

Study Method

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

27/01/2026



THE UNIVERSITY
of EDINBURGH

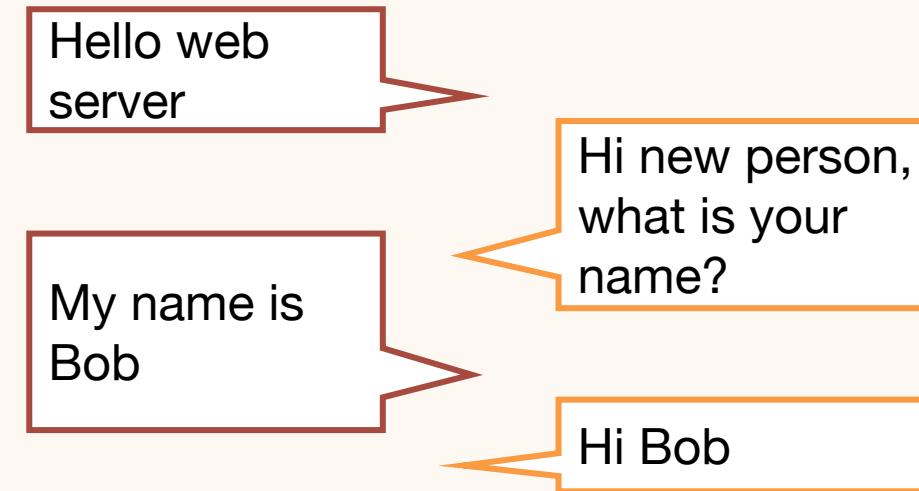
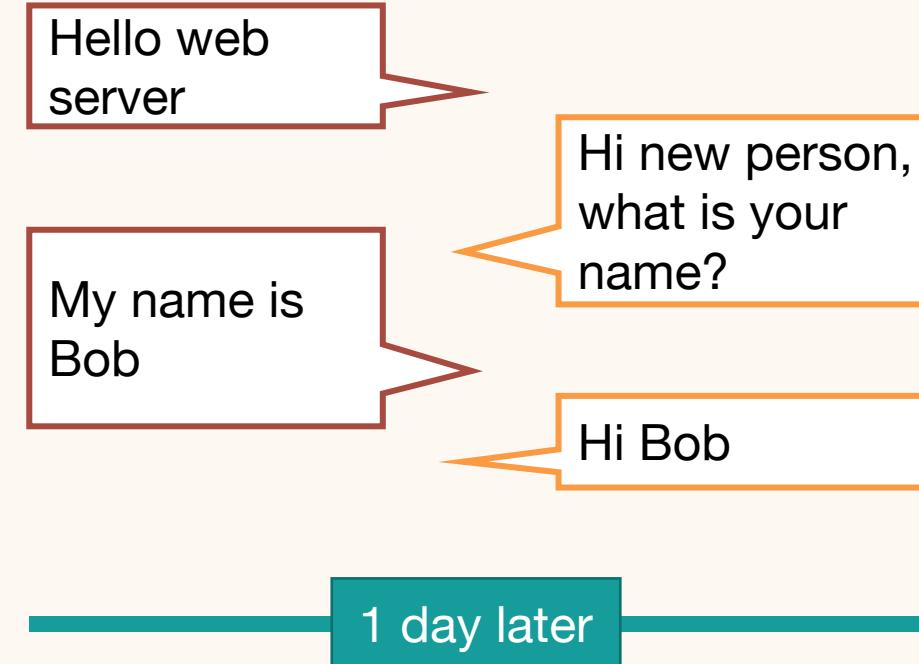
What is a cookie?

What does “opt-out” mean?

Designing the web cookie

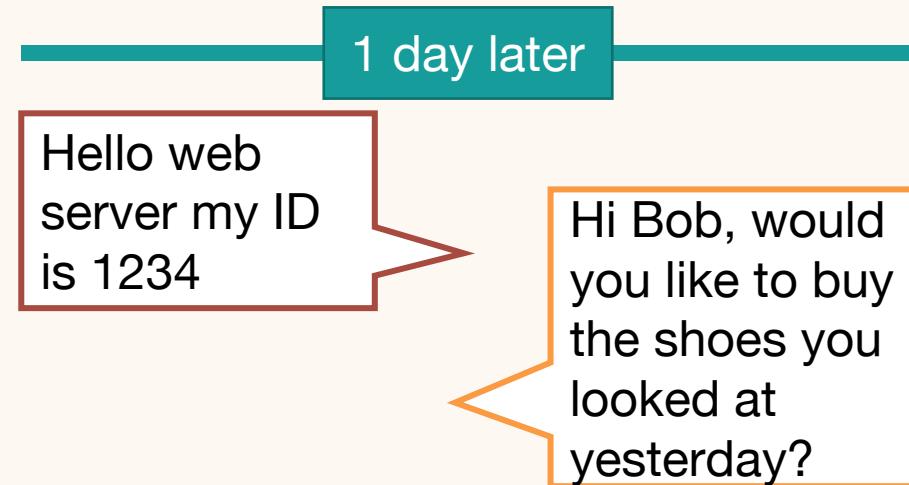
Heavily based on Lou Montulli's "The reasoning behind Web Cookies"

The year is 1994 and there is a problem... the internet has no ability to remember a person between page reloads.

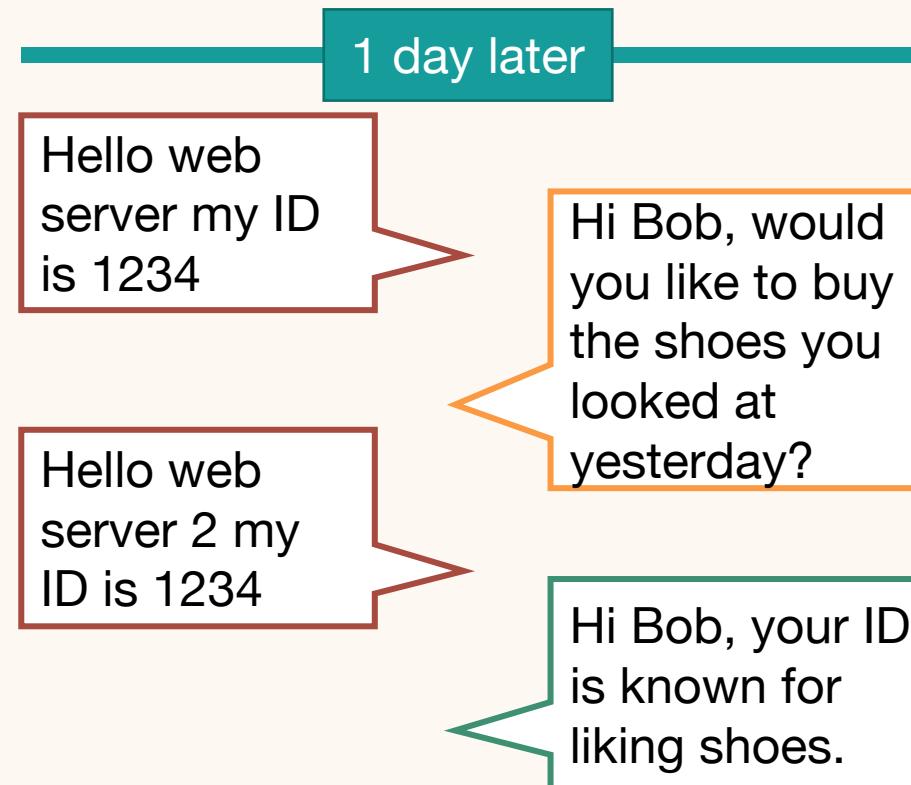


There is an obvious easy solution...

