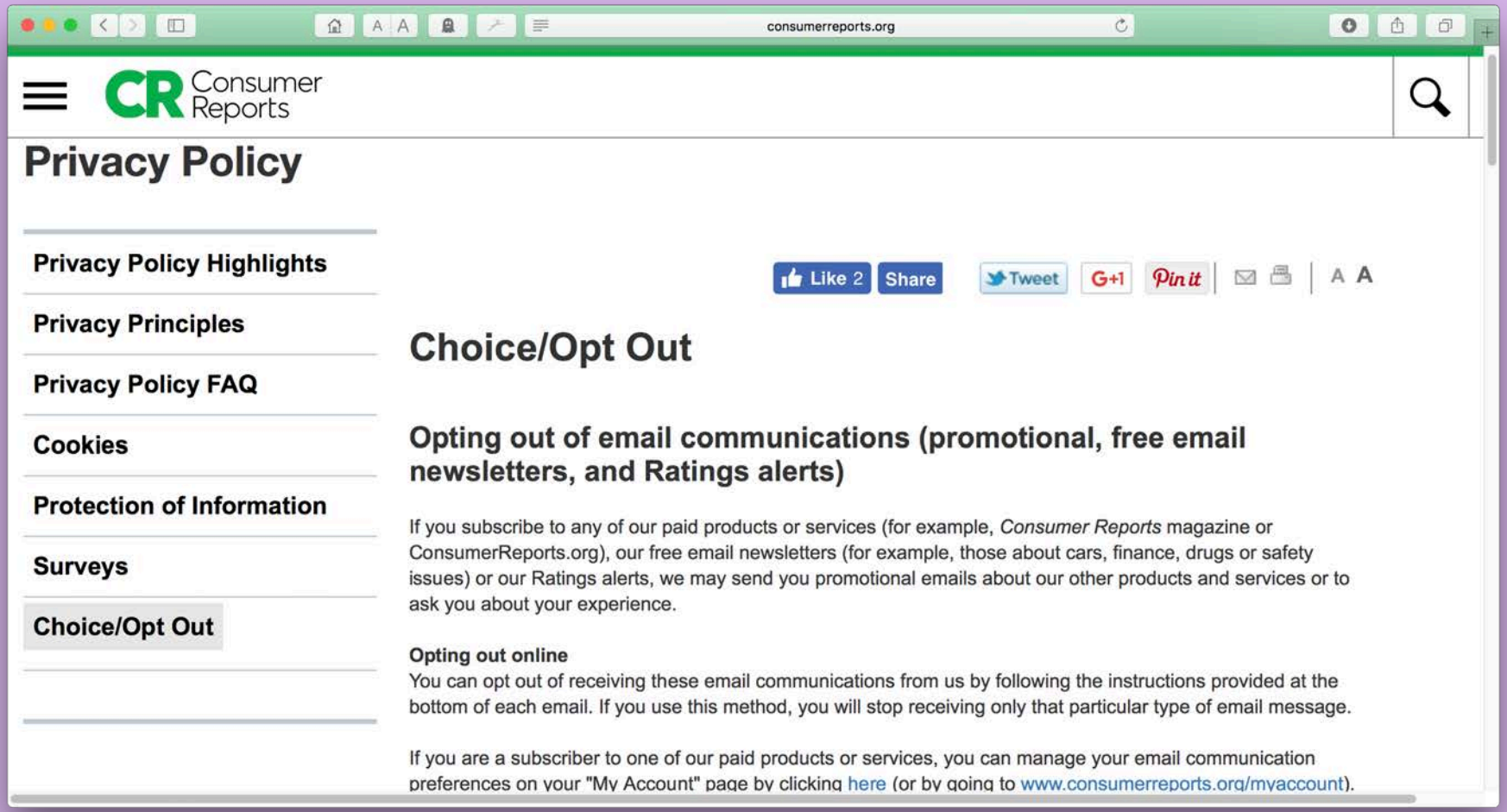

IMPORTANT
NOTICE

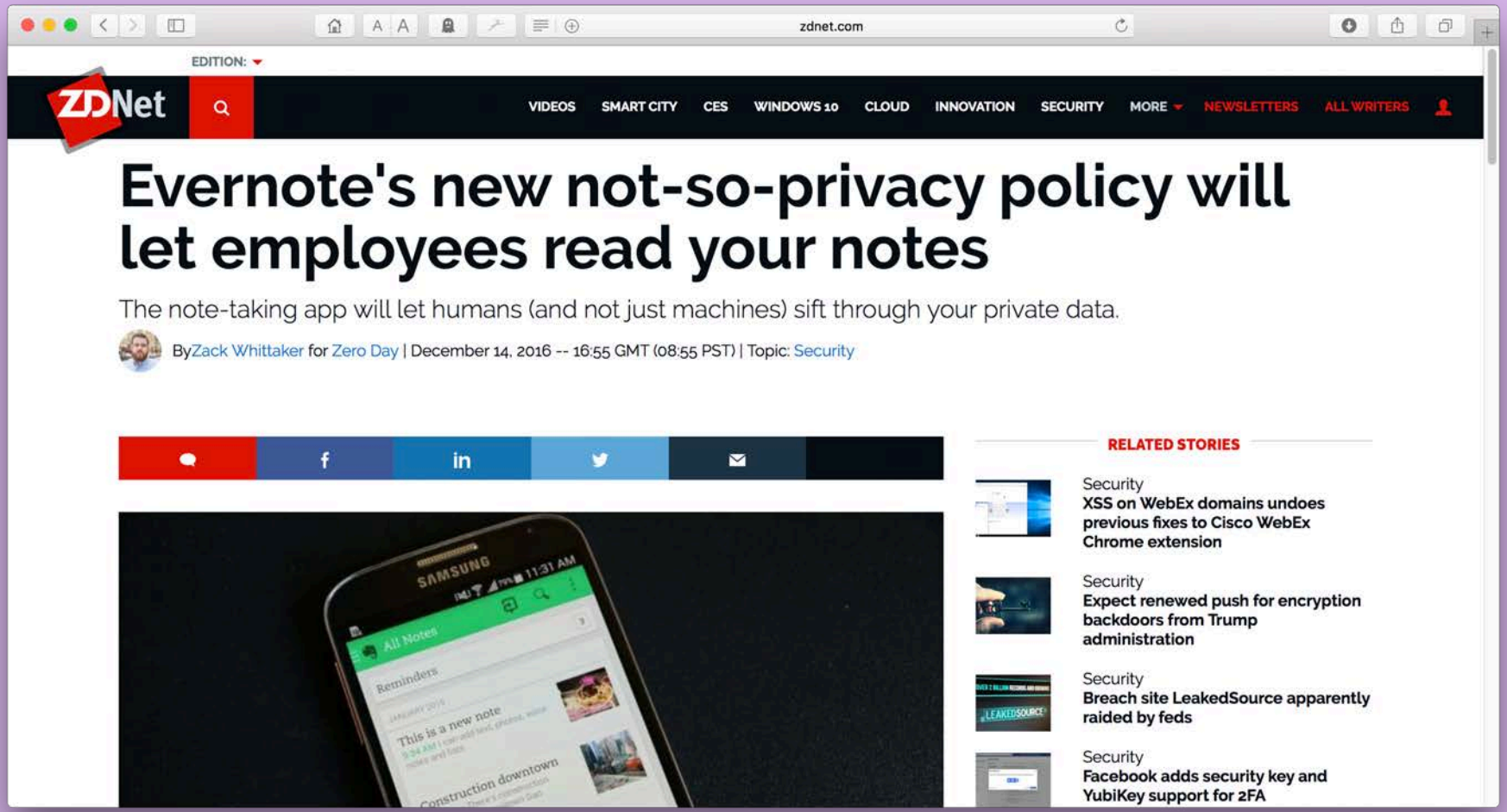


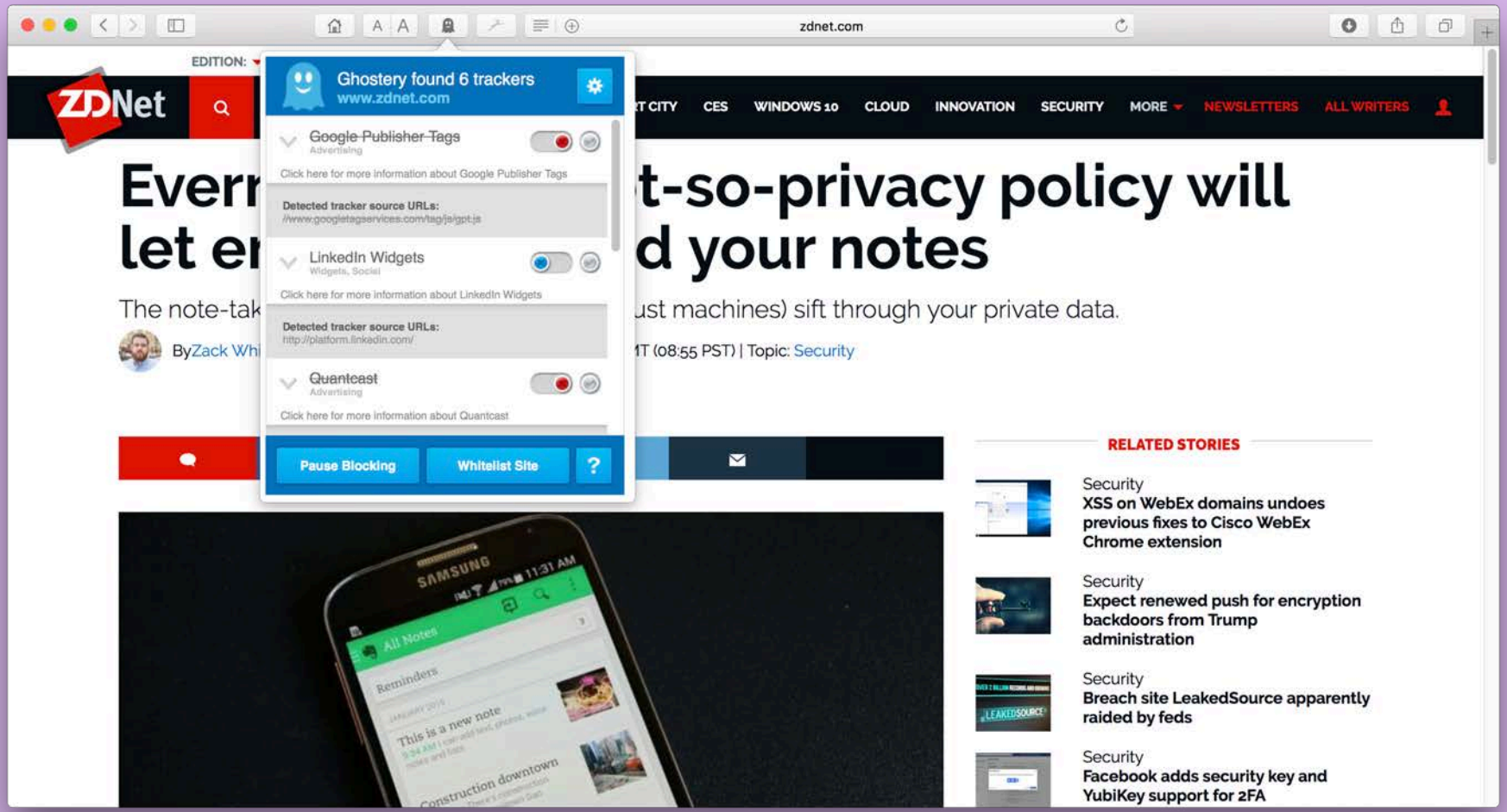



IMPORTANT
NOTICE


ftc.gov
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
MAIN MENU
SEARCH
Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices
Settlement ensures consumers can control targeted ads
FOR RELEASE
December 20, 2016


consumerreports.org
CR Consumer Reports
Privacy Policy
Privacy Policy Highlights
Privacy Principles
Privacy Policy FAQ
Cookies
Protection of Information
Surveys
Choice/Opt Out
Like 2
Share
Tweet
G+1
Pin it
A A
Choice/Opt Out
Opting out of email communications (promotional, free email newsletters, and Ratings alerts)
If you subscribe to any of our paid products or services (for example, Consumer Reports magazine or ConsumerReports.org), our free email newsletters (for example, those about cars, finance, drugs or safety issues) or our Ratings alerts, we may send you promotional emails about our other products and services or to ask you about your experience.
Opting out online
You can opt out of receiving these email communications from us by following the instructions provided at the bottom of each email. If you use this method, you will stop receiving only that particular type of email message.
If you are a subscriber to one of our paid products or services, you can manage your email communication preferences on your "My Account" page by clicking here (or by going to www.consumerreports.org/myaccount).


zdnet.com
EDITION:
ZDNet
VIDEOS
SMART CITY
CES
WINDOWS 10
CLOUD
INNOVATION
SECURITY
MORE
NEWSLETTERS
ALL WRITERS
Evernote's new not-so-privacy policy will let employees read your notes
The note-taking app will let humans (and not just machines) sift through your private data.
ByZack Whittaker for Zero Day | December 14, 2016 -- 16:55 GMT (08:55 PST) | Topic: Security
SAMSUNG
11:31 AM
All Notes
Reminders
This is a new note
Construction downtown
RELATED STORIES
