



PRIVACY CON

FEDERAL TRADE COMMISSION

📍 DC // 1.14.16



Opening Remarks

Chairwoman Edith Ramirez



PRIVACY CON
FEDERAL TRADE COMMISSION



Session 1: The Current State of Online Privacy



Ibrahim Altaweel

University of California, Berkeley

Web Privacy Census v 3.0

Co-author: Nathaniel Good (Good Research)



Web Privacy Census v3.0

Ibrahim Altaweel, UC Berkeley School of Information
Nathan Good, UC Berkeley School of Information
Chris Hoofnagle, UC Berkeley School of Information

This work has been published as Altaweel I, Good N, Hoofnagle C. Web Privacy Census. *Technology Science*. 2015121502. December 15, 2015. <http://techscience.org/a/2015121502>















This work was supported in part by TRUST, Team for Research in Ubiquitous Secure Technology, which receives support from the National Science Foundation (NSF award number CCF-0424422).



We Seek to Explore

- How many entities are tracking users online?
- What technologies are most popular for tracking users?
- Is there a shift from one tracking technology to another in tracking practices?
- Is there greater concentration of tracking companies online?
- What entities have the greatest potential for online tracking and why?

Methods

RANK	SITE	MONTHLY PEOPLE	DIRECTLY MEASURED
1	 google.com	232,288,144	
2	 youtube.com	208,776,272	
3	 msn.com	165,291,680	
4	 facebook.com	130,319,464	
5	 bing.com	93,572,256	
6	 yahoo.com	86,557,024	
7	 amazon.com	82,737,184	
8	 answers.com	71,685,376	
9	 microsoft.com	68,743,296	
10	 buzzfeed.com	68,035,880	
11	 Hidden profile	—	

We collect data on the top 100, 1,000, and 25,000 websites as ranked on Quantcast's top 1 million websites in the United States in July 2015

Methods

Collected:

- HTTP Cookies, HTML5 local storage objects, Flash cookies.

Processes:

- a shallow automated crawl
- deep automated crawl

The Crawler:

- OpenWPM, a web privacy measurement platform developed by Princeton University.

Limitations

Limitations of data collection methods:

- Only browser used is Firefox 39 with no add-ons
- The crawler did not log into any sites, nor bypass any modal dialogs
- We did not capture any retargeting based on a human action (e.g., adding items to a shopping cart)
- We limited deep crawls to HTML anchor tags found and did not follow links set by JavaScript
- We did not take into account page layout and visual layout in the selection process.

Limitations

- Skipped Hidden Profiles
- The ranking list used was Quantcast's top 1 million sites in the United States. This ranking may be different in other countries.

These limitations mean that the Web Privacy Census is a conservative measure of the total amount of tracking online.

How much tracking?

- We found that users who merely visit the homepages of the top 100 most popular sites would collect over 6,000 HTTP cookies twice as many as we detected in 2012.
- Some popular websites use a lot of cookies. In just visiting the homepage of popular sites, we found that 24 websites that placed over 100 cookies, 6 websites that placed over 200 cookies, and 3 websites placed over 300.

What technologies are most popular for tracking users?

- We measured HTTP, HTML5, and Flash Cookies
- Use of Flash Cookies has decreased.
- More sites are using HTML5 storage, which enables websites to store more information about consumers.

Is there a shift from one tracking technology to another in tracking practices?

- 83% of HTTP cookies were set by third party hosts, and just in visiting the homepage of popular sites, users would have cookies placed by 275 third-party hosts.
- If the user browsed to just two more links, the number of HTTP cookies would double.

Is there greater concentration of tracking companies online?

- Google's presence on top 100 website increased from 74 in 2012 to 92 in 2015.
- Percentage of cookie set by a third party host has increased from 84.7% to 93.5%.

What entities have the greatest potential for online tracking and why?

Google:

- We found that Google tracking infrastructure is on 92 of the top 100 most popular websites and on 923 of the top 1,000 websites, providing Google with a significant surveillance infrastructure online.

Facebook:

- Facebook had a presence on 57 of top 100 websites and 548 on the top 1000 websites

Steven Englehardt

Princeton University

The Web Never Forgets....

Co-authors: Arvind Narayanan, Christian Eubank (Princeton University);
Gunes Acar, Marc Juarez, Claudia Diaz (University of Leuven)



The Web Privacy Problem is a Transparency Problem

*How OpenWPM and the Transparency Census will bring
transparency to the web.*

Steven Englehardt
@s_englehardt



webtap.princeton.edu



The New York Times - Breaking News, World News & Multimedia

The New York Times - Breaking... | http://www.nytimes.com/ | Google | Feedback

Home Page | Today's Paper | Most Popular | Times Topics | Get Home Delivery-Bay Area

Advertising **GUCCI** **The New York Times** **Advertising** see what's inside

Tuesday, February 1, 2011 Last Update: 10:16 PM ET

Search: electric | **Advertising** | Follow Us: Facebook, Twitter, YouTube | Subscribe to Home Delivery-Bay Area | Personalize Your Website

Switch to Global Edition

Mubarak **Advertising** **Week New Term** **Opposition Demands That He Leave Sooner** **OPINION**

Jobs | Real Estate | Autos | All Classifieds

WORLD | U.S. | POLITICS | NEW YORK | BUSINESS | DEALBOOK | TECHNOLOGY | SPORTS | SCIENCE | HEALTH | OPINION | ARTS | Books | Movies | Music | Television | Theater | STYLE | Dining & Wine | Fashion & Style | Home & Garden | Weddings/Celebrations | TRAVEL | All Blogs | Cartoons | Classifieds | Corrections | Crossword/Games | Education | First Look | Learning Network | Multimedia | NYC Guide | Obituaries | Podcasts | Public Editor | Sunday Magazine | T Magazine | Video

Log In With Facebook

Log in to see what your friends are sharing on nytimes.com. [Privacy Policy](#) | [What's This?](#)

WHAT'S POPULAR NOW

- The Paradox of Corporate Taxes in America
- Why Not Regulate Seriously

Social

Video

MARKETS | At 10:14 PM ET

JAPAN	CHINA	EURO
Nikkei	HangSeng	Shanghai
18,470.50	23,828.39	2,798.36
+196.00	+343.64	Closed
+1.01%	+1.40%	

Delayed at least 15 minutes

1.30% **Advertising** **Video**

Path to Change in Power Still Unclear **Video**

By ANTHONY SHADID 56 minutes ago

President Hosni Mubarak's vow to step down in the fall was not enough for the hundreds of thousands who poured into Tahrir Square.

Post a Comment | Read (332)

Path to Change in Power Still Unclear

By DAVID D. KIRKPATRICK and MARK LANDLER 1 minute ago

The democracy movement is unfolding so rapidly in Egypt that Washington came close to being left behind.

Interactive Feature: A Timeline of Mubarak's Presidency

A chronology of President Hosni Mubarak's 30-year rule in Egypt.

More Photographs | Interactive Map: Protests

QUICK ACTS OF PROTEST ON A NOISY DAY

By KAREEM FAHMI and ANTHONY SHADID 54 minutes ago

Hundreds of thousands of Egyptians traveled like pilgrims to speak freely and to be heard.

- King of Jordan Dismisses His Cabinet
- Antiquities Chief Says Sites Are Largely Secure
- New Service Lets Voices From Egypt Be Heard
- The Lede: Updates From Day 8

Advertisement: iMeet

iMeet built a meeting room just for you.

Advertising 30-DAY FREE TRIAL

Source: Mayer & Mitchell; Third-Party Web Tracking: Policy and Technology



MARKETING EXPERIENCES

Mobile Marketing
TAPAD, LEADBOLT, Verve, etc.

Display & Native Ads
AdRoll, ChangeSimple, etc.

Video Marketing & Ads
Brightcove, Wistia, etc.

Search & Social Ads
Perfect Audience, etc.

Communities & Reviews
Jive, Disqus, etc.

Email Marketing
Constant Contact, etc.

Influencer Marketing
Influencer, etc.

Social Media Marketing
SocialMaven, etc.

Events & Webinars
Eventbrite, etc.

SEO
SEMrush, etc.

Customer Experience/VOX
InMoment, etc.

Loyalty/Referral/Gamification
Loyalty, etc.

Personalization & Chat
Demandbase, etc.

Testing & Optimization
Optimizely, etc.

Interactive Content
Offerpop, etc.

Content Marketing
Kopost, etc.

Creative & Design
Autodesk, etc.

Sales Enablement
Proseware, etc.

Audience & Market Data
InsideView, etc.

Channel/Local Mktg
Marketplace, etc.

Asset & Resource Mgmt
Widen, etc.

Call Analytics/Management
5iPhone, etc.

Team & Project Mgmt
Basecamp, etc.

Vendor Data/Analysis
Growth, etc.

MARKETING OPERATIONS

Performance & Attribution
MarketShare, etc.

Dashboards/Visualization
Tableau, etc.

Web & Mobile Analytics
Google, etc.

BI, CI & Data Science
Verov, etc.

MIDDLEWARE

Data Management Platforms/Customer Data Platforms
eLuminate, etc.

Tag Management
Tealium, etc.

Identity
Gigamon, etc.

Cloud Integration/ESBs
FTT, etc.

APIs
Apigee, etc.

BACKBONE PLATFORMS

Platform/Suite
Adobe, etc.

CRM
Salesforce, etc.

Marketing Automation/Campaign & Lead Mgmt
Marketo, etc.

Web Content/Experience Management
Acquia, etc.

E-commerce
Shopify, etc.