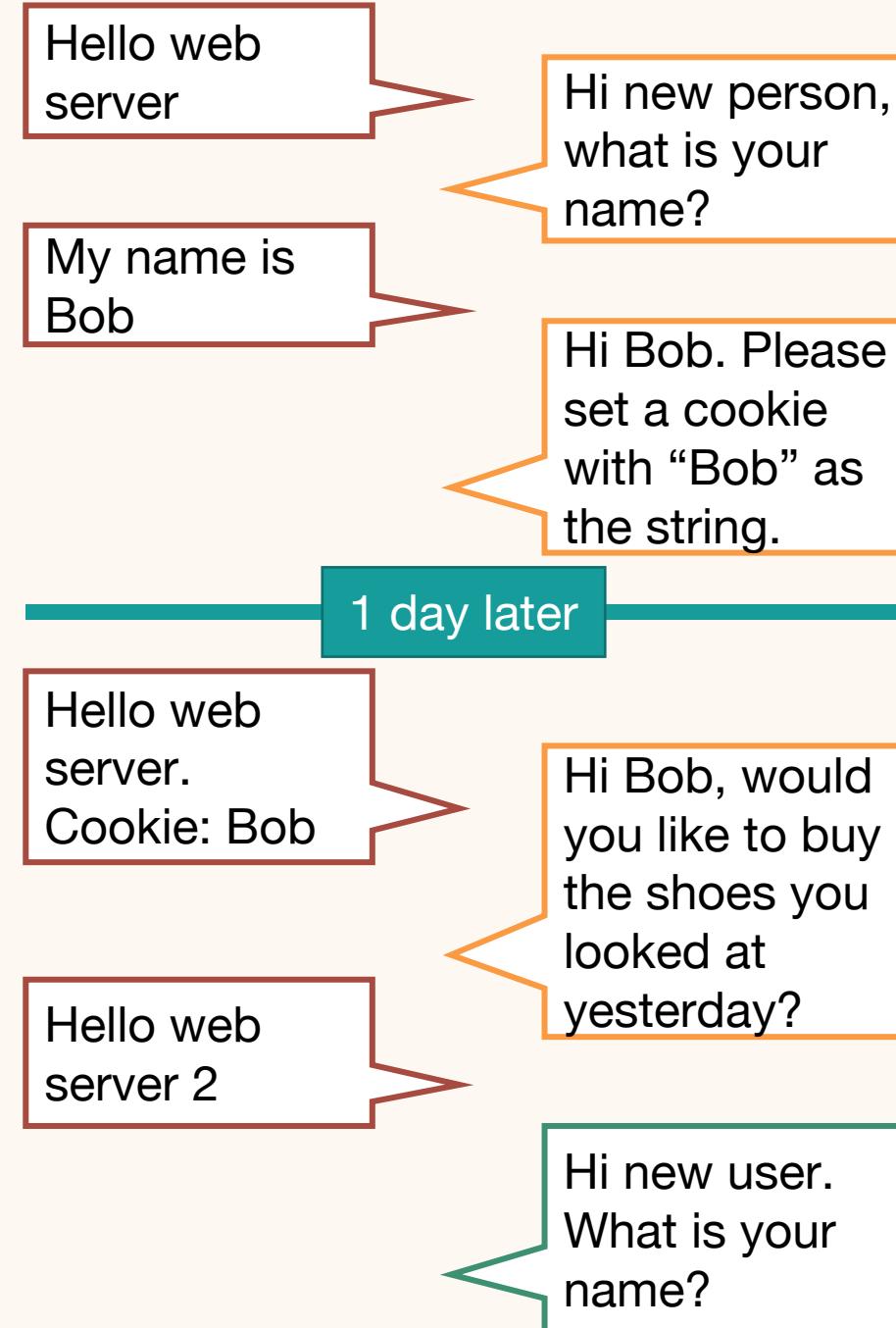
Give each browser a unique identifier that gets sent with every page request.



The problem with the obvious solution is privacy. Tracking would be possible with no visibility or control.



Instead Netscape implemented cookies. Small text strings the server could ask the browser to remember and give back to it later.



Giuliani's slipshod strategy backfires spectacularly on Trump



His surreal one-man messaging war caps a 10-month journey to the center of Trump's impeachment battle

Poll: Majority of US says impeachment inquiry is necessary

Fact-check in real time: Tapper calls out Republican's claims

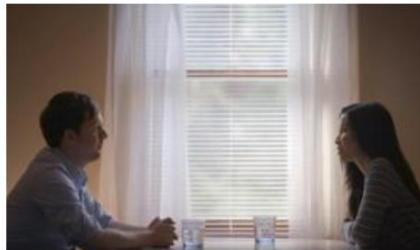
Ukraine: Sense of alarm that country will be victim of fallout

Pelosi: What Trump told me hours before impeachment inquiry

Top stories



Hong Kong protesters hit with blue water cannon after demonstrations turn violent



Addicted to porn at age 12. This is what he wants parents to know

Around the world



Politician's seized luxury supercars auctioned off

US sprinter crowned fastest man on earth

Secret-video scandal brought him down. Now controversial leader is set to return

Featured



Ferrari implosion gifts Hamilton surprise win



China preparing to show off some incredible weaponry

Response cookies

countryCode:

domain: .cnn.com
path: /
value: GB

geoData:

domain: .cnn.com
path: /
value: berwick-upon-tweed|NBL|td15 1ph|GB|EU|100|broadband

tryThing00:

domain: .cnn.com
expires: 2019-07-01T00:00:00.000Z
path: /
value: 0476

Request cookies

_gads: ID=eca290ce4d2041cd:T=1550155631:S=ALNI_MbVJ-s8-hThPxcDDEVC-y0zl6uXAg

_qca: P0-1596947158-1550155632110

_cb: Dhc35fR8rJzdliKh

_cb_ls: 1

_chartbeat2: .1550155641619.1551437811203.1000000000000001.L-wxqd_EyStJpiWfCFzknRDzs-BQ.1

ajs_anonymous_id: "65b0b48c-adf2-4b2c-8222-c00a3afcb635"

ajs_group_id: null

ajs_user_id: null

AMCV_7FF852E2556756057F000101@AdobeOrg: -1303530583|MCAID|2E32BFB58507EBAA-

6000010D8000C7E9|MCIDTS|18169|MCMID|920561

94144261380875921726535507589307|MCOPTOU

T-1569799377s|NONE|vVersion|3.3.0

AMCVS_7FF852E2556756057F000101@AdobeOrg: 1

countryCode: GB

FastAB: 0=9601,1=8428,2=6647,3=9874,4=7635,5=8957,6=3720,7=9919,8=5094,9=8302

geoData: berwick-upon-tweed|NBL|td15 1ph|GB|EU|100|broadband

gig_hasGmid: ver2

Who is tracking you?