Security
XSS on WebEx domains undoes previous fixes to Cisco WebEx Chrome extension
Security
Expect renewed push for encryption backdoors from Trump administration
Security
Breach site LeakedSource apparently raided by feds
Security
Facebook adds security key and YubiKey support for 2FA


zdnet.com
EDITION:
ZDNet
CES
WINDOWS 10
CLOUD
INNOVATION
SECURITY
MORE
NEWSLETTERS
ALL WRITERS
Ghostery found 6 trackers
www.zdnet.com
Google Publisher Tags
Advertising
Click here for more information about Google Publisher Tags
Detected tracker source URLs:
//www.googletagservices.com/tag/js/gpt.js
LinkedIn Widgets
Widgets, Social
Click here for more information about LinkedIn Widgets
Detected tracker source URLs:
http://platform.linkedin.com/
Quantcast
Advertising
Click here for more information about Quantcast
Pause Blocking
Whitelist Site
t-so-privacy policy will
d your notes
ust machines) sift through your private data.
T (08:55 PST) | Topic: Security
RELATED STORIES
Security
XSS on WebEx domains undoes previous fixes to Cisco WebEx Chrome extension
Security
Expect renewed push for encryption backdoors from Trump administration
Security
Breach site LeakedSource apparently raided by feds
Security
Facebook adds security key and YubiKey support for 2FA



"ONLY IN SOME FANTASY WORLD

do users actually read these notices and understand their implications before clicking to indicate their consent"

— President's Council of Advisors on Science and Technology, *Big Data and Privacy* May 2014






nest
COOLING
75
78


amazon


Tide
Bounty
Charmin



"The question is not whether consumers should be given a say over unexpected uses of their data; rather, **THE QUESTION IS HOW TO PROVIDE SIMPLIFIED NOTICE AND CHOICE.**"

— FTC Chairwoman Edith Ramirez,
January 2015
Speaking about IoT privacy

EU General Data Protection Regulation

"**transparent** and easily **accessible** policies"

"in an **intelligible** form, using **clear** and **plain language**"