INFRA-STRUCTURE

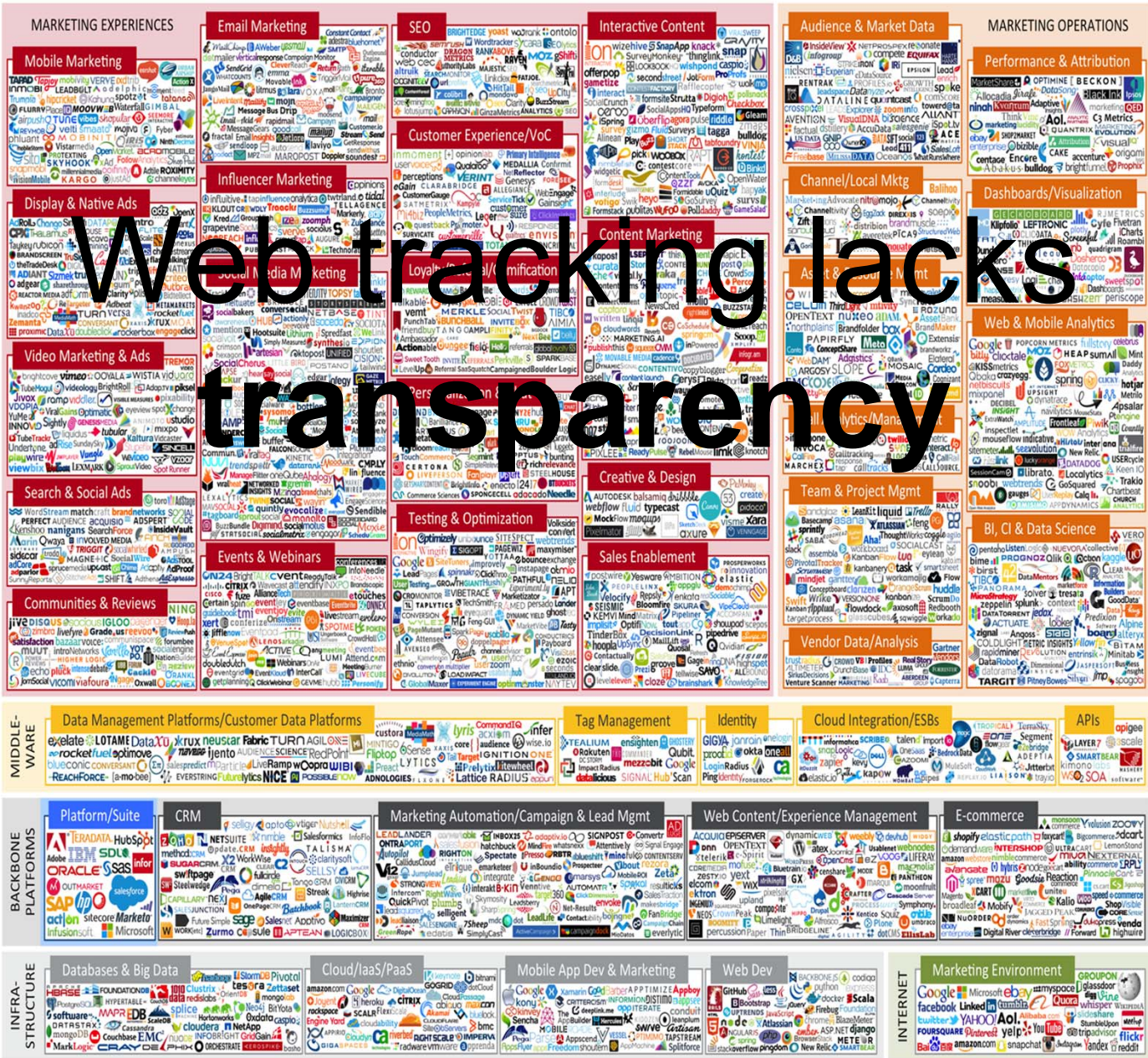
Databases & Big Data
Hadoop, etc.

Cloud/IaaS/PaaS
Amazon, etc.

Mobile App Dev & Marketing
Appcelerator, etc.

Web Dev
GitHub, etc.

INTERNET
Google, etc.



Web tracking lacks transparency



Web tracking lacks transparency

... but we are changing that



Web tracking lacks transparency

...but we are changing that (and I'll show you how we already have)

Transparency encourages best practices



Canvas
Fingerprinting
Introduced

Figure 7: Difference maps for a group on text_arial

May 2012



Transparency encourages best practices



Canvas
Fingerprinting
Introduced

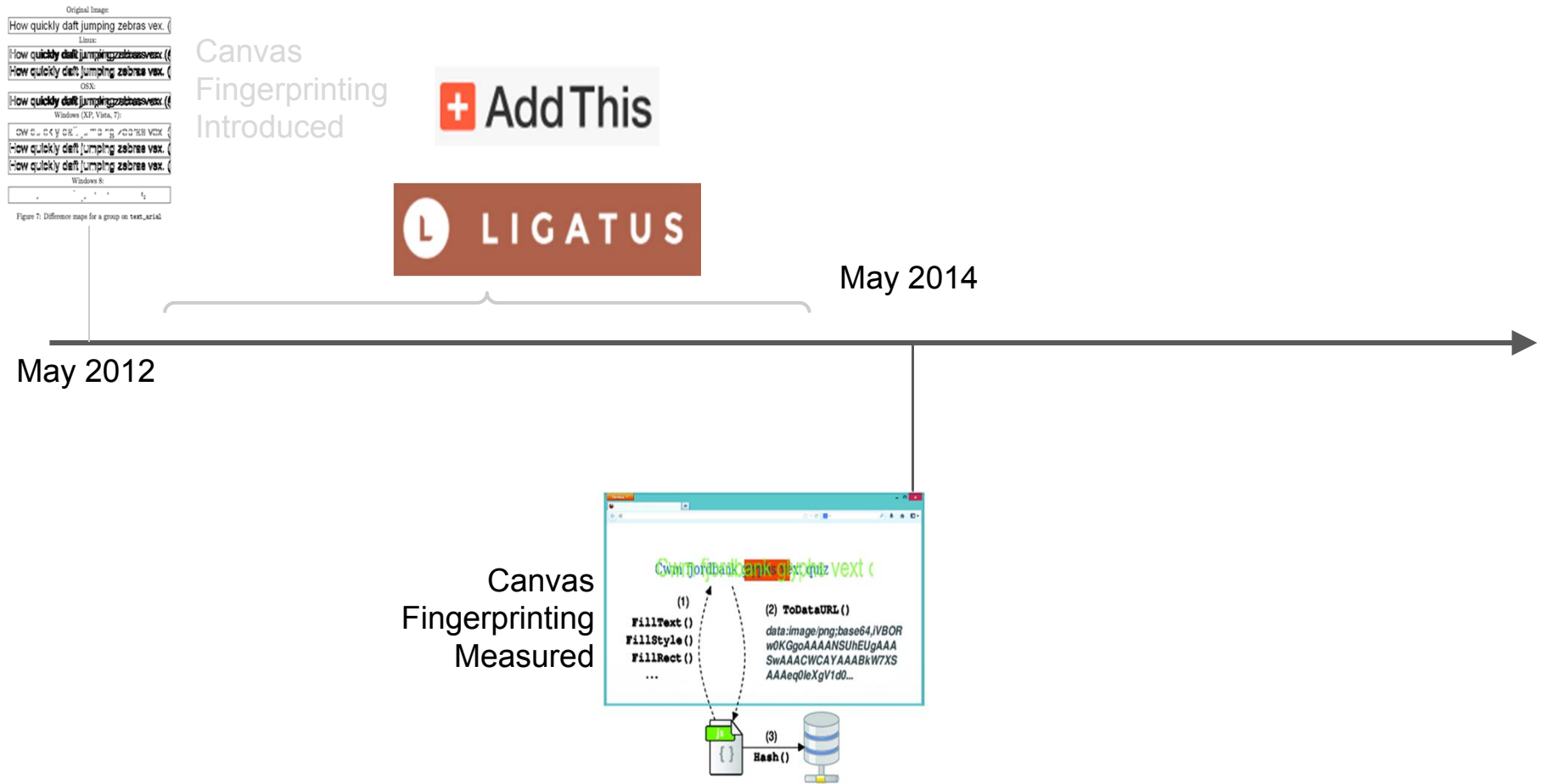


May 2014

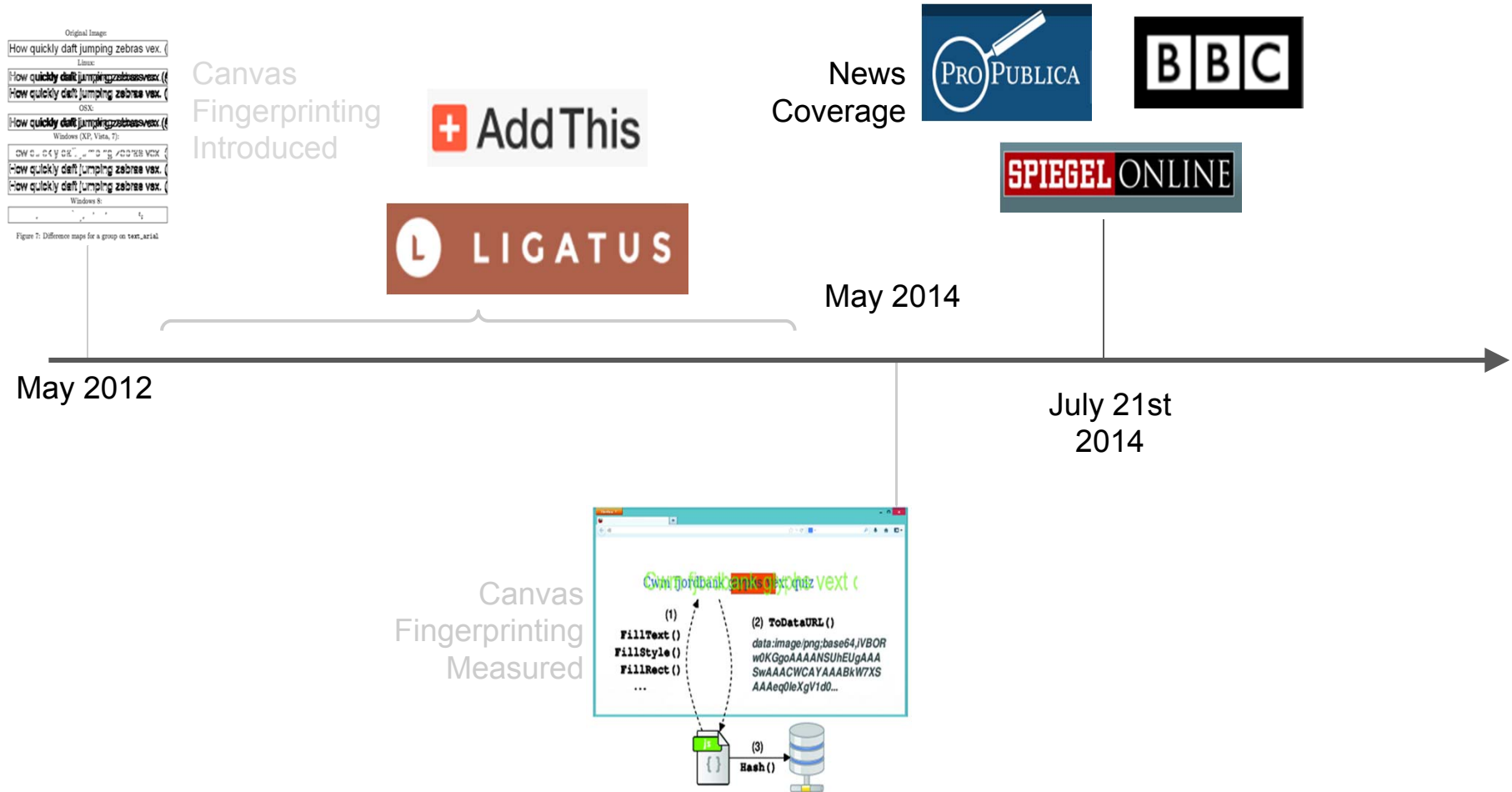
May 2012



Transparency encourages best practices



Transparency encourages best practices



Transparency encourages best practices



Canvas Fingerprinting was a known technique for **2 years**.