3rd party cookie reasoning

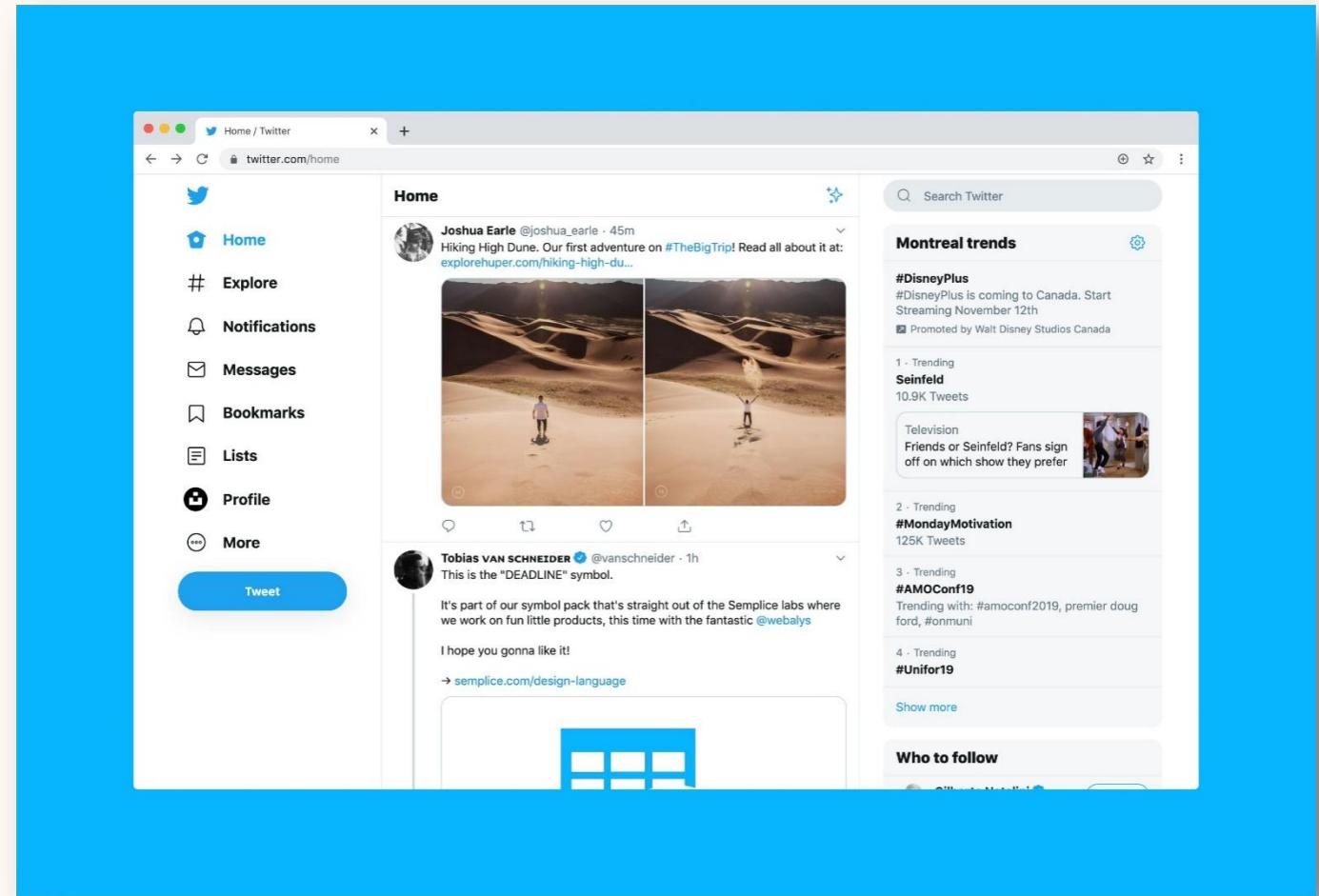
“Any company that had the ability to track users across a large section of the web would need to be a large publicly visible company.

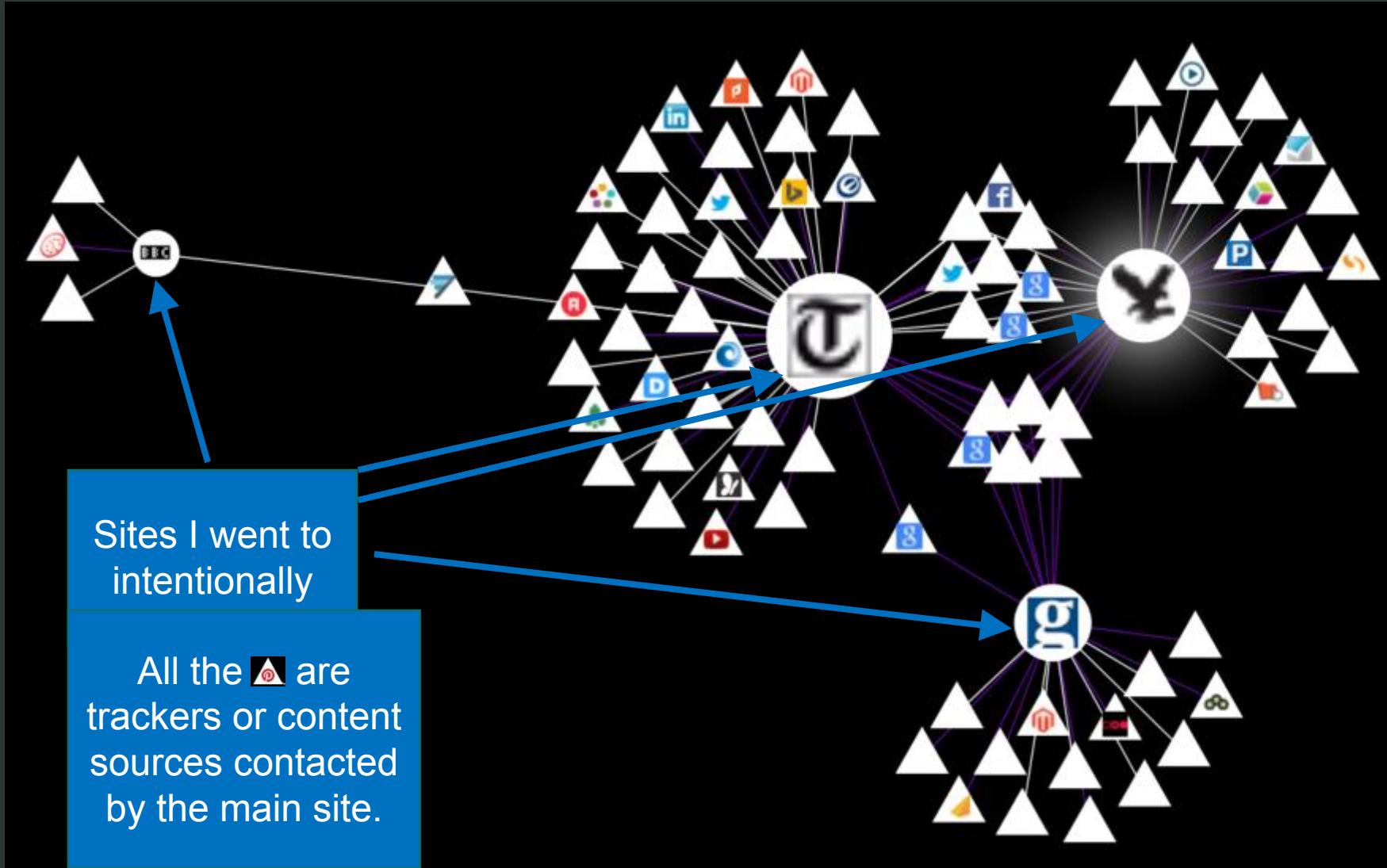
Cookies could be seen by users so a tracking company can't hide from the public.