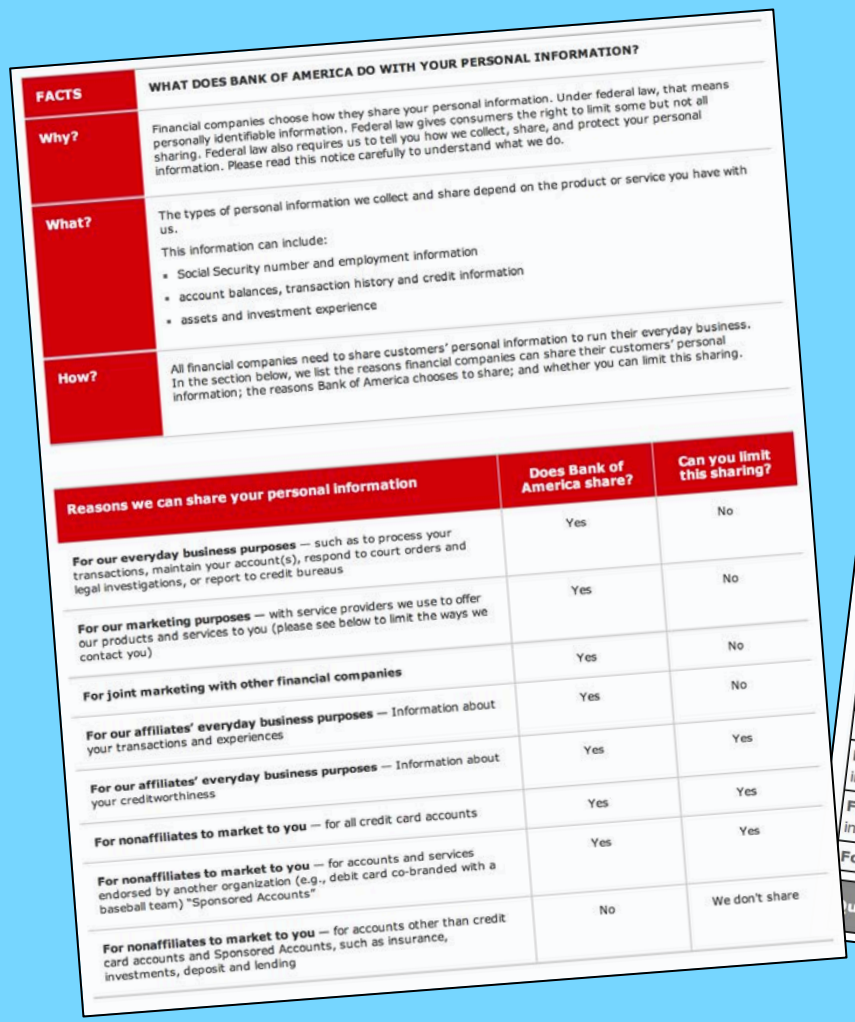

FACTS
WHAT DOES BANK OF AMERICA DO WITH YOUR PERSONAL INFORMATION?
Why?
Financial companies choose how they share your personal information. Under federal law, that means personally identifiable information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires 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:
• 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
Acme
information we collect
ways we use your information
information sharing
provide service and maintain site
marketing
telemarketing
profiling
other companies
public forums
contact information
cookies
demographic information
financial information
health information
preferences
purchasing information
social security number & gov't ID
your activity on this site
your location
opt out
Access to your information
How to resolve privacy-related disputes with this site
acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com
we will collect and use your information in this way
by default, we will collect and use your information in this way unless you tell us not to by opting out
we will not collect and use your information in this way
opt in
by default, we will not collect and use your information in this way unless you allow us to by opting in
PrivacyVille
start here
play games
0%
BELL
4:21 PM
100%
AWESOME APP
PRIVACY DASHBOARD
seal of trust
DATA COLLECTED
BROWSER HISTORY
YES
PHONE & TEXT LOGS
YES
BIOMETRICS
YES
FINANCIAL
NO
CONTACTS
NO
USER FILES
NO
FULL PRIVACY POLICY
TM

Acme

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						

Bell Group

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 in			opt out	
cookies						
demographic information		opt in			opt out	
financial information						
health information						
preferences		opt in			opt out	
purchasing information		opt in			opt out	
social security number & gov't ID						
your activity on this site		opt in			opt out	
your location						



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: ▪ 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	No
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: • 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

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



Your Data is Used Only for the Intended Use



Your Data May be Used for Purposes You Do Not Intend



Your data is never given to advertisers.



Site gives your data to advertisers.



Your data is never bartered or sold.



Your data may be bartered or sold.



Data is given to law enforcement only when legal process is followed.



Data may be given to law enforcement even when legal process is not followed.



Your data is kept for less than 1 month.









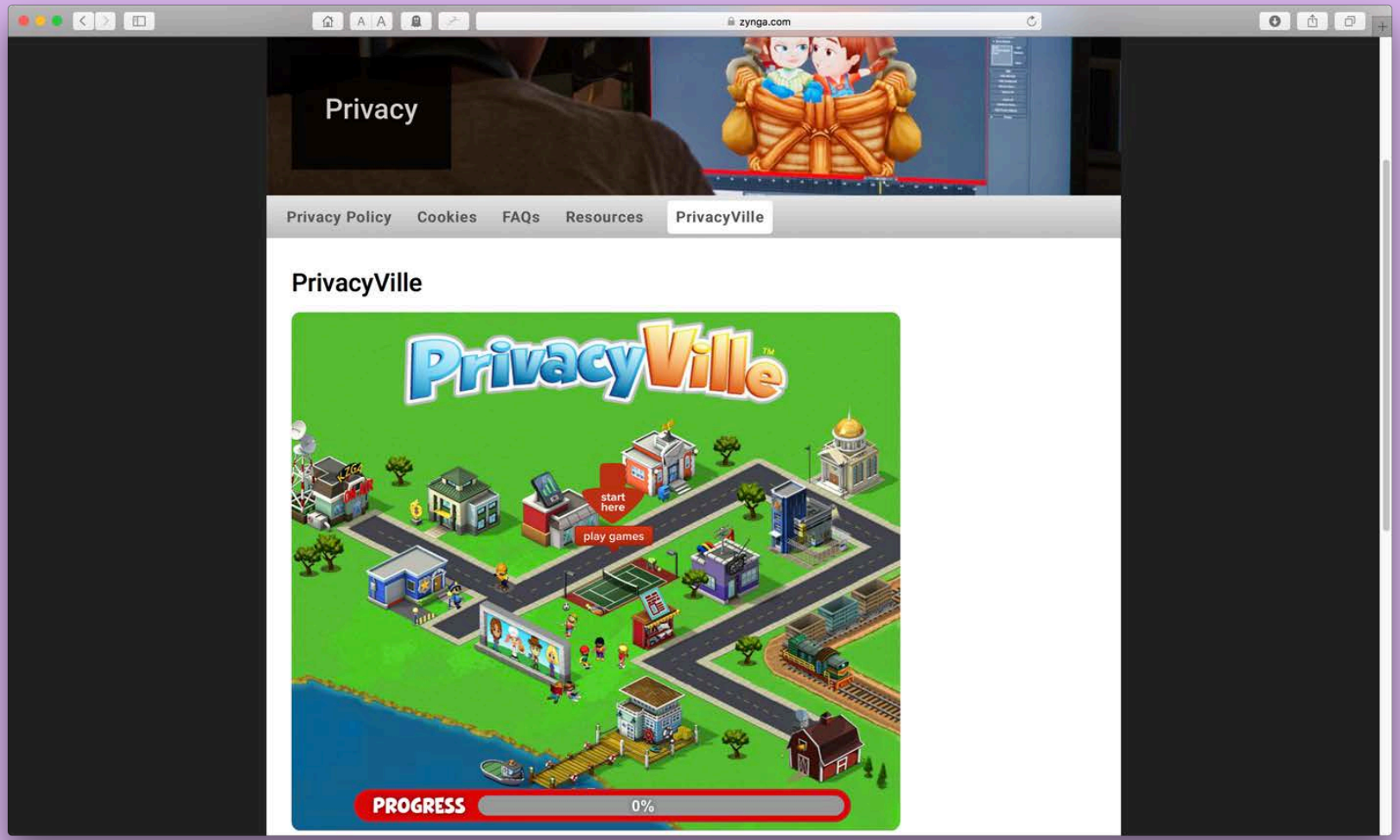
Your data may be kept indefinitely.