In just **2 months** following our measurement work the largest users of canvas fingerprinting stopped.



Why?

Our measurement work removed **information asymmetry** between trackers and the rest of the web.

Our measurement work removed **information asymmetry** between trackers and the rest of the web.



Dragnets

Tracking Censorship and Surveillance

Meet the Online Tracking Device That is Virtually Impossible to Block

A new kind of tracking tool, canvas fingerprinting, is being used to follow visitors to thousands of top websites, from WhiteHouse.gov to YouPorn.

by [Julia Angwin](#)

ProPublica, July 21, 2014, 8 a.m.

 This is part of an ongoing [Dragnets](#)

Our measurement work removed **information asymmetry** between trackers and the rest of the web.

PRO PUBL

BBC Sign in News Sport Weather Shop Earth Travel Me

Home Our Investigat

NEWS

Home Video World US & Canada UK Business Tech Science Magazine Ent

Dragnets
Tracking Censorship and

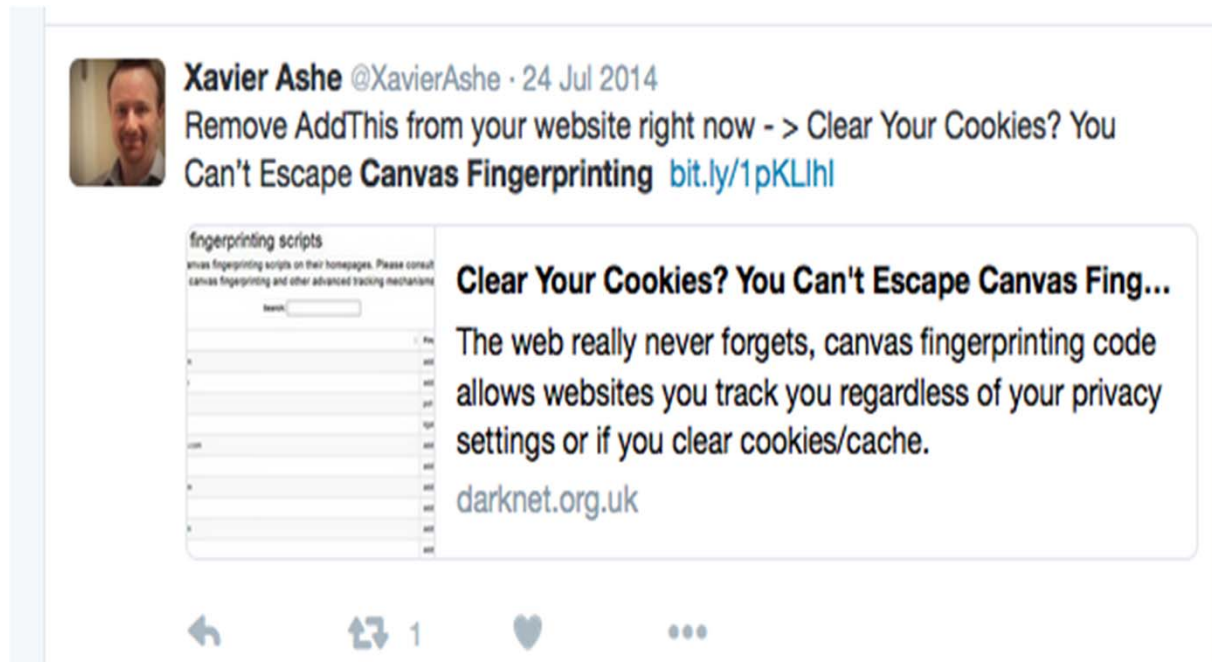
Meet the Virtually Anonymous: Browser 'fingerprints' help track users

A new kind of tracking...
WhiteHouse.gov to Y

22 July 2014 | Technology

by *Julia Angwin*
ProPublica, July 21, 2014, &

Our measurement work removed **information asymmetry** between trackers and the rest of the web.



Xavier Ashe @XavierAshe · 24 Jul 2014

Remove AddThis from your website right now - > Clear Your Cookies? You Can't Escape **Canvas Fingerprinting** bit.ly/1pKLlhl

fingerprinting scripts
Anvix fingerprinting scripts on their homepages. Please consult canvas fingerprinting and other advanced tracking mechanisms

Search:	File
	...
	...
	...
	...
	...
	...
	...
	...
	...
	...
	...

Clear Your Cookies? You Can't Escape Canvas Fing...

The web really never forgets, canvas fingerprinting code allows websites you track you regardless of your privacy settings or if you clear cookies/cache.

darknet.org.uk

Retweet 1

Our measurement work removed **information asymmetry** between trackers and the rest of the web.



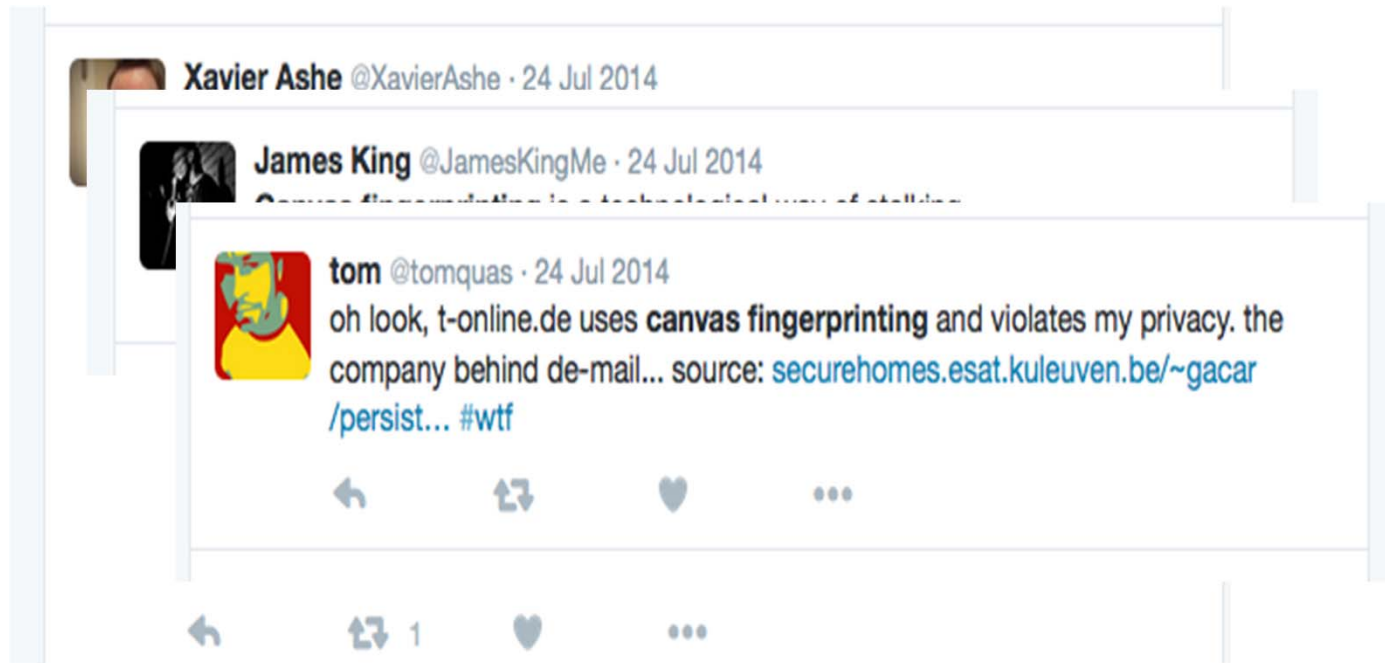
A screenshot of a Twitter thread. The top tweet is from Xavier Ashe (@XavierAshe) dated 24 Jul 2014. It contains a quote from James King (@JamesKingMe) dated 24 Jul 2014. The quoted tweet states: "Canvas fingerprinting is a technological way of stalking" and includes a screenshot of a browser's developer console. The console screenshot shows a list of IP addresses and a URL: "darknet.org.uk". Below the quoted tweet are icons for reply, retweet (with a count of 1), like, and a menu icon.

Xavier Ashe @XavierAshe · 24 Jul 2014

James King @JamesKingMe · 24 Jul 2014
Canvas fingerprinting is a technological way of stalking

allows websites you track you regardless of your privacy settings or if you clear cookies/cache.
darknet.org.uk

Our measurement work removed **information asymmetry** between trackers and the rest of the web.



Our measurement work removed **information asymmetry** between trackers and the rest of the web.



Our measurement work removed **information asymmetry** between trackers and the rest of the web.

Xavier Ashe @XavierAshe · 24 Jul 2014

James King @JamesKingMe · 24 Jul 2014

tom @tomquas · 24 Jul 2014

Jstheater @istheater · 22 Jul 2014

Alex Sherer @cymcym · 22 Jul 2014
I feel gross, because I used @addthis to share this article. But, everyone should know about #canvasfingerprinting news.genius.com/Gizmodo-what-y...

Tor Works: 2

Tor client
is path to
rver. Green
uplet, red
clear.

Gizmodo - What You Need to Know About the Sne...

What do the White House and YouPorn have in common? Their websites both use canvas fingerprinting, a newer form of online tracking designed to make it har...

genius.com

Our measurement work removed **information asymmetry** between trackers and the rest of the web.

The screenshot shows a Mozilla Support forum thread. At the top, the Mozilla Support logo is visible. Below it, a breadcrumb trail reads: HOME > SUPPORT FORUM > FIREFOX > WHY IS FIREFOX ALLOWING "CANVAS ...". The main heading of the thread is "Support Forum". A yellow banner with diagonal stripes contains the text: "This thread was archived. Please ask a new question if you need help." The thread title is "Why is FireFox allowing \"Canvas Fingerprinting\" to track me?". Below the title, the thread statistics are: 2 REPLIES, 14 HAVE THIS PROBLEM, 1010 VIEWS, LAST REPLY BY JSCHER2000, 1 YEAR AGO. A user profile picture for "jraff" is shown next to their post, which reads: "Since \"Canvas Fingerprinting\" seems to be the new way of tracking one. How does one TURN IT OFF! ---".