In this way the public has a natural feedback mechanism to constrain those that would seek to track them.”

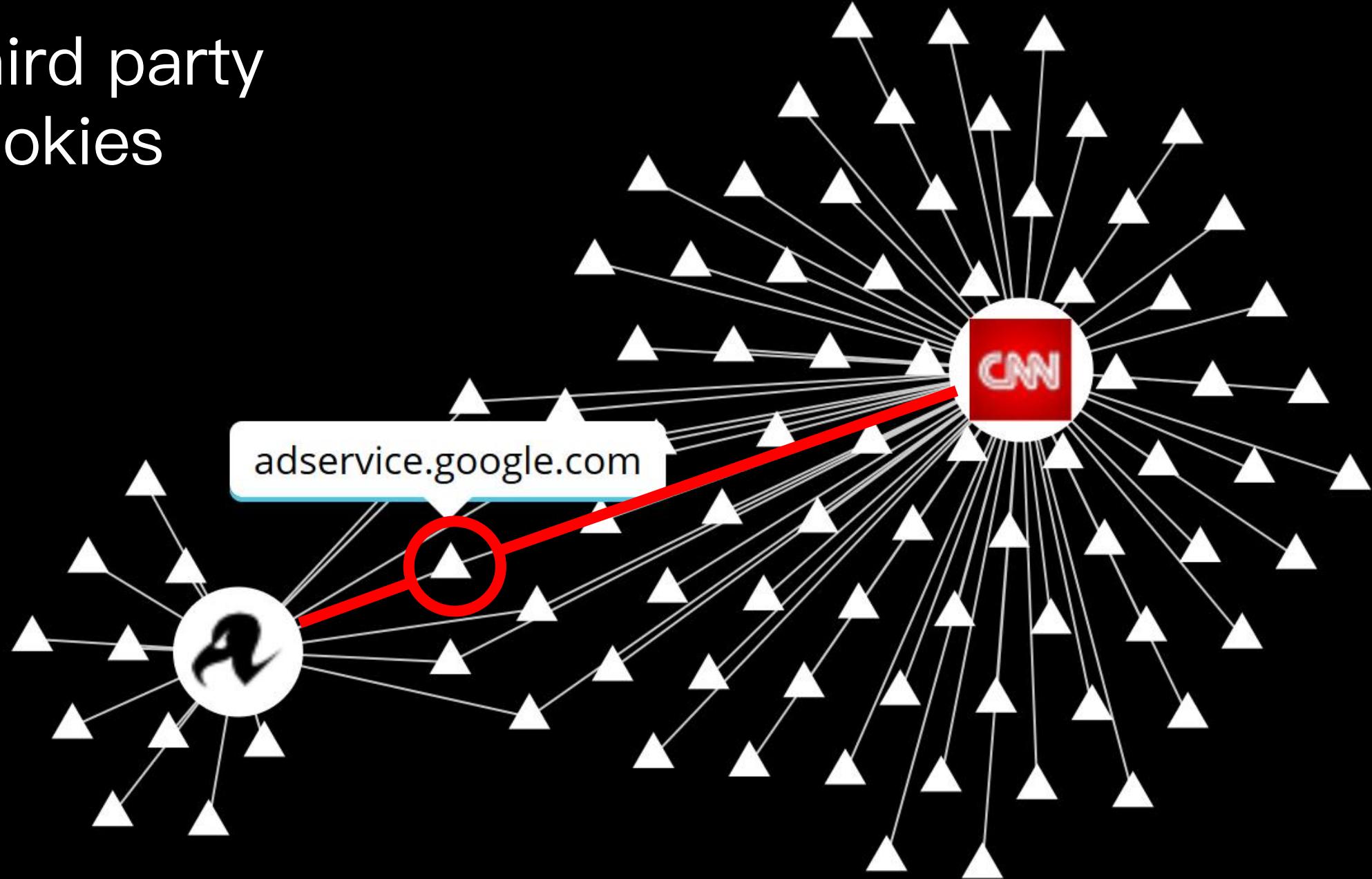
— Lou Montulli

Websites are made up of many elements from many sources





Third party cookies



| | | |
|---|----------|--------|
| Name | Protocol | Method |
| view?xai=AKAOjssvMM_k3wzigmDs9iUYGjotBAAvny... https://securepubads.g.doubleclick.net/bcs/ | HTTP/2 | ^ |

Headers **Body** **Parameters** **Cookies** **Timings**

Request URL: <https://tags.bluekai.com/site/4538?id=03F...>

Request Method: GET

Status Code: 200 / OK

Request Headers

Accept: image/png, image/svg+xml, image/*; q=0.8, */*; q=0.5

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US, en; q=0.5

Connection: Keep-Alive

Cookie: bkdc=phx; bku=5LD99vg/jP0PYpyb

Host: tags.bluekai.com

Referer: <https://stags.bluekai.com/site/50134?ret=html&id=03F...>

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.89 Safari/537.36

style-installer.js
<https://raw.githubusercontent.com/ampproject/amphm...>

The Register
Biting the hand that feeds IT

[DATA CENTRE](#) [SOFTWARE](#) [SECURITY](#) [DEVOPS](#) [BUSINESS](#) [PERSONAL TECH](#) [SCIENCE](#) [EMERGENT TECH](#) [BOOTNOTES](#) [LECTURES](#)

[Twitter](#) [Facebook](#) [8+](#) [LinkedIn](#)



GPS is Doomed (No Joke)

The World Economy runs on GPS. It needs a backup plan.

XY

TOP STORIES



Oh Snap! Gimme-root-now security bug lets miscreants sock it to your Ubuntu boxes
Get an update, or risk giving a dodgy user or malware an upgrade

Take your pick: Linux on Windows 10 hardware, or Windows 10 on Linux hardware
We can't see the Arm in having a little tinker

Pandas so useless they just look at delicious kid who fell into enclosure
Urgh, you're infuriating!