TYPE OF DATA COLLECTED	GENERAL DATA PRACTICES	DATA SHARING
contact: name, mailing address, email, or phone number	**ad customization:** user data may be used for the purpose of customizing advertising	**affiliates:** affiliates and subsidiaries bound by the same privacy practices
computer: IP address, browser type, or operating system	**third party tracking:** site allows third parties to place advertisements that may track user behavior	**contractors:** third party contractors bound by the same privacy practices
interactive: browsing behavior or search history	**public display:** service allows users to contribute information which may be displayed publicly	**third parties:** third parties not subject to same data practices
financial: account status or activity, credit information, or purchase history	**user control:** users allowed to access and correct personal data collected	
content: contents of personal communications, stored documents or media	**data retention:** explicitly stated duration of retention for personal data collected	

TRUSTe ▸
Certified Privacy

TM

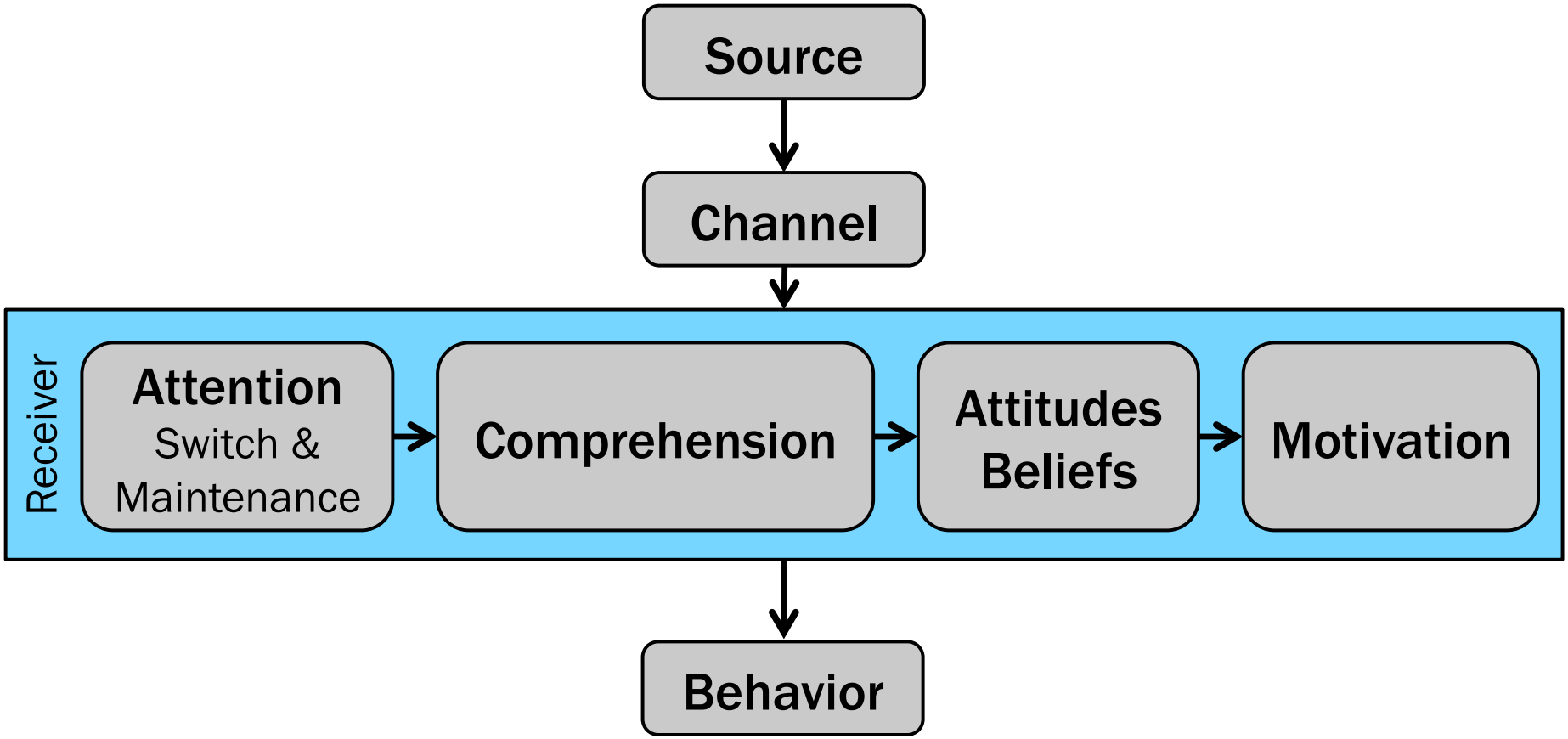

zynga.com
Privacy
Privacy Policy
Cookies
FAQs
Resources
PrivacyVille
PrivacyVille
PrivacyVille
start here
play games
PROGRESS
0%


privacyassistant.org


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:
• 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
Acme
information we collect
ways we use your information
information sharing
provide service and maintain site
marketing
telemarketing
profiling
other companies
public forums
contact information
cookies
demographic information
financial information
health information
preferences
purchasing information
social security number & gov't ID
your activity on this site
your location
opt out
Access to your information
How to resolve privacy-related disputes with this site
acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com
we will collect and use your information in this way
by default, we will collect and use your information in this way unless you tell us not to by opting out
we will not collect and use your information in this way
opt in
by default, we will not collect and use your information in this way unless you allow us to by opting in
PrivacyVille
start here
play games
0%
BELL
4:21 PM
100%
AWESOME APP
PRIVACY DASHBOARD
seal of trust
DATA COLLECTED
BROWSER HISTORY
YES
PHONE & TEXT LOGS
YES
BIOMETRICS
YES
FINANCIAL
NO
CONTACTS
NO
USER FILES
NO
FULL PRIVACY POLICY
TM

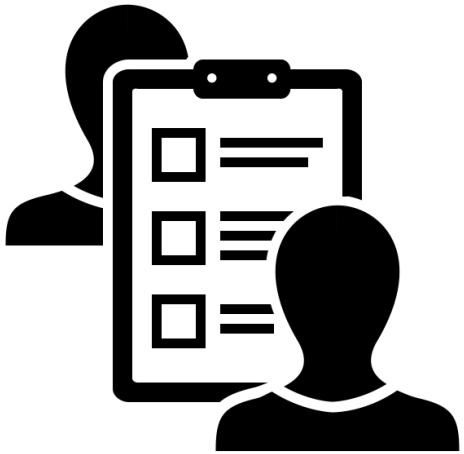
IMPORTANT
NOTICE





Michael Wogalter, C-HIP Model (simplified)

IMPORTANT
NOTICE

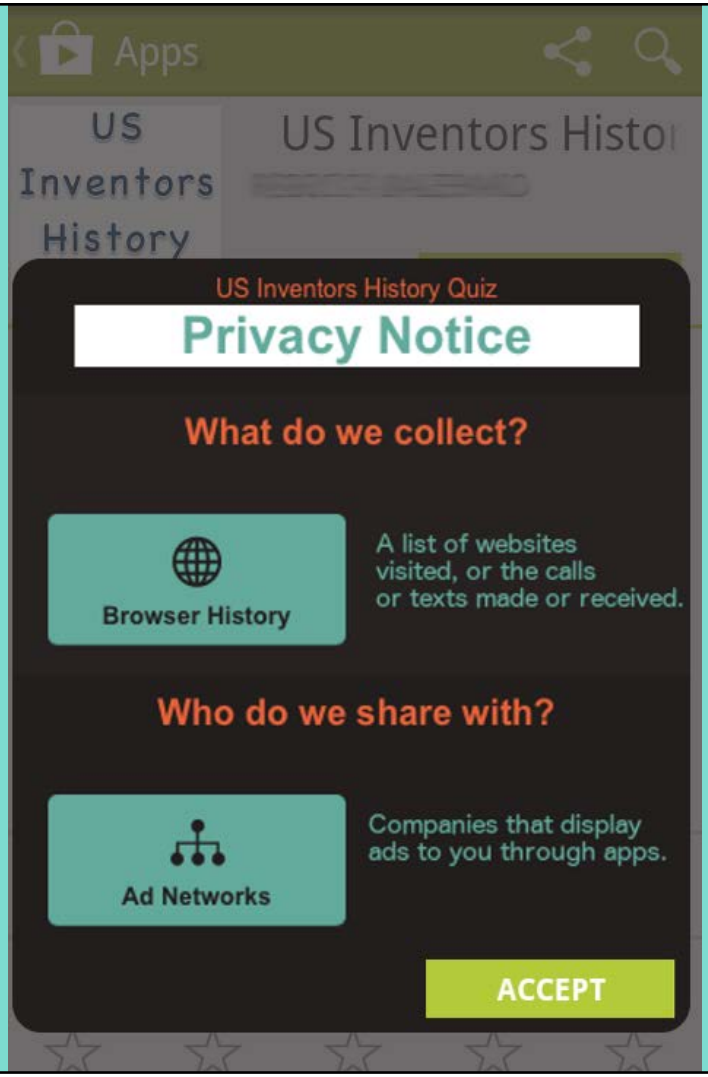


Attention



R. Balebako, F. Schaub, I. Adjerid, A. Acquisti, L. Cranor. The Impact of Timing on the Salience of Smartphone App Privacy Notices. SPSM 2015.