Information asymmetry not just between trackers and users.

Dragnets

Tracking Censorship and Surveillance

Meet the Online Tracking Device That is Virtually Impossible to Block

A new kind of tracking tool, canvas fingerprinting, is being used to follow visitors to thousands of top websites, from WhiteHouse.gov to YouPorn.

by Julia Angwin
ProPublica, July 21, 2014, 8 a.m.

Update: After this article was published, YouPorn contacted us to say it had removed AddThis technology from its website, saying that the website was "completely unaware that AddThis contained a tracking software that had the potential to jeopardize the privacy of our users." A spokeswoman for the German digital marketer Ligatus also said that is no longer running its test of canvas fingerprinting, and that it has no plans to use it in the future.

This story was co-published with Mashable.

A new, extremely persistent type of online tracking is shadowing visitors to thousands of

- most read
- An Unbelievable Story c
- Devils, Deals and the D
- Why Small Debts Matte Lives
- Out of Options, Califor Troubled Children Out c
- 'All of This Because Sor Work'
- Small-Scale Violations c Cause the Most Harm

“YouPorn contacted us to say...’[the website was] completely unaware that AddThis contained a tracking software...”

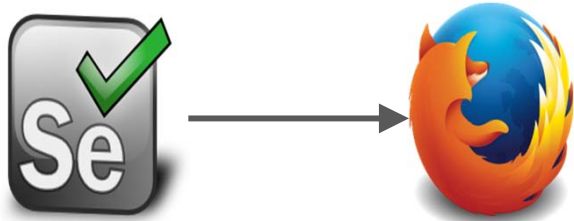
Transparency is effective at returning control to users and publishers

**Automated, large-scale measurements
can provide this transparency**

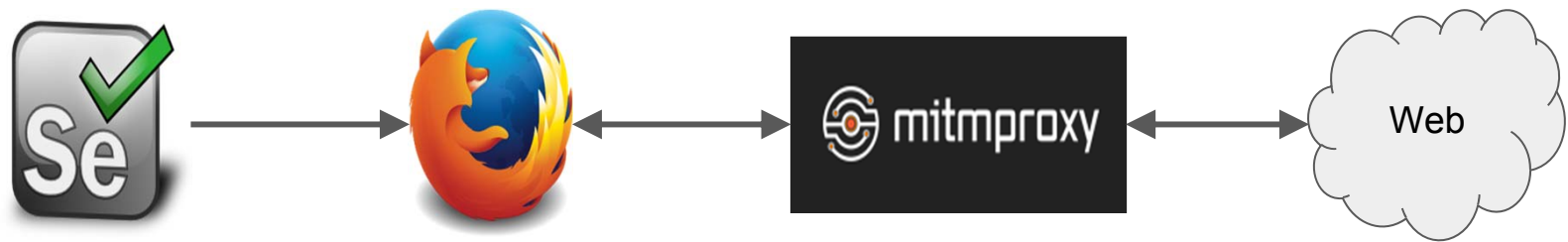
We're doing three things to help:

1. Developing OpenWPM
2. Running monthly, 1 million site measurements
3. Building an analysis layer on top of the data

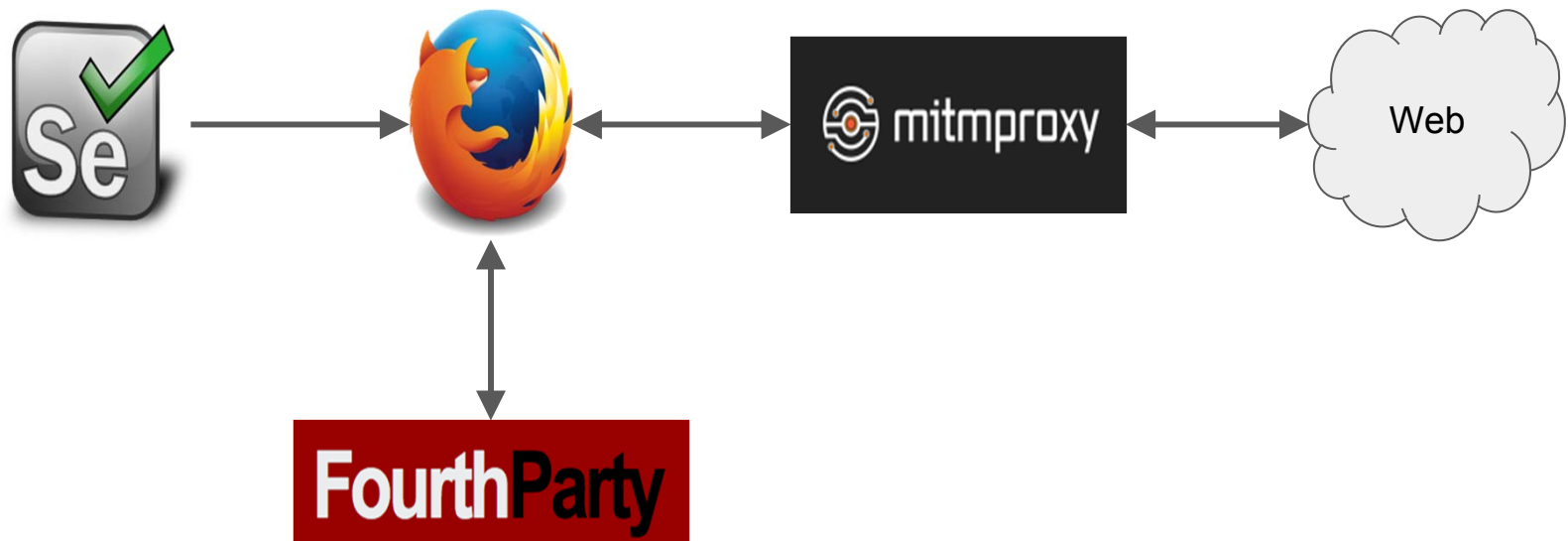
OpenWPM



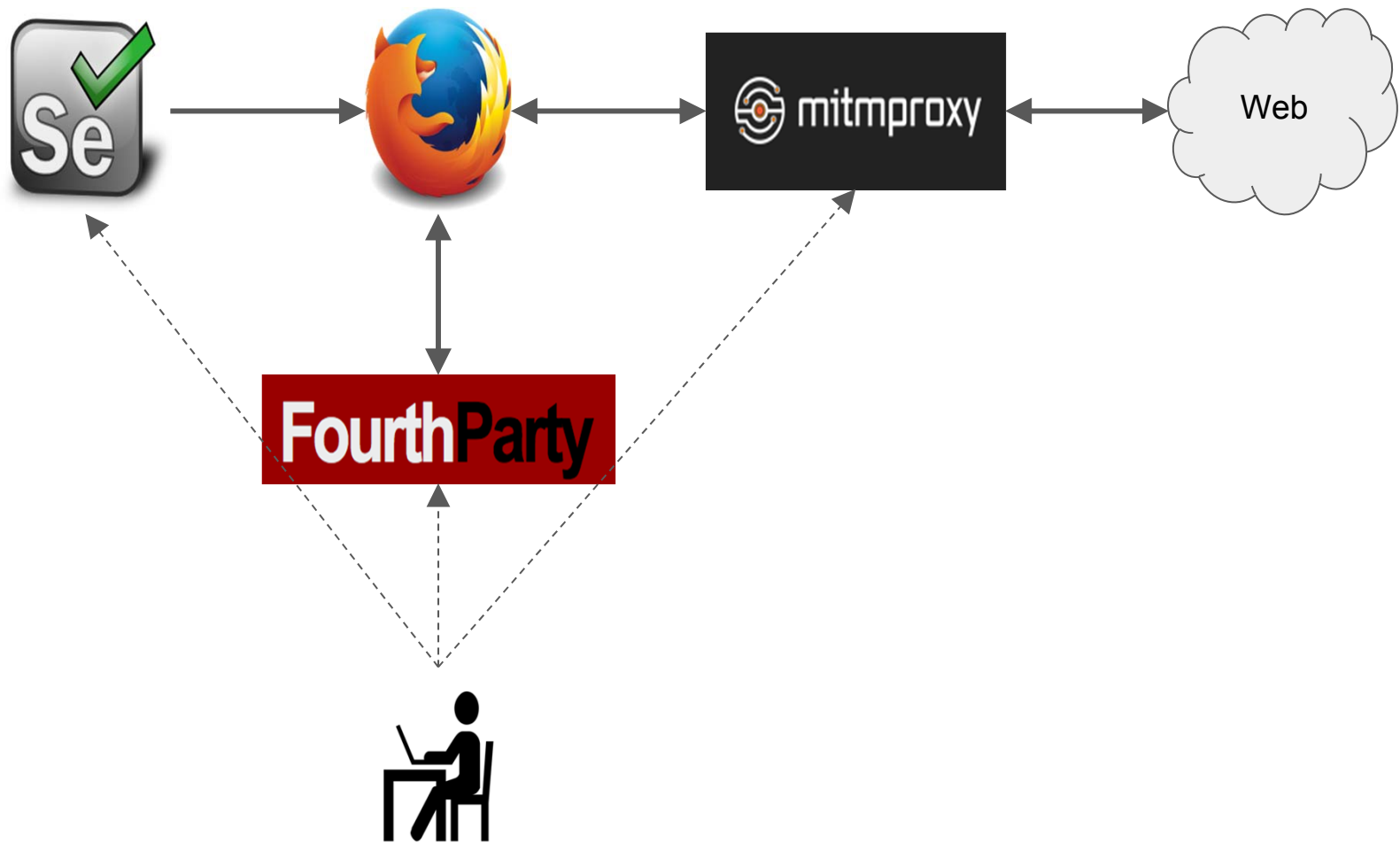
OpenWPM



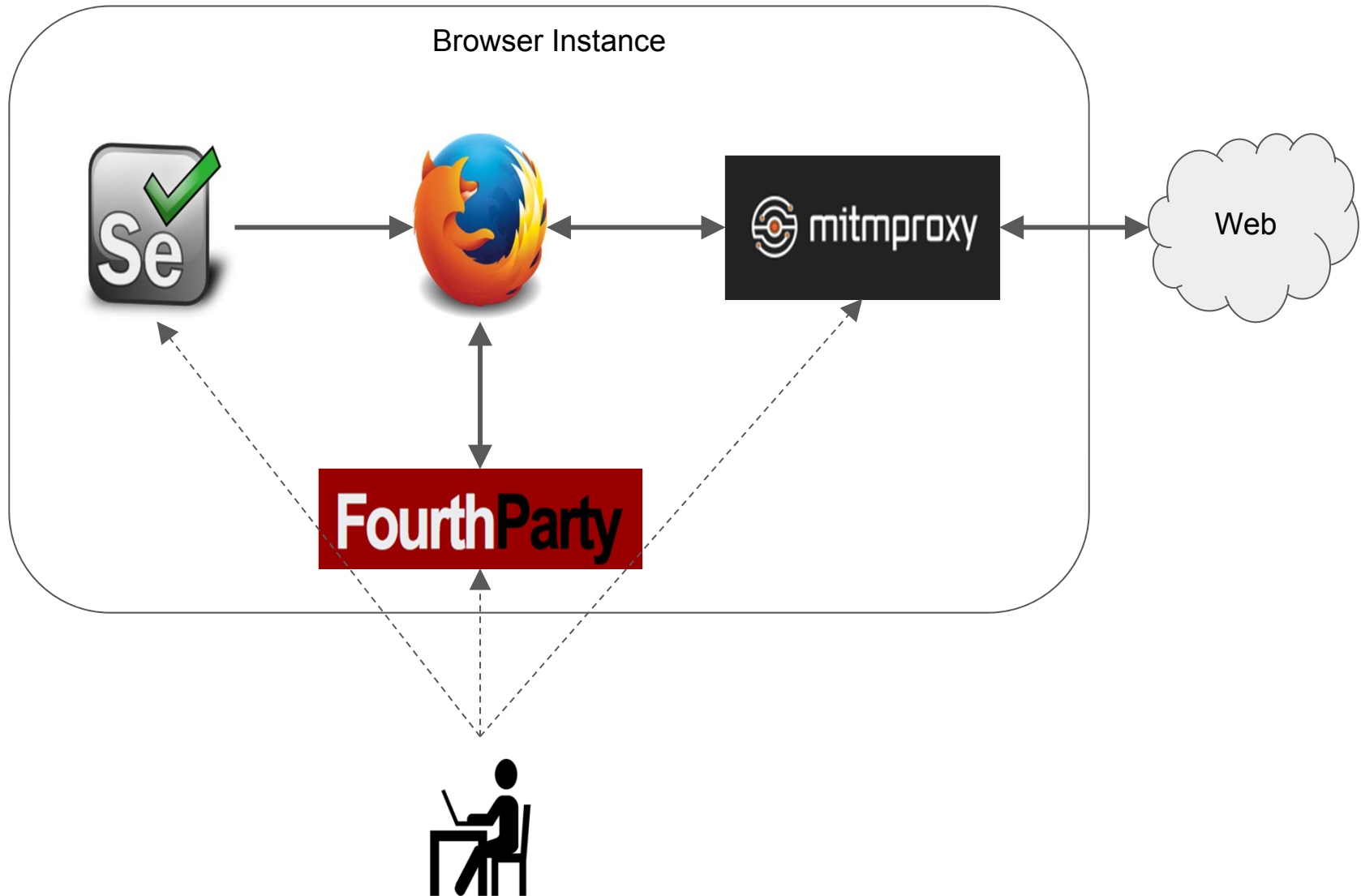
OpenWPM

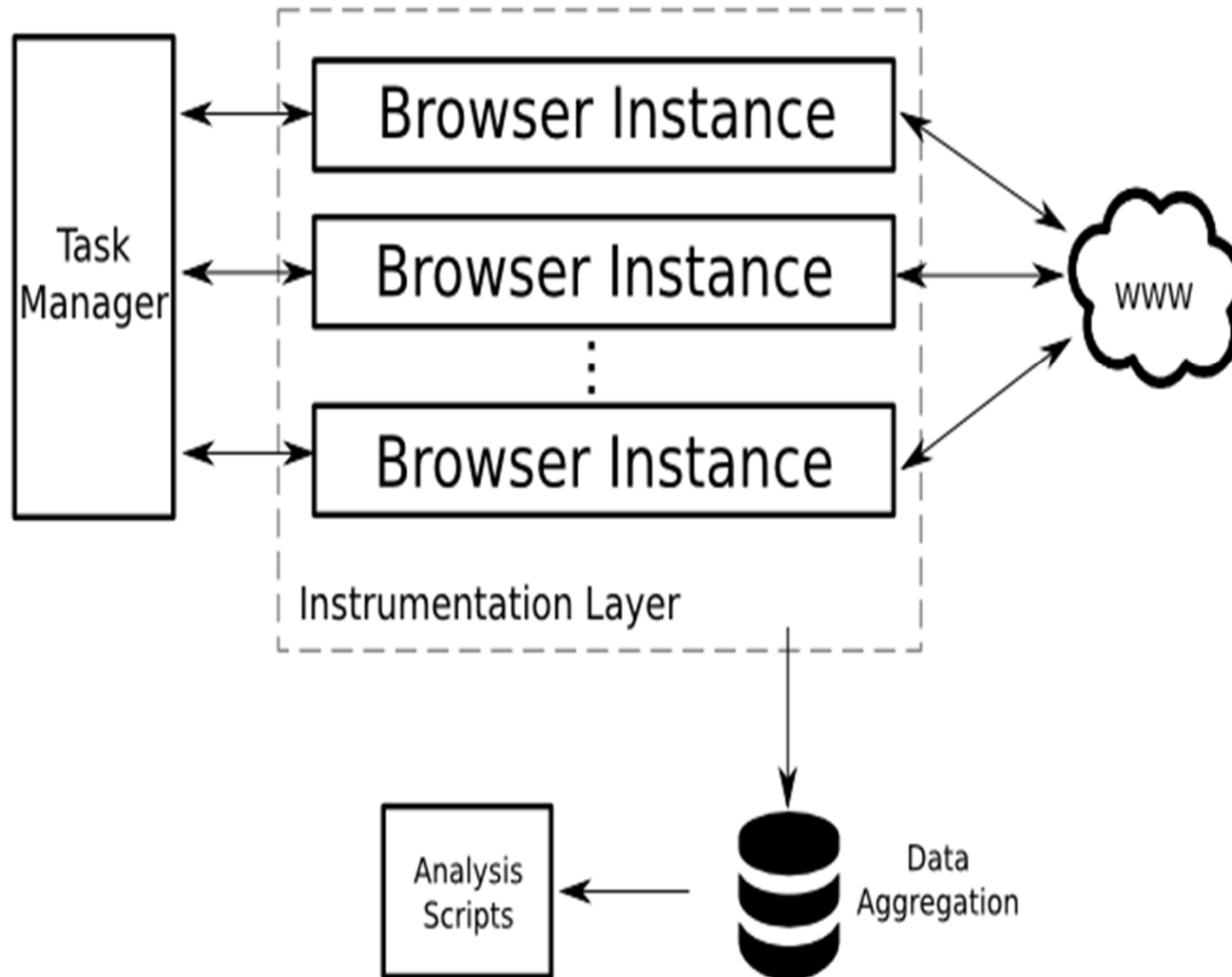


OpenWPM



OpenWPM





OpenWPM supports browsing with persistent state

Browser can keep profile through crashes and freezes

- Cookie setting over a session

- Cookie synchronization (id sharing)

- Zombie Cookies

OpenWPM uses a real browser

Extensions

AdBlock Plus, Ghostery, ...

Privacy Features

Block third-party cookies, FF tracking protection, ...

Support for new web technologies

WebRTC, Audio, Video, WebGL

OpenWPM is already used by at least 7 research groups

At Princeton

4 published studies and several ongoing

Ongoing Research

Columbia University

In published studies:

The Web Privacy Census (UC Berkeley / Berkeley Law)

Variations in Tracking in Relation to Geographic Location (CMU / RAND)

Forthcoming WWW'16 study by Nick Nikiforakis (Stony Brook)

By journalists

By regulators

The Web Transparency Census

Monthly
1 Million Site Crawl

The Web Transparency Census

Monthly
1 Million Site Crawl

Collecting:

- Javascript Calls
- All javascript files
- HTTP Requests and Responses
- Storage (cookies, Flash, etc)