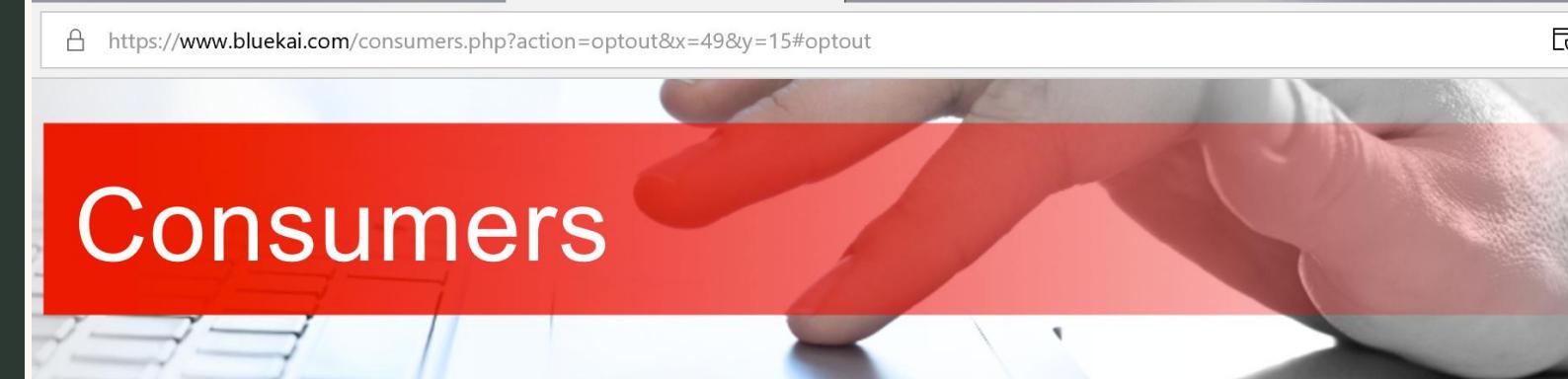
A once-in-a-lifetime Opportunity: NASA bids emotional farewell to its cocky, hardworking RC science car on Mars
Amazing what you can achieve on unforgiving dust world over 15 years with a 20MHz RISC CPU and a bunch of probes

We use cookies to improve performance, for analytics and for advertising. You can manage your preferences at any time by visiting our cookie policy. [Ok](#)

14

So I went to BlueKai's opt-out page and asked to opt-out.

Doing so set a cookie so that the next time I visit a site using BlueKai tracker the cookie tells the site not to track me.



Oracle's stance on consumer transparency

Oracle believes that participants in the online advertising industry should:

- Provide consumers with insight into how interest-based advertising occurs.
- Help consumers understand the benefits of interest-based advertising.
- Provide consumers with tools to enable choice.

To this end, Oracle provides the following tools for consumers. For more information about Oracle's involvement with interest-based advertising and these tools, please visit the [Oracle Marketing Cloud & Oracle Data Cloud Privacy Policy](#)

Opt Out Tool

Your cookie is currently opted out. To opt back in please clear cookies on your browser.

- ✓ You may also opt-out through certain industry group websites. See the "Opting-Out" section of the [Oracle Marketing Cloud & Oracle Data Cloud Privacy Policy](#) for more information. Use of these opt-outs will allow you to opt out of online targeting enabled by Oracle Data Cloud services as well as other member companies.
- ✓ For information about the effect of opting out and other important considerations, please see the "Opting-Out" section of the [Oracle Marketing Cloud & Oracle Data Cloud Privacy Policy](#).

Registry Tool

Oracle provides a tool, called the Oracle Data Cloud Registry, that allows consumers to see the types of interest data associated with the Oracle Data Cloud cookies deposited within the consumer's web browser. [Click here](#) to view the Oracle Data Cloud Registry. At the Registry, consumers can delete individual interest segments at their discretion. For information about the Oracle Data Cloud Registry, please see the "Accessing and Removing Interest Data" section of the [Oracle Marketing Cloud & Oracle Data Cloud Privacy Policy](#).

Featured Article

Oracle's BlueKai tracks you across the web. That data spilled online

Billions of records exposed.

Zack Whittaker [@zackwhittaker](#) / 3:30 PM GMT+1 • June 19, 2020



BEFORE OPT-OUT

| Headers | Body | Parameters | Cookies | Timings |
|--|------|------------|---------|---------|
| Request URL: https://tags.bluekai.com/site/4538?id=03F... | | | | |
| Request Method: GET | | | | |
| Status Code: 200 / OK | | | | |
| Request Headers | | | | |
| Accept: image/png, image/svg+xml, image/*; q=0.8, */*;... | | | | |
| Accept-Encoding: gzip, deflate, br | | | | |
| Accept-Language: en-US, en; q=0.5 | | | | |
| Connection: Keep-Alive | | | | |
| Cookie: bkdc=phx; bku=5LD99vg/jP0PYpyb | | | | |
| Host: tags.bluekai.com | | | | |
| Referer: https://stags.bluekai.com/site/50134?ret=html&... | | | | |
| User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)... | | | | |

AFTER OPT-OUT

| Headers | Body | Parameters | Cookies | Timings |
|--|------|------------|---------|---------|
| Request URL: https://stags.bluekai.com/site/50134?ret=h... | | | | |
| Request Method: GET | | | | |
| Status Code: 200 / OK | | | | |
| Request Headers | | | | |
| Accept: text/html, application/xhtml+xml, application/x... | | | | |
| Accept-Encoding: gzip, deflate, br | | | | |
| Accept-Language: en-US, en; q=0.5 | | | | |
| Connection: Keep-Alive | | | | |
| Cookie: bku=0000000000000000; BKIgnore=1; bkdc=phx | | | | |
| Host: stags.bluekai.com | | | | |
| Referer: https://www.nytimes.com/ | | | | |
| Upgrade-Insecure-Requests: 1 | | | | |
| User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)... | | | | |

BTW, why “cookie”?

- “Magic cookie”: a token or short packet of data passed between communicating programs



- (Web) cookie

Opting out causes the page to set an “opt out” cookie that is typically blank or all 0’s.

Instead of sending a cookie with a tracking number, your browser will now instead send the blank cookie, preventing the site from tracking you.

Are Cookie opt-out options really effective? How do people actually configure opt-out options?

Why we need to conduct a study?

- **Assess needs:** what should we build?
- **Examine trade-offs:** which features/approaches best fit needs?
- **Evaluate:** are requirements met? what can we improve?
- **Finding root causes:** what underlying problems need to be fixed?

Why we need to conduct a study?