11:22 AM
Apps
US Inventors History Quiz
US Inventors Histo
REBECCA BALEBAKO
INSTALL
Question 11 of 11
Otis Boykin (1920-1982) invented more than 25 electronic devices before he died of a heart failure. One of the devices he is most famous for is:
the yo-yo
a control unit for the artificial heart pacemaker
a glove to translate sign language into speech
the smallpox vaccination
Privacy Notice
What do we collect?
A list of websites visited, or the calls or texts made or recieved
Who do we share with?
Companies that display ads to you through apps
About
Apr 14, 2014
5+ downloads
1.62MB
+1 Be the first to +1 this.
Rate this app


Apps
US Inventors History
US Inventors Histo
US Inventors History Quiz
Privacy Notice
What do we collect?
Browser History
A list of websites visited, or the calls or texts made or received.
Who do we share with?
Ad Networks
Companies that display ads to you through apps.
ACCEPT

Comprehension





P. Leon, J. Cranshaw, L. Cranor, J. Graves, M. Hastak, B. Ur, G. Xu. What Do Online Behavioral Advertising Disclosures Communicate to Users? WPES 2012

AdChoices

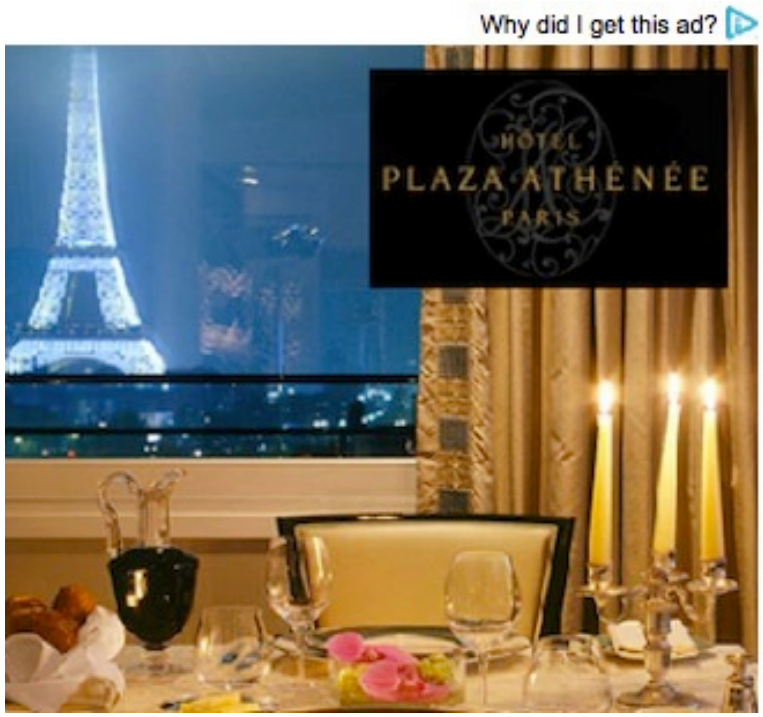
Why did I get this ad?

Interest based ads

Sponsor ads

Learn about your ad choices

Configure ad preferences



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



Behavior

Privacy Facts

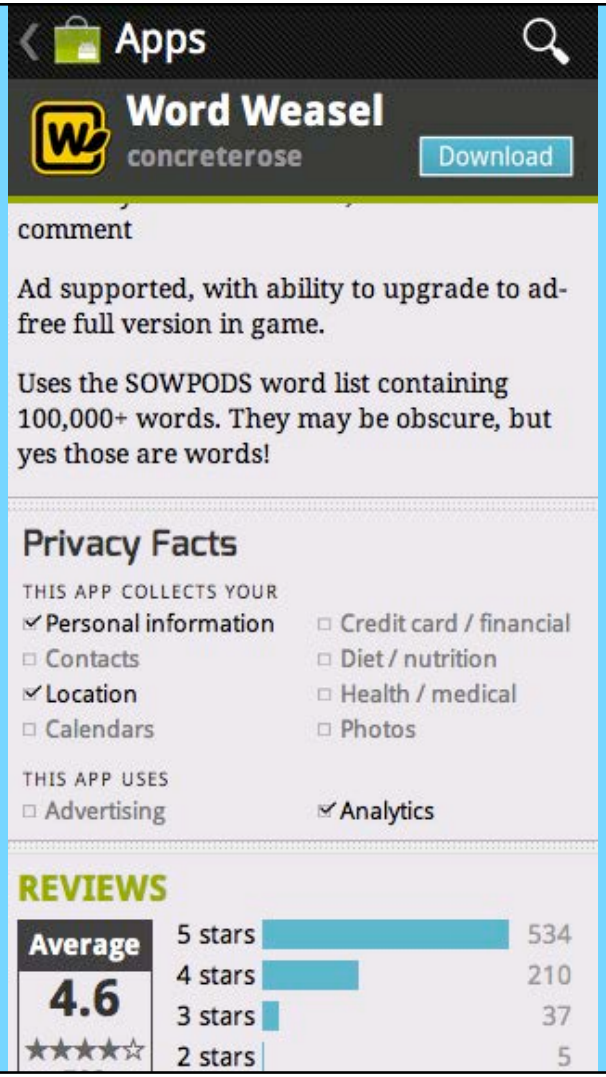
THIS APP COLLECTS YOUR

- ☑ Personal information
- ☑ Contacts
- ☑ Location
- ☐ Calendars
- ☑ Credit card / financial
- ☐ Diet / nutrition
- ☐ Health / medical
- ☑ Photos