Supporting a variety of measurements

1. Effectiveness of Privacy Tools

- Ghostery
- AdBlock Plus
- HTTPS Everywhere

Supporting a variety of measurements

1. Effectiveness of Privacy Tools

- Ghostery
- AdBlock Plus
- HTTPS Everywhere

2. Effectiveness Browser Protections

- DNT
- Third-party cookie Blocking
- Firefox Tracking Protection

Supporting a variety of measurements

1. Effectiveness of Privacy Tools

- Ghostery
- AdBlock Plus
- HTTPS Everywhere

2. Effectiveness Browser Protections

- DNT
- Third-party cookie Blocking
- Firefox Tracking Protection

3. Use of javascript for tracking

- Canvas Fingerprinting
- Property Enumeration
- WebRTC Local IP Sniffing

Supporting a variety of measurements

1. Effectiveness of Privacy Tools

- Ghostery
- AdBlock Plus
- HTTPS Everywhere

2. Effectiveness Browser Protections

- DNT
- Third-party cookie Blocking
- Firefox Tracking Protection

3. Use of javascript for tracking

- Canvas Fingerprinting
- Property Enumeration
- WebRTC Local IP Sniffing

4. Tracking Practices

- Cookie Syncing
- Cookie Respawning
- Setting ID cookies

Case Study 1: Canvas Fingerprinting

Case Study 2: WebRTC Local IP Sniffing

2012: Canvas Fingerprinting Introduced

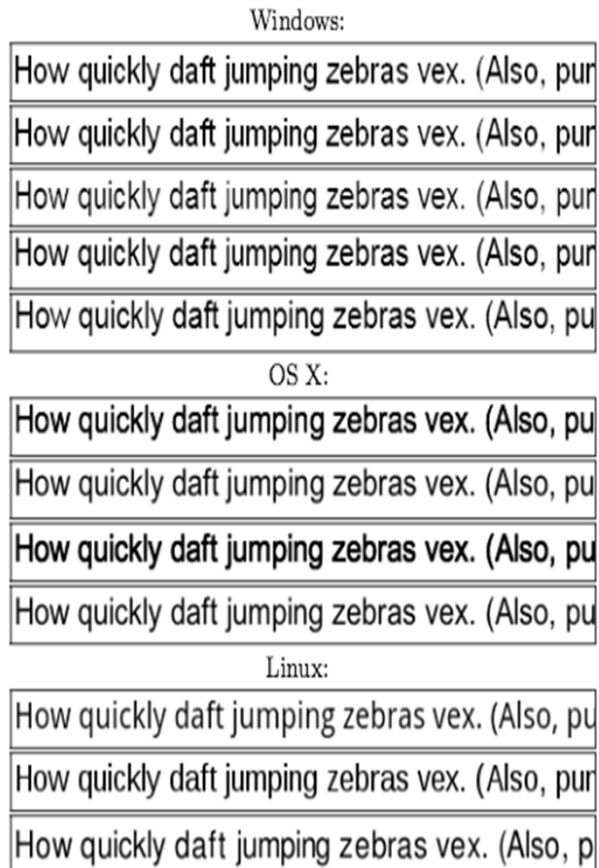


Figure 6: 13 ways to render 20px Arial

2012: Canvas Fingerprinting Introduced

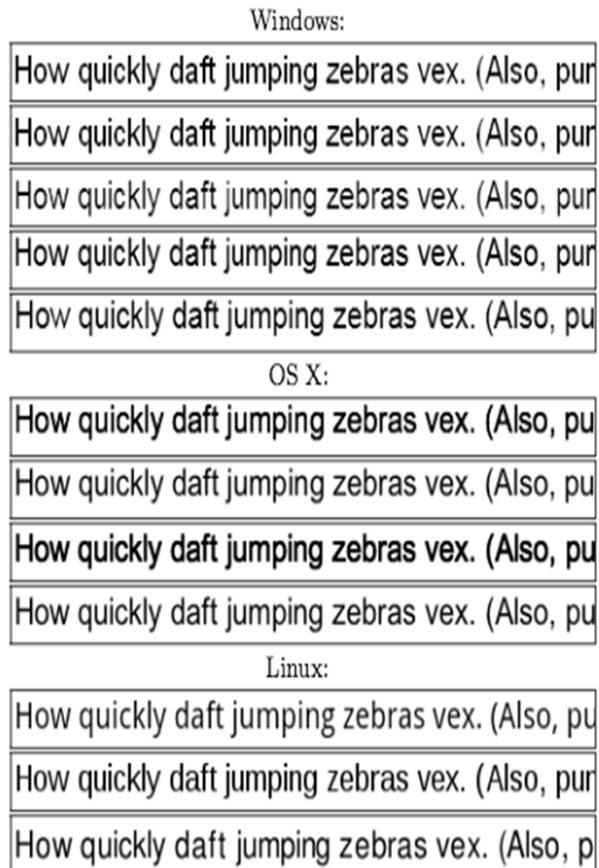


Figure 6: 13 ways to render 20px Arial

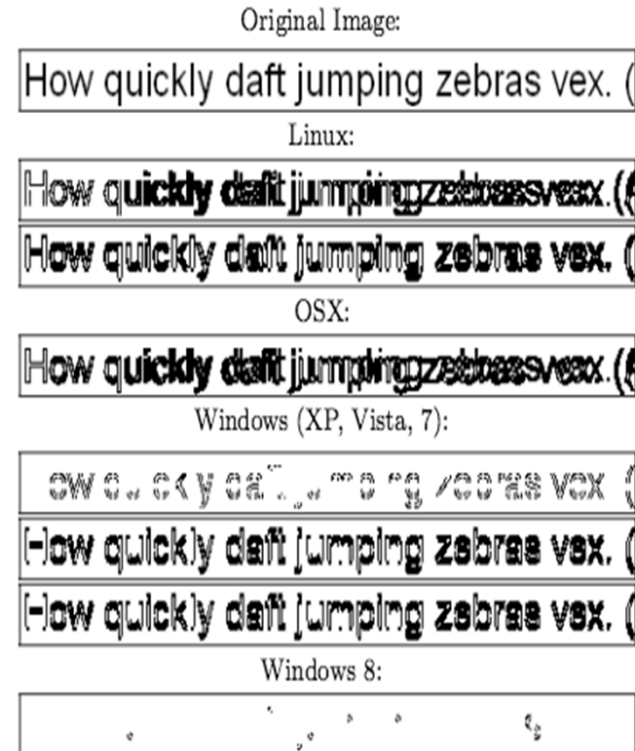


Figure 7: Difference maps for a group on text_arial

2014: Canvas Fingerprinting Measured



The Web Never Forgets: Persistent Tracking Mechanisms in the Wild

Gunes Acar¹, Christian Eubank², Steven Englehardt², Marc Juarez¹
Arvind Narayanan², Claudia Diaz¹

¹KU Leuven, ESAT/COSIC and iMinds, Leuven, Belgium
{name.surname}@esat.kuleuven.be

²Princeton University
{cge,ste,arvindn}@cs.princeton.edu

ABSTRACT

We present the first large-scale studies of three advanced web tracking mechanisms — canvas fingerprinting, evercookies and use of “cookie syncing” in conjunction with evercookies.

1. INTRODUCTION

A 1999 New York Times article called cookies comprehensive privacy invaders and described them as “surveillance

2014: Canvas Fingerprinting Measured



Source: Acar, Eubank, Englehardt, Juarez, Narayanan, Diaz; *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*

2014: Canvas Fingerprinting Measured

1. Write a Firefox patch
1. Write automation with Selenium
1. Write analysis code



Case Study 1: Canvas Fingerprinting

Case Study 2: WebRTC Local IP Sniffing

1.I saw a tweet that nytimes.com is IP sniffing

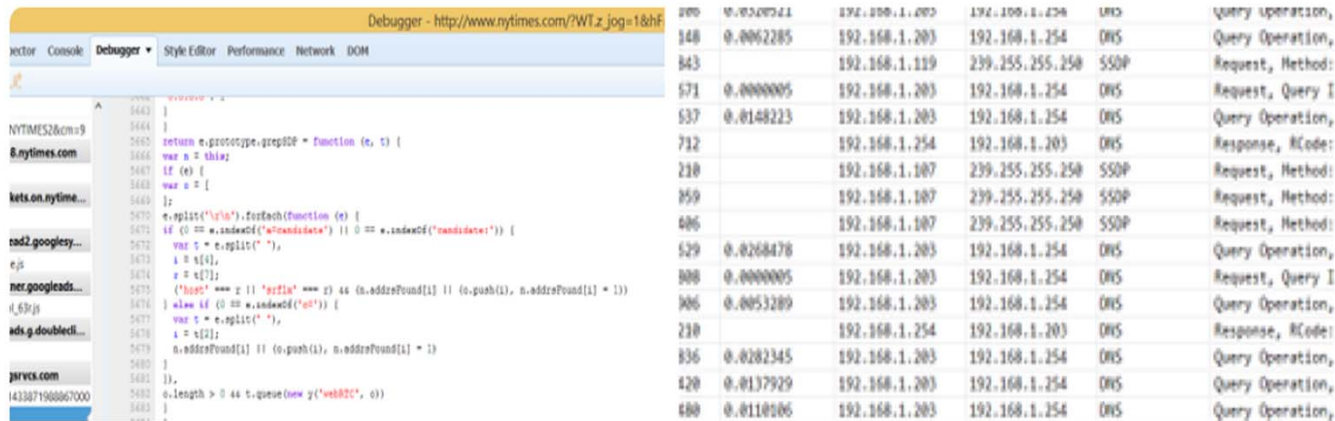


Mike O'Neill
@incloud



 Follow

WebRTC being used now by embedded 3rd party on nytimes.com to report visitors' local IP addresses.



The screenshot shows a browser's developer console with the following components:

- Debugger:** Shows a list of JavaScript code snippets from various domains, including `nytimes.com`, `kets on nytime...`, `rad2 googlesy...`, `e.js`, `ner.googleads...`, `ads.g.doublecl...`, and `jsrvcs.com`.
- Network:** Displays a series of network requests. The first few are DNS queries to `192.168.1.254`. Subsequent requests are SSDP (Simple Service Discovery Protocol) requests to `239.255.255.250`, which is a multicast address used for local network discovery and can be used to sniff local IP addresses.

2. I added code to JS Instrumentation for next crawl

```
// Access to webRTC
instrumentObject(window.mozRTCPeerConnection.prototype
                 "mozRTCPeerConnection",
                 prototype=true);
```

3. I wrote some analysis code

- Grab all urls that execute
 - mozRTCPeerConnection.onicecandidate
 - mozRTCPeerConnection.createDataChannel
 - mozRTCPeerConnection.createOffer

- Check JS Files to confirm

4. I found several third-parties sniffing local IP

121 first-party sites (October 2015)

29 in the top 10k

24 unique scripts

Only 1 of which is blocked by
EasyList/EasyPrivacy

Measurement with OpenWPM is much easier

Canvas Fingerprinting

1. Write a Firefox patch

1. Write automation with Selenium

1. Write analysis code

WebRTC Local IP Sniffing

Measurement with OpenWPM is much easier

Canvas Fingerprinting

1. Write a Firefox
patch

1. Write automation
with Selenium

1. Write analysis code

WebRTC Local IP Sniffing

1. Write 1 line of JavaScript

Measurement with OpenWPM is much easier

Canvas Fingerprinting

~~1. Write a Firefox patch~~

~~1. Write automation with Selenium~~

1. Write analysis code

WebRTC Local IP Sniffing

1. Write 1 line of JavaScript

1. Use OpenWPM

Measurement with OpenWPM is much easier

Canvas Fingerprinting

~~1. Write a Firefox patch~~

~~1. Write automation with Selenium~~

1. Write analysis code

WebRTC Local IP Sniffing

1. Write 1 line of JavaScript

1. Use OpenWPM

1. Write analysis code

Where to go from here:

1. Inform the public
2. Provide data for privacy tools
3. Make data more accessible to less technical investigators

We'd like to collaborate with you

1. Submit pull requests for OpenWPM
2. Use OpenWPM to run measurements and release the data
3. Download our data and build analysis on top of it
 - a. (Coming soon!)

Help us make the web more transparent!

Contribute:

github.com/citp/OpenWPM

Collaborate:

webtap.princeton.edu

Email: ste@cs.princeton.edu

Twitter: [@s_englehardt](https://twitter.com/s_englehardt)

Chris Jay Hoofnagle

University of California, Berkeley Law

Alan Westin's Privacy Homo Economicus

Co-author: Jennifer Urban (University of California, Berkeley Law)



Alan Westin's Privacy Homo Economicus

Chris Jay Hoofnagle
Adjunct Professor, School of Information, UC Berkeley
For the FTC PrivacyCon Conference
January 14, 2016

About this work

- In collaboration with Professor Jennifer M. Urban, UC Berkeley Law
- Overseen by our staff statistician, Dr. Su Li.
- Most complete publication is in *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest Law Review 261 (2014).

Homo Economicus & US Policy

- Homo economicus reliably makes an appearance in regulatory debates concerning information privacy.
- Under the still-dominant U.S. “notice and choice” approach to consumer information privacy, the rational consumer is expected to negotiate for privacy protection by reading privacy policies and selecting services consistent with her preferences.
- To be tenable as a protection for consumer interest, “notice and choice” requires homo economicus to be broadly reliable as a model.