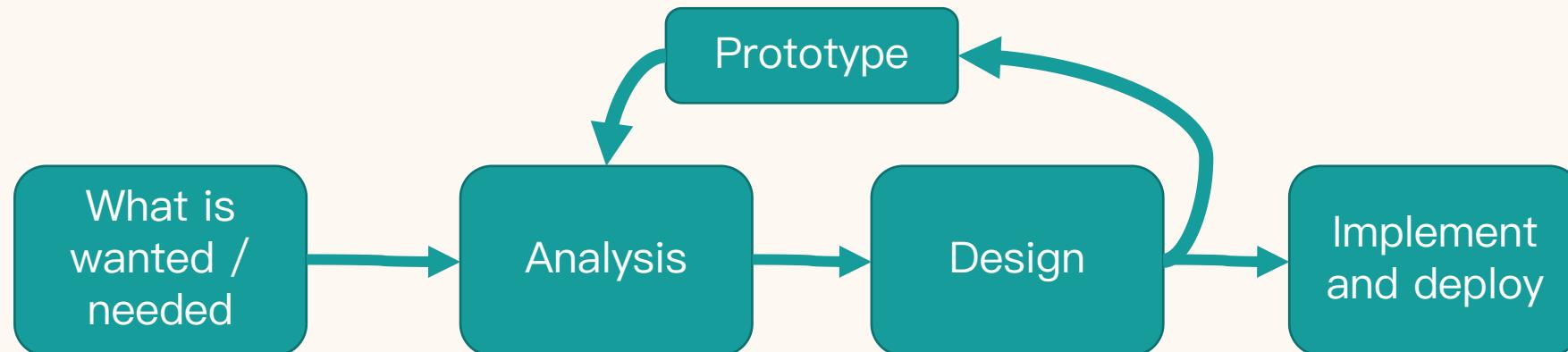
- **Assess needs:** a better cookie notice?
- **Examine trade-offs:** which placement is more accessible?
- **Evaluate:** how fast/accurate people do opt-out?
- **Finding root causes:** dark pattern?

Why we need to conduct a study?

- Assess needs
- Examine trade-offs
- Evaluate
- Finding root causes

*CMU USEC

Project lifecycle



Before we actually start

- Identify research questions
- Decide on the type of study and demographics
- Design study protocol
- Obtain ethics approval
- Design study
- Pilot studies
- Revise study....

Ethics guidelines



The Informatics ethics procedure is in place to ensure that all research conducted in the School abides by the required ethical standards. To this end, the School follows a set of guiding principles which are in line with those of the College and University. There is more information on the School's ethics and integrity guiding principles under the tab of the same name.

[Ethics and integrity guiding principles](#)

Since the implementation of the UK General Data Protection Regulation (UK GDPR) in 2018, the School is making increased efforts to ensure any project working with personal data takes the appropriate steps to ensure secure handling of personal information. For a summary of the relevance of the UK GDPR in ethical research, see [Ethics and the UK GDPR](#).

[Ethics and the UK GDPR](#)

Each project in the School of Informatics needs to be reviewed by the ethics committee. Since June 2019, this can be done by completing the online Informatics ethics form. The form guides the PI through mandatory questions and a data protection impact assessment (DPIA) as required, as well as prompting the user to produce relevant documents (e.g. consent forms). Once submitted, the committee will aim to reply within 10 working days. The online form as well as a PDF reference are available under the [Ethics procedure](#) tab.

[Ethics procedure](#)

<https://uoe.sharepoint.com/sites/inf-researchservices/SitePages/Ethics-and-integrity.aspx>

Testing Usability...How?

Many ways to test usability

- A/B Testing
- Affinity Diagramming
- Card Sorting
- Case Studies
- Cognitive Walkthrough
- Competitive Testing
- Critical Incident Technique
- Customer Experience Audit
- Desirability Testing
- Diary Studies
- Ergonomic Analysis
- Experience Sampling
- Experiments
- Eye tracking
- Fly-on-the-wall Observation
- Focus Groups
- Graffiti Walls
- Heuristic Evaluation
- Interviews
- KJ Technique
- Observation
- Participatory Action Research

A LANDSCAPE OF USER RESEARCH METHODS

Behavioral – measures how people actually behave, what they do.

Attitudinal – measures what people say they think or how they say they behave.

BEHAVIORAL

ATTITUDINAL

QUALITATIVE (DIRECT)

QUANTITATIVE (INDIRECT)

KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

● Natural use of product

■ Scripted (often lab-based) use of product

▲ De-contextualized / not using product

◆ Combination / hybrid

A LANDSCAPE OF USER RESEARCH METHODS

Qualitative – unstructured data such as natural language.

Quantitative – numerical data. Anything that can be counted or measured with numbers.

BEHAVIORAL

Usability Lab Studies

Ethnographic Field Studies

ATTITUDINAL

Participatory Design
Focus Groups
Interviews

Eyetracking

Usability Benchmarking (in lab)

Moderated Remote Usability Studies

Unmoderated Remote Panel Studies

Unmoderated UX Studies

Clickstream Analysis
A/B Testing

True Intent Studies

Concept Testing

Diary/Camera Studies

Customer Feedback

Desirability Studies

Card Sorting

Intercept Surveys

Email Surveys

QUALITATIVE (DIRECT)

QUANTITATIVE (INDIRECT)

KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

Natural use of product

Scripted (often lab-based) use of product

De-contextualized / not using product

Combination / hybrid

A LANDSCAPE OF USER RESEARCH METHODS

Qualitative – unstructured data such as natural language.

Quantitative – numerical data. Anything that can be counted or measured with numbers.

BEHAVIORAL

Usability Lab Studies

Ethnographic Field Studies

ATTITUDINAL

Participatory Design
Focus Groups
Interviews

Eyetracking

Usability Benchmarking (in lab)

Moderated Remote Usability Studies

Unmoderated Remote Panel Studies

Unmoderated UX Studies

Clickstream Analysis
A/B Testing

True Intent Studies

Concept Testing

Diary/Camera Studies

Customer Feedback

Desirability Studies

Card Sorting

Intercept Surveys

Email Surveys

QUALITATIVE (DIRECT)

QUANTITATIVE (INDIRECT)

KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

Natural use of product

Scripted (often lab-based) use of product

De-contextualized / not using product

Combination / hybrid

Interviews — users express their attitudes by providing qualitative answers to questions.

Clickstream Analysis — measure the links users click on to get quantitative data on what users do.



A LANDSCAPE OF USER RESEARCH METHODS

Lab Studies – users perform a set of tasks often talking about their experience as they do so.

Surveys – Ask about user opinion often with multiple choice answers.

BEHAVIORAL

Artefact Analysis

Usability Lab Studies

Ethnographic Field Studies

ATTITUDINAL

Participatory Design
Focus Groups
Interviews

QUALITATIVE (DIRECT)

● / ■ Eyetracking

■ Usability Benchmarking (in lab)

■ Moderated Remote Usability Studies

■ Unmoderated Remote Panel Studies

● Clickstream Analysis
● A/B Testing

■ Unmoderated UX Studies
● True Intent Studies

◆ ← Concept Testing →

● Diary/Camera Studies

● Customer Feedback

◆ ← Desirability Studies →

◆ ← Card Sorting →

● Intercept Surveys

△ Email Surveys

QUANTITATIVE (INDIRECT)

KEY FOR CONTEXT OF PRODUCT USE DURING DATA COLLECTION

● Natural use of product

■ Scripted (often lab-based) use of product

△ De-contextualized / not using product

◆ Combination / hybrid

Think–pair–share

For each of the following problems, name one behavioral question you could ask and one attitudinal question.

- Mobile phone login
- Cookie dialogs
- Fake news
- Encryption of all webpages by default

Lab studies are a simple idea. You ask a user to come into a physical space and ask them to interact with the interface there.

Lab Study

- Basic idea: Have a participant come to a physical place (lab) and interact with the interface there
- You setup the lab so it mimics the situation you want to test
- Pros
 - Full control over the environment so limited confounds
 - Detailed data from each subject
 - Ability to ask them why they did something
- Cons
 - Small sample sizes
 - Being in the lab changes user behavior. They feel safer and their normal distractions are gone. That can be bad for deception studies.