THIS APP USES

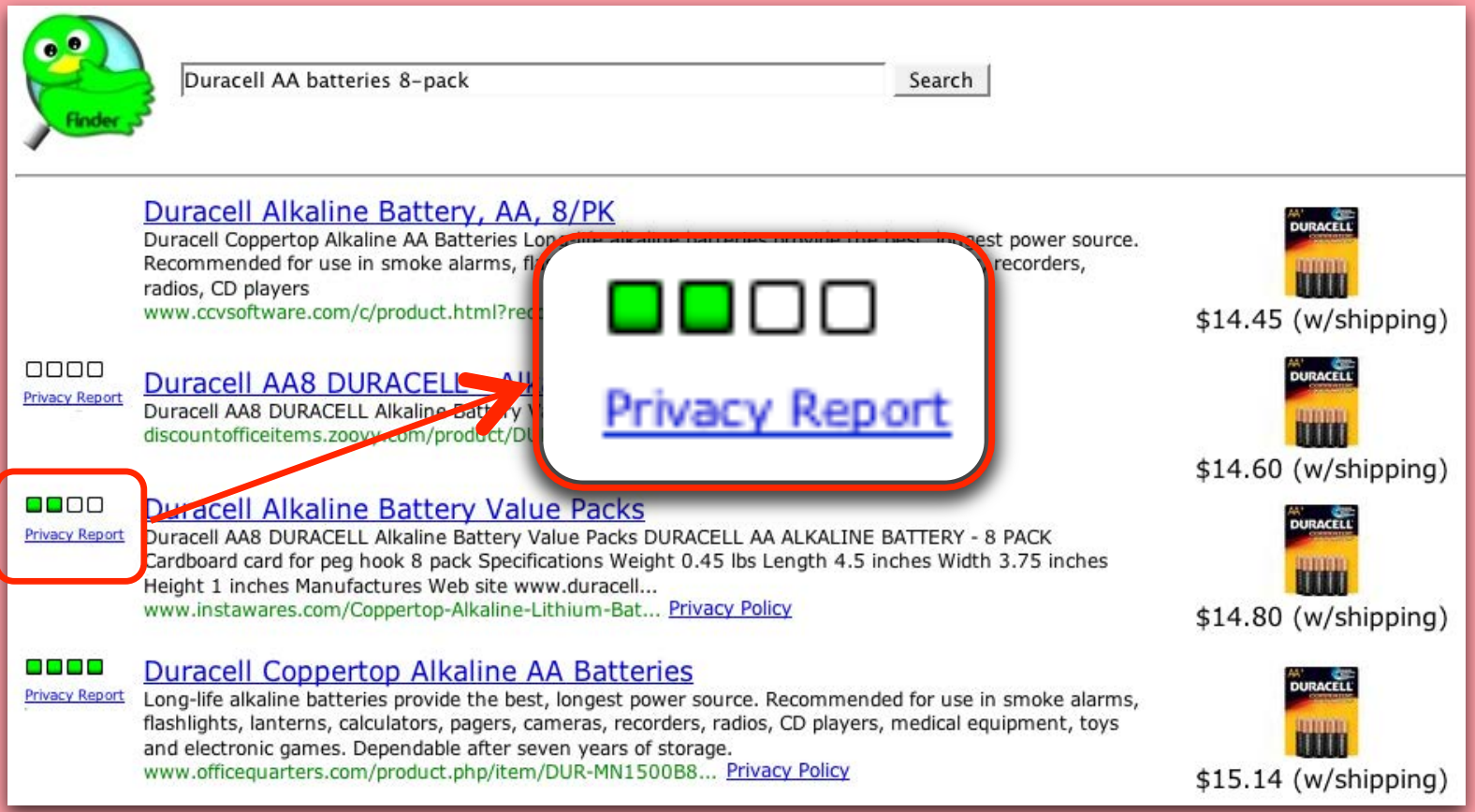
- ☑ Advertising
- ☑ Analytics

P.G. Kelley, L.F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. CHI 2013.



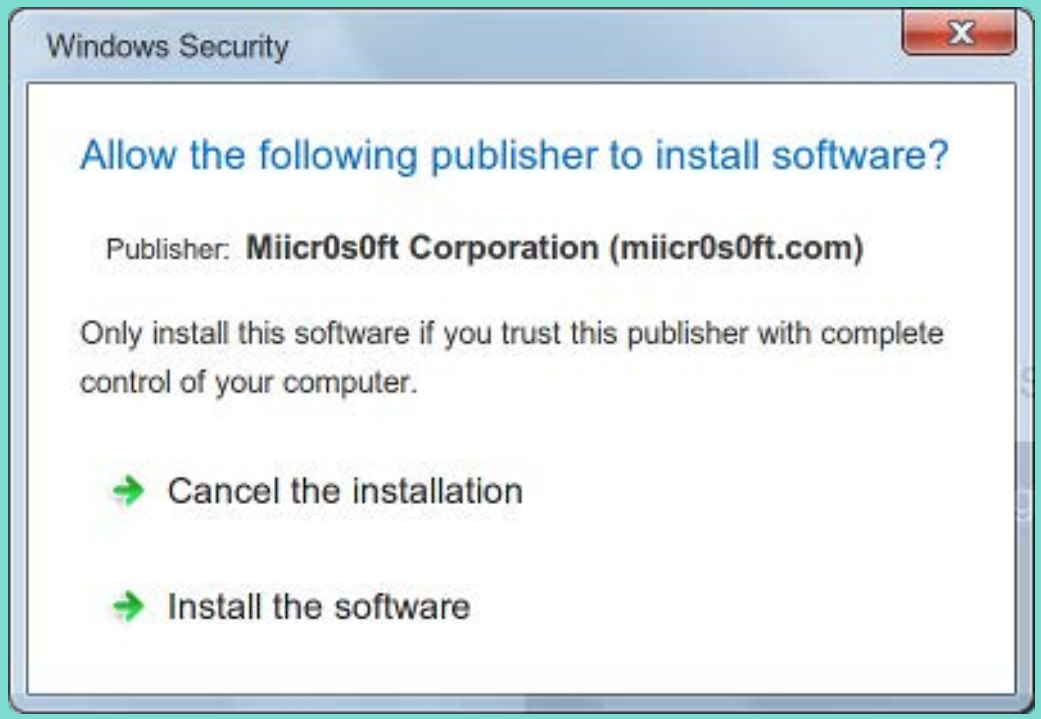
Privacy Facts influenced behavior

Privacy is just one factor

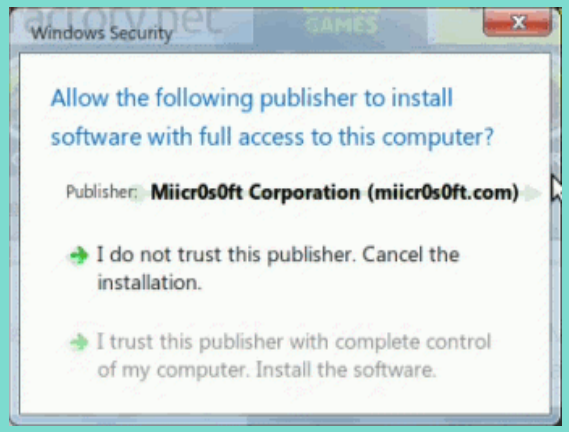


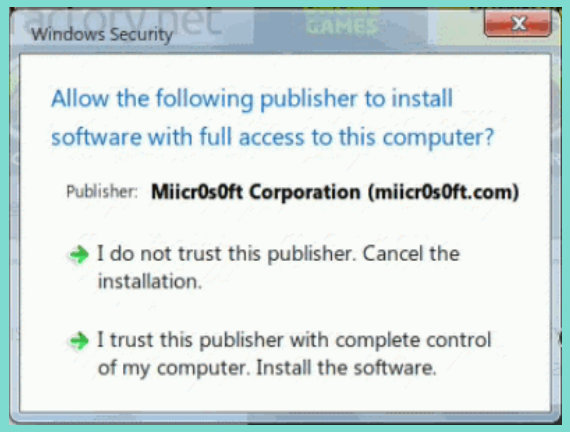
S. Egelman, J. Tsai, L. Cranor, A. Acquisti. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. CHI 2009.

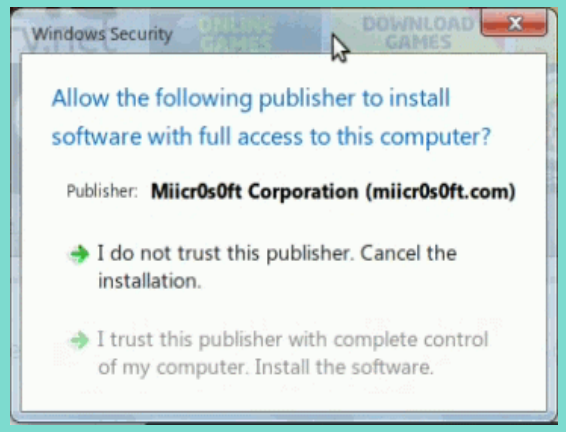
Behavior



C. Bravo-Lillo, L.F. Cranor, J. Downs, S. Komanduri, R.W. Reeder, S. Schechter, and M. Sleeper. Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore. SOUPS 2013.