Theoretical Background: RCT

- Public policy discussion, privacy laws often based upon rational choice theory assumptions
 - Expected utility maximization
 - Stability, transitivity of preferences
 - Preferences need not be rational
 - Individual choices and collective outcomes

Alan Westin's Influence

- Established “segmentation” of public into high, mid, and low-concern consumers
- Very influential frame to understand privacy
- Argues that public policy should serve mid-level concern consumers, the “privacy pragmatists.”
- But rarely subject to empirical testing or academic critique

Evaluating Westin's work procedurally

- Is this consulting or academic work?
 - If consulting, may be subject to sponsor pre-publication review, censorship.
 - If academic, many institutions ban sponsor publication veto
 - Consider POM case (U. Chicago researcher with sponsor pre-publication veto), historically, Blaisdell's 1932 history of the FTC.
- Who is the sponsor?
 - Some don't disclose, see Yale Brozen in the 1970s
- Are there hypotheses?
- Is there a serious literature review?
- Are counterarguments ignored?

Westin: Privacy Fundamentalists

"Privacy Fundamentalists (about 25%). This group sees privacy as an especially high value, rejects the claims of many organizations to need or be entitled to get personal information for their business or governmental programs, thinks more individuals should simply refuse to give out information they are asked for, and favors enactment of strong federal and state laws to secure privacy rights and control organizational discretion."

Westin: Privacy Fundamentalists

"Privacy Fundamentalists (about 25%). This group sees privacy as an especially high value, rejects the claims of many organizations to need or be entitled to get personal information for their business or governmental programs, thinks more individuals should **simply refuse to give out information they are asked for, and favors enactment of strong federal and state laws to secure privacy rights and control organizational discretion.**"

Westin: Privacy Pragmatists

“Privacy Pragmatists (about 55%). This group weighs the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, looks to see whether fair information practices are being widely enough observed, and then decides whether they will agree or disagree with specific information activities -- with their trust in the particular industry or company involved a critical decisional factor. The Pragmatists favor voluntary standards over legislation and government enforcement, but they will back legislation when they think not enough is being done -- or meaningfully done -- by voluntary means.”

Westin: Privacy Pragmatists

“Privacy Pragmatists (about 55%). This group **weighs** the value to them and society of various business or government programs calling for personal information, **examines** the relevance and social propriety of the information sought, **looks to see** whether fair information practices are being widely enough observed, and then **decides whether** they will agree or disagree with specific information activities -- with their **trust** in the particular industry or company involved a critical decisional factor. **The Pragmatists favor voluntary standards** over legislation...

Westin: Privacy Unconcerned

- "Privacy Unconcerned (about 20%) This group doesn't know what the "privacy fuss" is all about, supports the benefits of most organizational programs over warnings about privacy abuse, has little problem with supplying their personal information to government authorities or businesses, and sees no need for creating another government bureaucracy to protect someone's privacy."

Westin: Pragmatists are Key

- “Most Consumers Are Shrewd Privacy Balancers”
- Privacy pragmatists are key to privacy, because their decisions steer society on questions of technology
 - Echoes RCT
- “In the politics of privacy, the battle is for the hearts and minds of the Privacy Pragmatists.”

Westin Segment Questions

- Consumers have lost all control over how personal information is collected and used by companies. 2.5% skip
- Most businesses handle the personal information they collect about consumers in a proper and confidential way. 4.2% skip
- Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. 4.7% skip

Analysis 1: Segmentation Text

- Pragmatists coded as default category
- Westin's questions probed consumer control, business use of data, and existing law. None of these questions address the specific behaviors that define pragmatism.
- What do you do with people who do not answer the segmentation questions? (8 percent in our studies!)

Segmentation Text Con't

- Privacy Unconcerned
 - One could imagine a consumer agreeing with the first question concerning a lack of control, yet being nonchalant about that lack of control.
 - She may, for example, consider loss of control a problem, but rationalize it by trusting existing law and business practices for protection.

Segmentation Text Con't

- Are there objectively correct answers to Westin's segmentation?
 - Credit reporting, Snowden disclosures paint picture of world with only limited individual control (e.g. correcting a credit report)
 - 2nd Question asks about confidential treatment of data, but most users do not enjoy confidentiality
 - In the U.S., confidentiality is generally limited to the professions

Analysis 2: Empirical

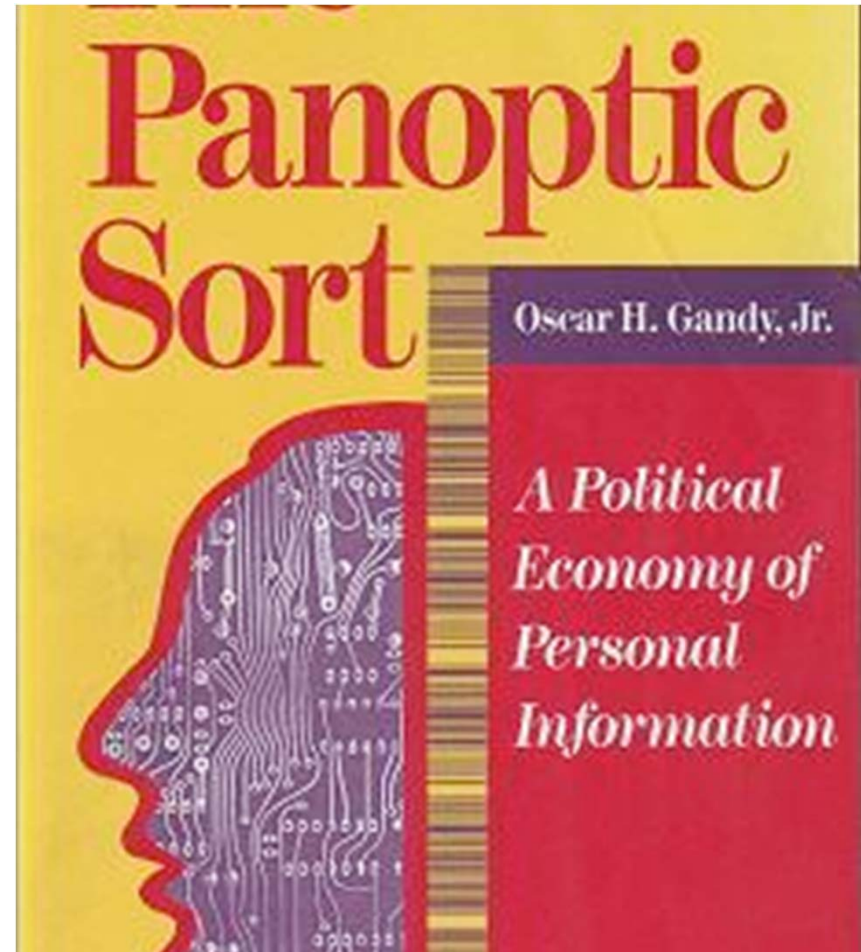
- Turow (2003) survey concludes: “overwhelming majority of U.S. adults who use the internet at home have no clue about data flows... Even if they have a sense that sites track them and collect individual bits of their data, they simply don’t fathom how those bits can be used...”
- “In fact, when presented with a common way that sites currently handle consumers’ information, they say they would not accept it. The findings suggest that years into attempts by governments and advocacy groups to educate people about internet privacy, the system is more broken than ever.”

Turow: Privacy Policy as Seal

- 57 percent agreed with: “When a web site has a privacy policy, I know that the site will not share my information with other websites or companies.”
 - Turow 2003
- 59% answered true to the statement, “When a website has a privacy policy, it means the site will not share my information with other websites and companies.”
 - Turow 2005

Gandy: Disconnect bt Perceptions and Practices

Gandy observed that in one survey, almost 40 percent of respondents thought that information sharing among businesses was something to be concerned about. However, 97 percent agreed that it was a “bad thing” that companies could buy information about consumer characteristics from mailing list companies.



Gandy: Knowledge & Privacy

- ...I discovered that the extent to which people had read or heard about the “potential use or misuse of computerized information about consumers” was a powerful explanatory factor. The more they had heard or read, the more they were concerned about threats to their privacy, the more concerned they were about the sale of personal information...
 - The Role of Theory in the Policy Process, A Response to Professor Westin (1995)

FCC Critique in CPNI Proceeding

- ...the [Westin] survey questions ask broadly whether it is acceptable for a customer's local telephone company to look over "customer records" to determine which customers would benefit from hearing about new services, without explaining the specific types of information that would be accessed...This data can be translated into subscriber profiles (1988)

Contrary to what marketers say,
**AMERICANS
 REJECT
 TAILORED
 ADVERTISING**
AND THREE ACTIVITIES THAT ENABLE IT

Joseph Turov
 Annenberg School for Communication, University of Pennsylvania

Jennifer King
 University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Chris Jay Hoofnagle
 University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Amy Bleakley
 Annenberg Public Policy Center, University of Pennsylvania

Michael Hennessy
 Annenberg Public Policy Center, University of Pennsylvania

Electronic copy available at: <http://journals.comabstrack-147824>

**HOW DIFFERENT
 ARE YOUNG ADULTS
 FROM OLDER ADULTS
 WHEN IT COMES TO
 INFORMATION PRIVACY
 ATTITUDES & POLICIES?**
 APRIL 14, 2010

"WE SUGGEST...THAT YOUNG-ADULT AMERICANS HAVE AN ASPIRATION FOR INCREASED PRIVACY EVEN WHILE THEY PARTICIPATE IN AN ONLINE REALITY THAT IS OPTIMIZED TO INCREASE THEIR REVELATION OF PERSONAL DATA." (p. 100-101)