Is it really simple?

What is different about security

- Large **information asymmetry** between participant and researcher
 - The researcher likely understand security of their tool
 - Participant likely doesn't even know that security problem exists
- **Deception** studies are common
 - You told the participant to accomplish task A, but you are really looking to see if they do B activity

Why Johnny Can't Encrypt

In Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 169-183

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 this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

ive when used
ovably correct
ovide security if
to click on the
y, give up on a
re too confused
need to use, or
rol mechanisms
able. Problems
s: at least one
ration errors are

Users need to:

- understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people
- understand that authentication is achieved through digital signatures, and figure out how to sign email and how to verify signatures on email from other people
- understand that in order to sign email and allow other people to send them encrypted email a key pair must be generated, and figure out how to do so
- understand that in order to allow other people to verify their signature and to send them encrypted email, they must publish their public key, and figure out some way to do so
- understand that in order to verify signatures on email from other people and send encrypted email to other people, they must acquire those people's public keys
- manage to avoid such dangerous errors as accidentally failing to encrypt, trusting the wrong public keys, failing to back up their private keys, and forgetting their pass phrases
- be able to succeed at all of the above within a few hours of reasonably motivated effort

Tested usability using two methods

- Cognitive Walkthrough
 - A set of experts review and the experts make an informed guess about what will be problematic
 - Paired with heuristics – The experts state how the user interface supports or violates common HCI principles (Heuristics)
- Lab Study
 - Ask the participant to perform a set of tasks
 - Very similar to a think aloud, but without the talking aloud part

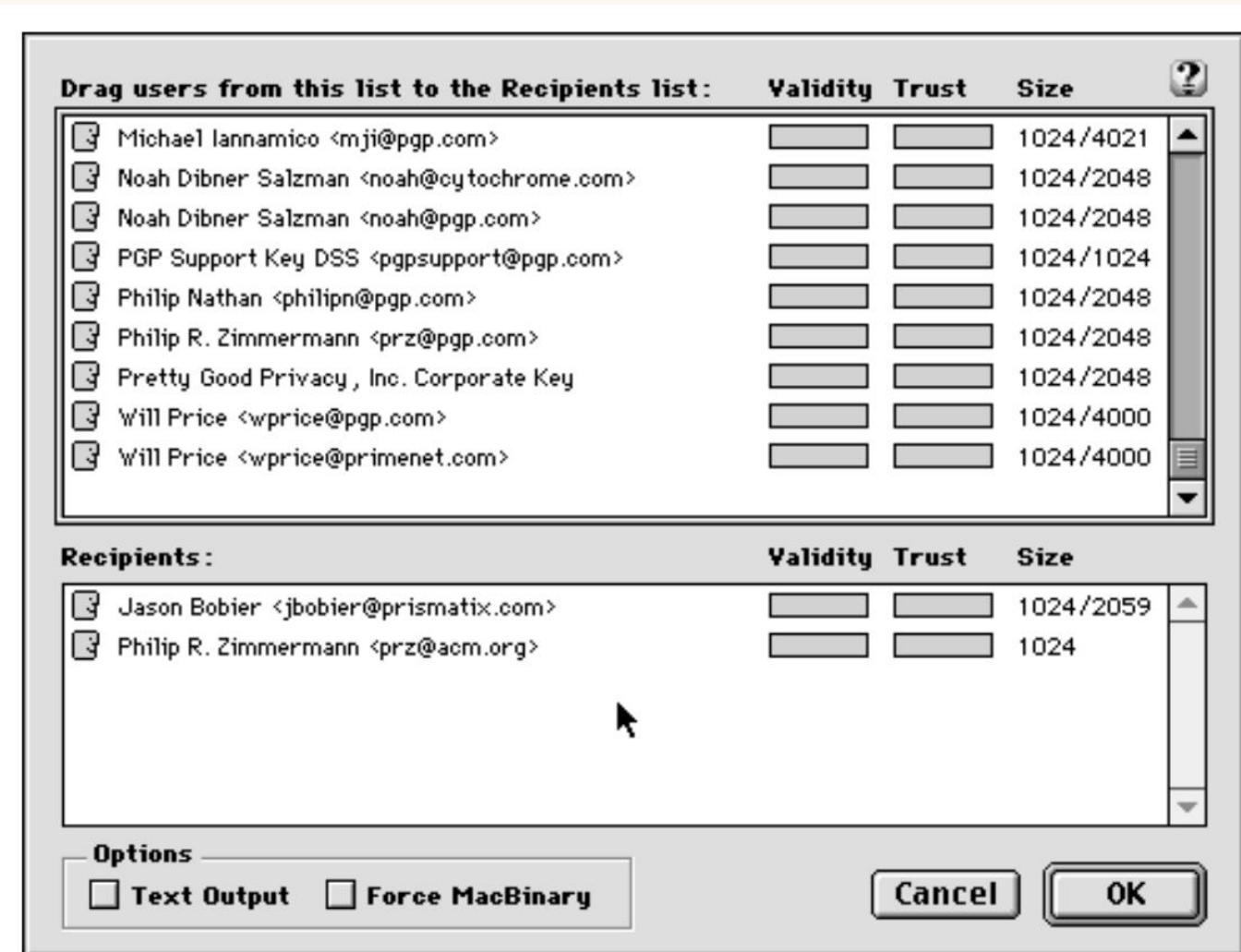
Cognitive walkthrough outcomes

- **Visual metaphors** – Do key and lock pictures make sense?
- **Different key types** – Public vs private keys, or maybe signing and encryption keys?
- **Key server** – Used for sharing keys
- **Key management policy** – Trust and validity ratings
- **Consistency** – Use of the same terms everywhere
- **Too much information** – Information like key size, hashes, and trust
- **Irreversible actions**
 - Accidentally deleting the private key
 - Accidentally publicizing a key
 - Accidentally revoking a key
 - Forgetting the pass phrase
 - Failing to back up the key rings

Lab study

- 12 participants with CS backgrounds
- Participant had to send several emails to team members (the researchers)
 - Creating a key pair
 - Sending their public key to team members
 - Getting team members' public keys
 - Sending the email
 - Decrypting response email
- 3 – emailed the private key to the team member
 - 1 never realized the error
- 1 – forgot their pass phase and had to re-generate keys
- 1 – never figured out how to encrypt
- 7 – used their public keys to encrypt
 - 1 created a separate key pair for each team member
- 3 – successfully sent an encrypted email to the whole team and were able to decrypt an response email

Whitten and Tygar evaluated PGP encryption in 1999, surely it must be more usable now.