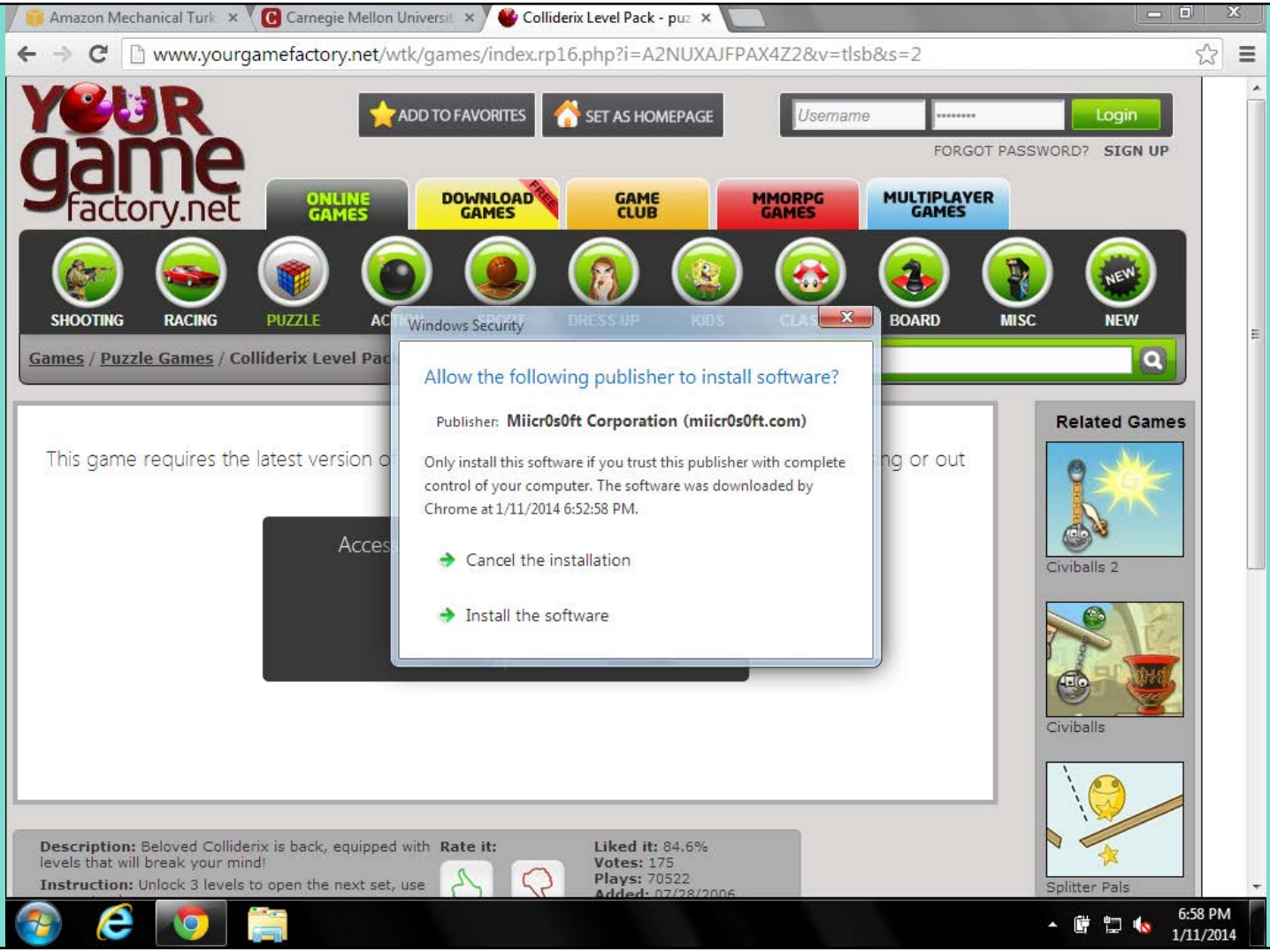

Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.

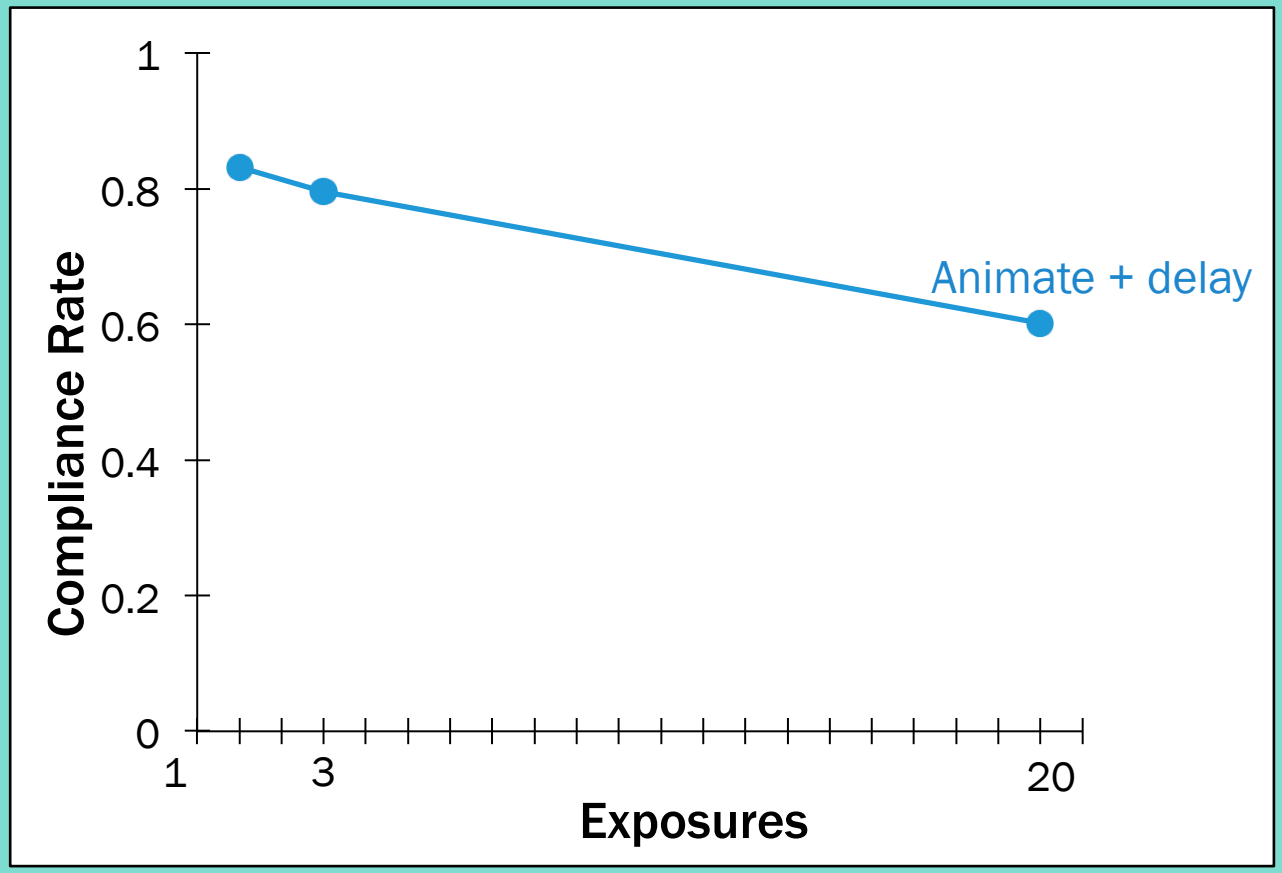

Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.


Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.

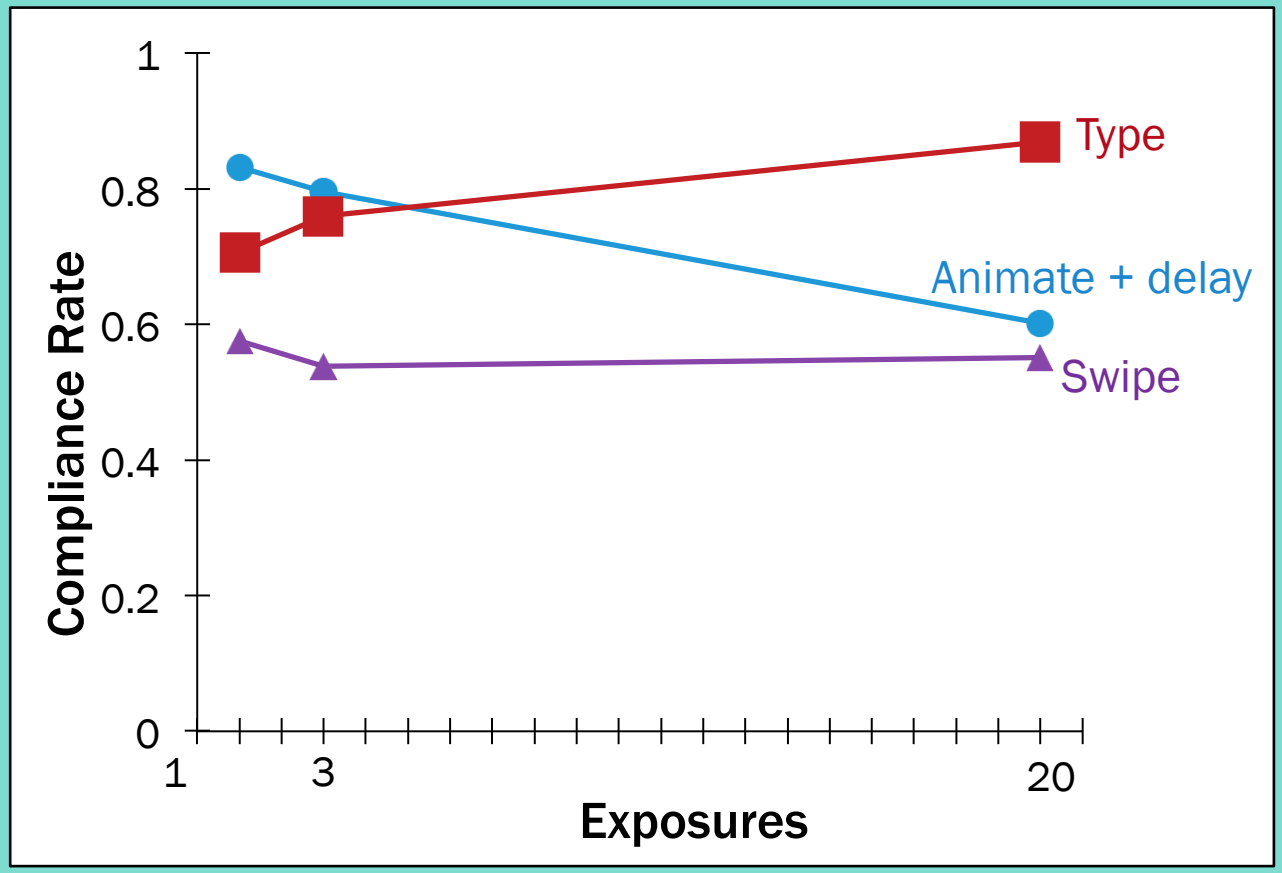

Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.


Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
miicr0s0ft corpo
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.

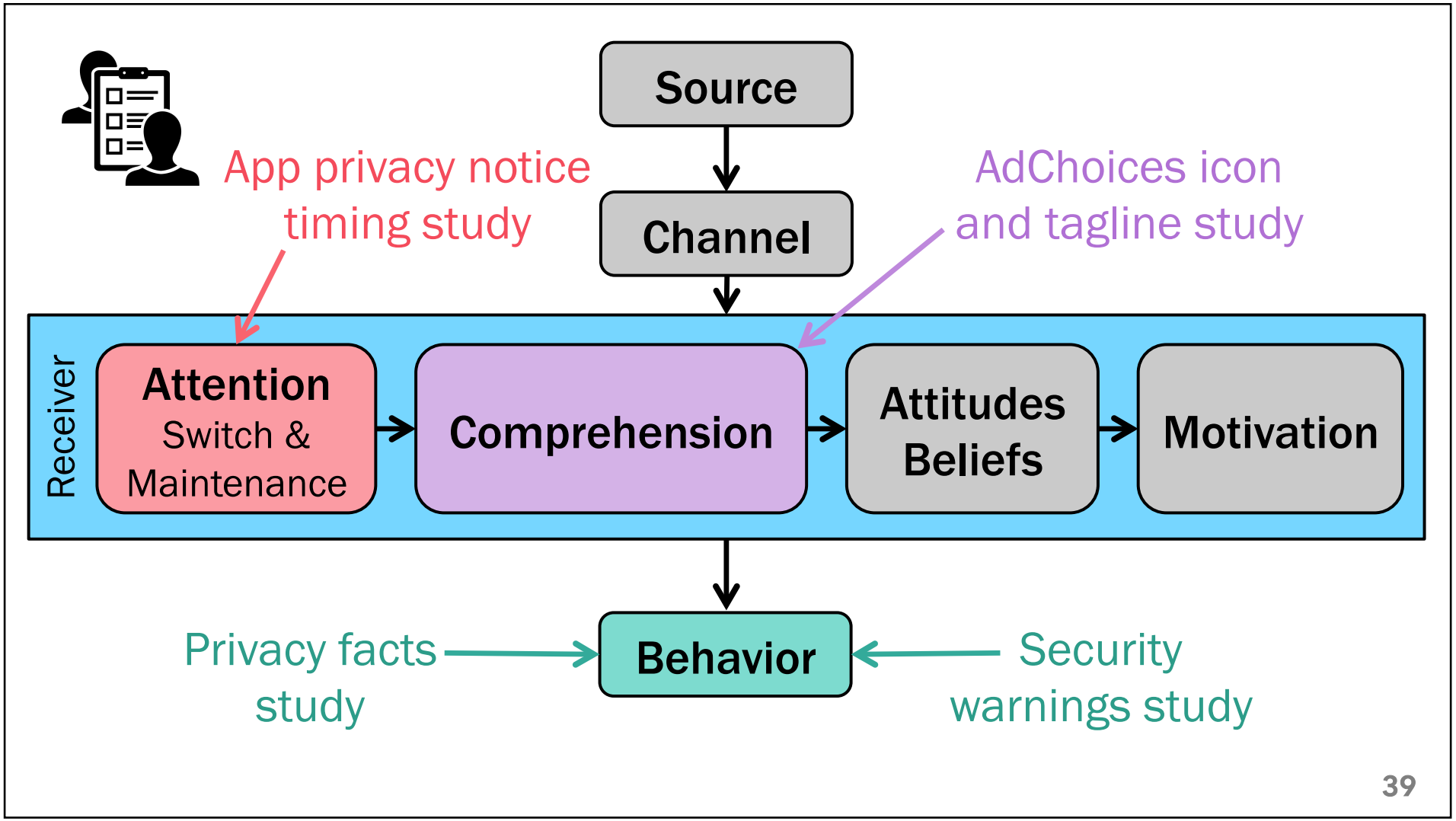

Amazon Mechanical Turk
Carnegie Mellon Universit
Colliderix Level Pack - puz
www.yourgamefactory.net/wtk/games/index.rp16.php?i=A2NUXAJFPAX4Z2&v=tlsb&s=2
YOUR game factory.net
ADD TO FAVORITES
SET AS HOMEPAGE
Username
Login
FORGOT PASSWORD? SIGN UP
ONLINE GAMES
DOWNLOAD GAMES
GAME CLUB
MMORPG GAMES
MULTIPLAYER GAMES
SHOOTING
RACING
PUZZLE
BOARD
MISC
NEW
Games / Puzzle Games / Colliderix Level Pac
Windows Security
Allow the following publisher to install software?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
Only install this software if you trust this publisher with complete control of your computer. The software was downloaded by Chrome at 1/11/2014 6:52:58 PM.
Cancel the installation
Install the software
This game requires the latest version
Related Games
Civiballs 2
Civiballs
Splitter Pals
Description: Beloved Colliderix is back, equipped with levels that will break your mind!
Instruction: Unlock 3 levels to open the next set, use
Rate it:
Liked it: 84.6%
Votes: 175
Plays: 70522
6:58 PM
1/11/2014



C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, M. Sleeper. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. SOUPS 2014.



C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, M. Sleeper. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. SOUPS 2014.


Source
Channel
App privacy notice timing study
AdChoices icon and tagline study
Receiver
Attention
Switch & Maintenance
Comprehension
Attitudes Beliefs
Motivation
Behavior
Privacy facts study
Security warnings study


Putting Disclosures to the Test
an FTC Workshop
September 15, 2016
Important to test, even on low budget
Test comprehension in context
ftc.gov/testingdislosures

cups.cs.cmu.edu

CMU research discussed in this talk was funded in part by grants from the National Science Foundation, DARPA Brandeis, US Army Research Office, The Privacy Projects, and Google

Creative Commons image credits for icons on slide 5: ludmil and Miroslav Kosa from Noun Project

Carnegie Mellon University

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy



CyLab Security and Privacy Institute

privacy ENGINEERING