A personal story during my PhD

Kaleido: Real-Time Privacy Control for Eye-Tracking Systems

Jingjie Li, Amrita Roy Chowdhury, Kassem Fawaz, and Younghyun Kim

University of Wisconsin–Madison

{jingjie.li, roychowdhur2, kfawaz, younghyun.kim}@wisc.edu

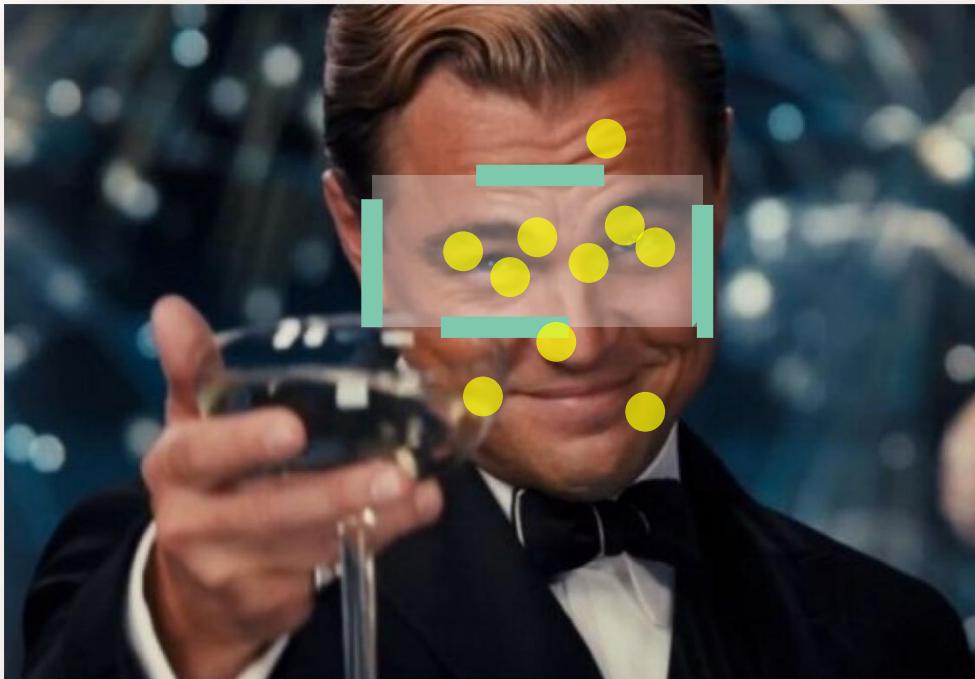
Abstract

Recent advances in sensing and computing technologies have led to the rise of eye-tracking platforms. Ranging from mobiles to high-end mixed reality headsets, a wide spectrum of interactive systems now employs eye-tracking. However, eye gaze data is a rich source of sensitive information that can reveal an individual's physiological and psychological traits. Prior approaches to protecting eye-tracking data suffer from two major drawbacks: they are either incompatible with the current eye-tracking ecosystem, or provide no formal



Figure 1: Eye gaze heatmaps from an individual user with and without Kaleido's noising effect on a web page.

Privacy Implications of Eye Tracking



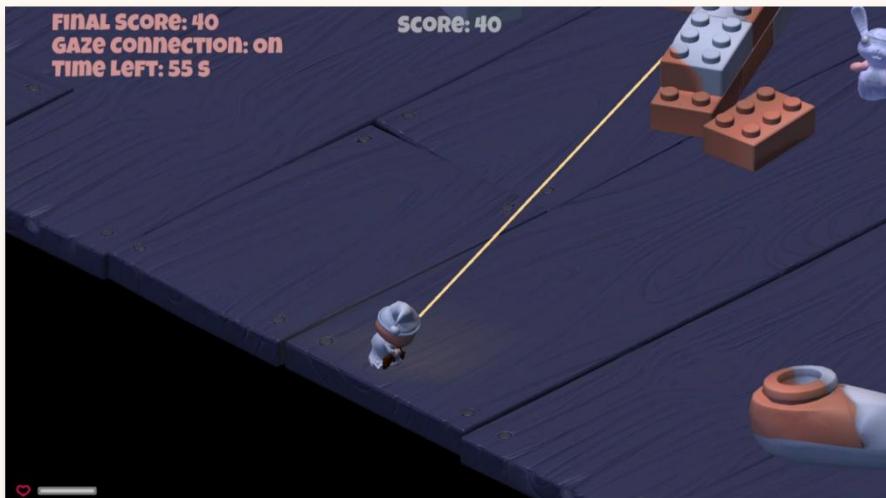
Eye gazes from people with **low social anxiety**



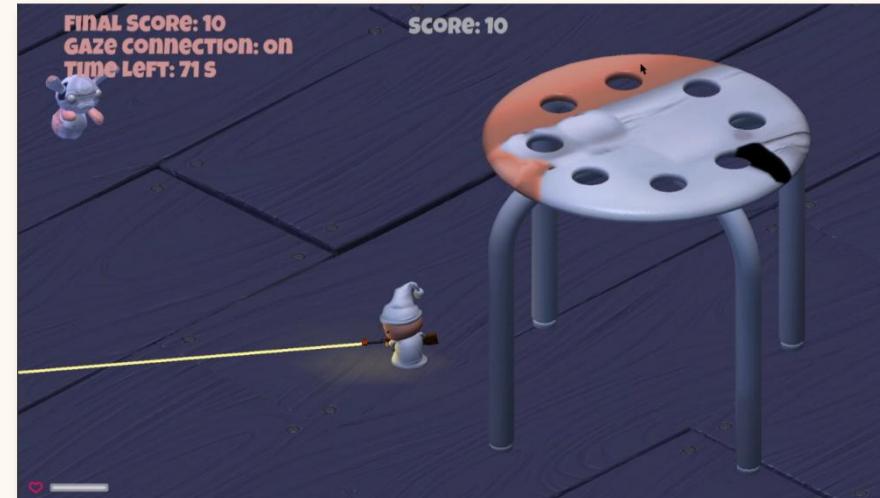
Eye gazes from people with **high social anxiety**

Some background

- Test out whether/how user experience is impacted by a privacy control we designed in an eye tracking game setting



Kalido off



Kalido on

How to do user studies?



My original plan in
03/2020 to do lab
studies with a VR
setup

Then...Guess what?

| | | |
|--|--|-----------|
|  WG | WISEST Group Meeting 0707 ≈ Call ended - 30m 55s | 7/7/2020 |
|  WS | WISEST Seminar ≈ Call ended - 33m 44s | 6/23/2020 |
|  | ≈ Call ended - 3m 23s | 6/16/2020 |
|  MN | Meet Now ≈ Call ended - 51m 34s | 6/11/2020 |
|  JS | Jingjie study ████████ has left this conversation | 6/11/2020 |
|  WS | WISEST Seminar ≈ Call ended - 54m 11s | 6/2/2020 |

“The remote user study design was approved by the Institutional Review Board (IRB) of our institution... Each remote session took 35 minutes on average, and we provided each participant with \$15 worth of supplies as a token of appreciation for participating.”

Questions

Take-home

- Zhang, Z., Jia, M., Lee, H.P., Yao, B., Das, S., Lerner, A., Wang, D. and Li, T., 2024. "It's a Fair Game", or Is It? Examining How Users Navigate Disclosure Risks and Benefits When Using LLM-Based Conversational Agents. In *Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI 2024, Honolulu, HI, USA, May 11-16, 2024* (pp. 156-1). ACM.
- Reuters – DeepSeek hit by cyberattack as users flock to Chinese AI startup