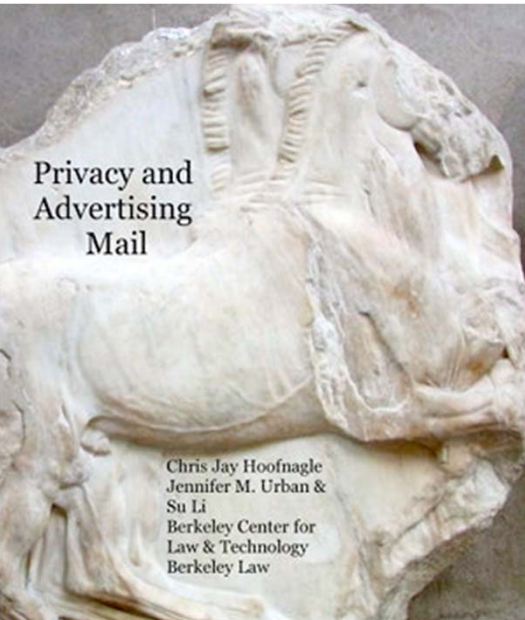
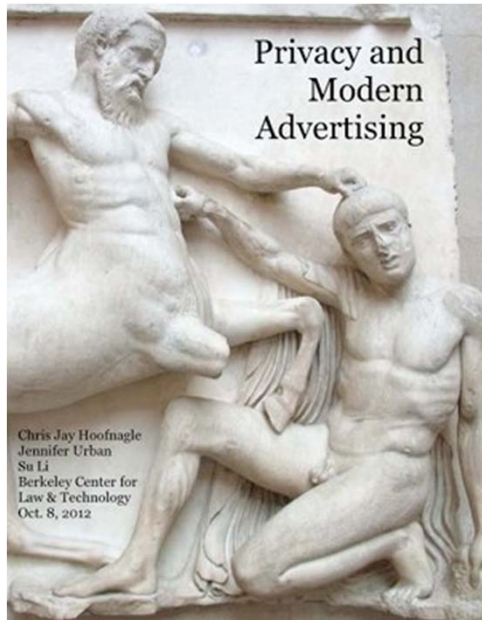
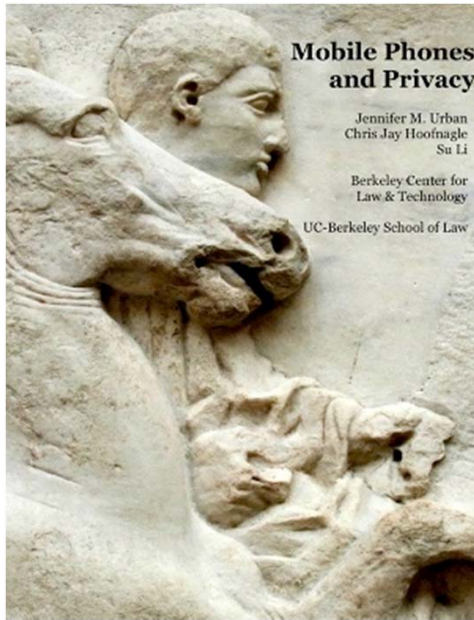
Chris Hoofnagle
 UC Berkeley School of Law, Berkeley Center for Law and Technology

Jennifer King
 UC Berkeley School of Information

Su Li
 UC Berkeley School of Law, Center for the Study of Law and Society

Joseph Turov
 Annenberg School for Communication, University of Pennsylvania

Electronic copy available at: <http://journals.comabstrack-158864>



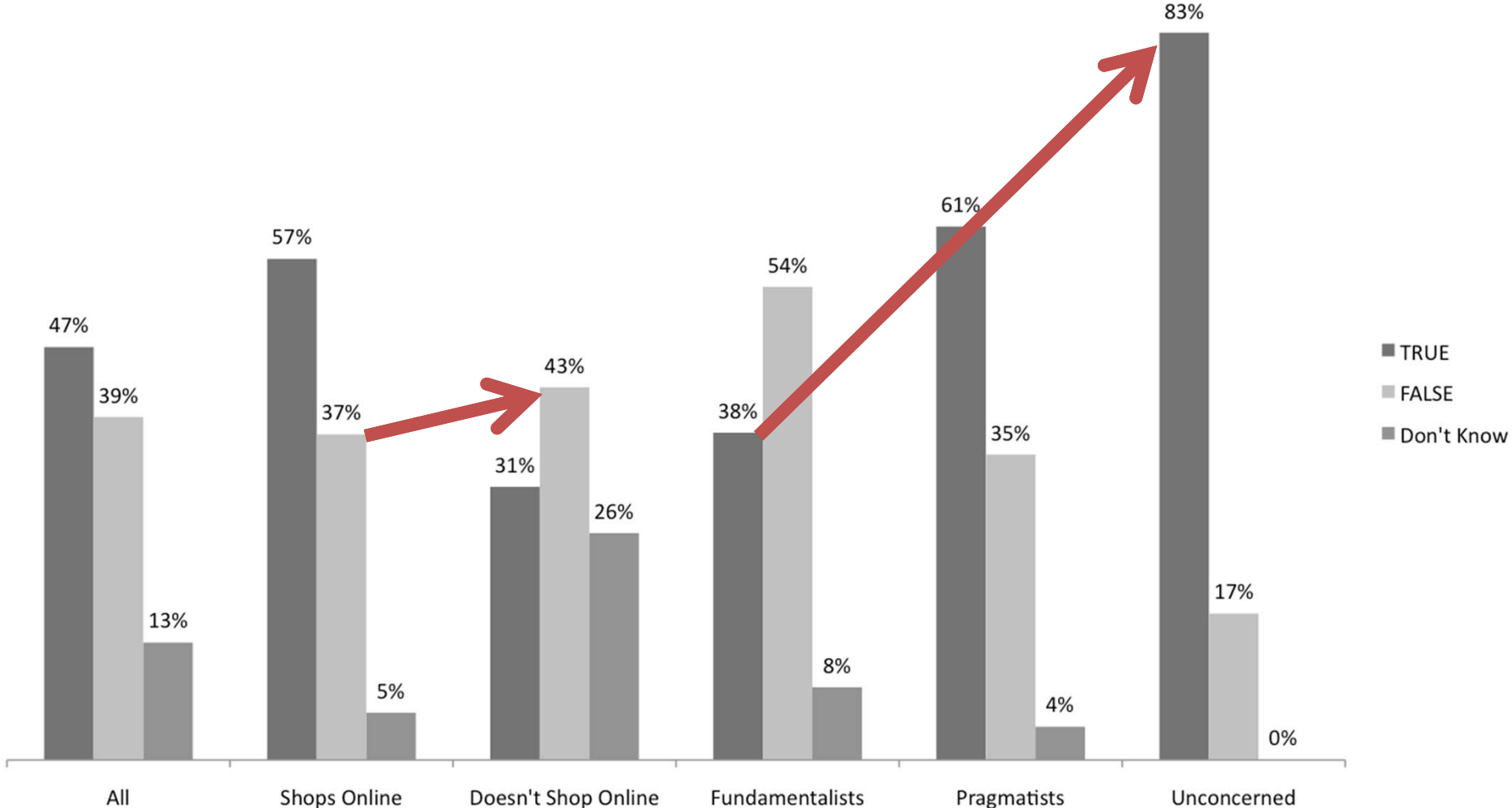
What is the extent of consumer naiveté on privacy?

- We have conducted 7 surveys with privacy quizzes:
 - Golden Bear telephonic (California only, 2007)
 - National wireless/wireline telephonic (2009, 2011, 2013 x3)

Golden Bear (2007, CA Only)

- We asked a series of true/false questions with crosstabs on
 - Internet shopping
 - Westin's privacy segmentation
 - N is pretty small—about 200

If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies.



2009 Study

- No one was interested in California-only data!
- Nationwide, wireline & wireless
- PSRAI conducted the surveys
- Internet users only

2009 Privacy Quiz

- 62% said true to, “If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.”
- 54% said true to, “If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.”

2009 Quiz Con't

- 30% true, 50% DK: “If a website has a TRUSTe privacy seal, it means that the site has the strongest privacy protections possible.”
- 38% true, 34% DK: “Advertisers are not allowed to follow your internet activity on medical websites.”
- 33% true, 19% DK: If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.

2009: Low Levels of Privacy Knowledge

- 75% answered two or fewer online questions correctly
- 30% none correct
- Being a digital native doesn't help. 18-24 were the worst—42% none correct

2012 Study

- “When you use the internet to learn about medical conditions, advertisers are not allowed to track you in order to target advertisements”
- 22% true, **35% false** 41% DK:
- Privacy Fundamentalists 49.5% false***
- Privacy Pragmatists 34% false
- Privacy Unconcerned 32% false

2012 Con't

- Free websites that are supported by advertising are allowed to sell information gathered from users of the site, even if they have a privacy policy
- **40% true**, 19% false, 40% DK
- Privacy Fundamentalists 52.6% true***
- Privacy Pragmatists 37.6% true
- Privacy Unconcerned 35% true*

2012 Con't

- When visiting free websites supported by advertising, you have the right to require the website to delete the information it has about you
- 25% true, **32% false**, 42% DK
- Privacy Fundamentalists 40.5% false***
- Privacy Pragmatists 30% false
- Privacy Unconcerned 35% false

The Knowledge Gap & Pragmatism

- Westin's segmentation has confused pragmatism with ordinary consumer decision making
- Like many decisions, these are often poorly informed
- We cannot and will never have a perfect view of business practices

The private sector is a major concern

Contrary to libertarian narratives, American consumers are just as concerned about private-sector collection and use of data as government information practices.

TABLE 3: LOCATION OF PRIVACY CONCERN—GOVERNMENT VS. PRIVATE COMPANIES

	<i>11/13</i>	<i>9/13</i>	<i>8/13</i>	<i>2/12</i>
Government (or)	13	16	13	11
Private companies (or)	14	15	14	19
Both the government and private companies (or)	66	63	65	66
(VOL.) Neither	5	4	6	2
Don't know/Refused	2	2	2	2

THE POLLS—A REPORT

PUBLIC OPINION TRENDS: PRIVACY AND INFORMATION TECHNOLOGY

JAMES E. KATZ AND
ANNETTE R. TASSONE

While there have been numerous cross-sectional analyses of public opinion toward privacy (Harris and Westin, 1979), and especially computers and privacy (SNET, 1984; Gandy, 1989; Anderson, 1972), there have been few trend analyses. Consequently, we have had no good answers for the fundamental question, Is public concern over privacy rising? One answer to this question is a clear “No.” Basing their position on data collected through 1983, Dutton and Meadow (1987: 168), in their definitive review of surveys on privacy, concluded that “the perceived likelihood of privacy invasions and their impact on American life has remained stable since 1974. Likewise, while computing was increasingly seen as a threat to privacy between 1973 and 1979, this trend has leveled off since then” (see also Dutton and Meadow, 1985). Yet polls conducted since Dutton and Meadow’s review suggest that public concern over privacy is rising in the mid to late 1980s and what was a definitive statement a few years ago may now need to be modified. In this article we present some trends from recent poll results about privacy in general and in regard to information technology (specifically computers and telephones).

Results of Surveys

IMPORTANCE OF PRIVACY

Surveys in 1988 and 1989 show that people overwhelmingly say that privacy as an abstract concept is important (Table 1).¹ When inter-

JAMES E. KATZ is a sociologist at Bell Communication Research (Bellcore). ANNETTE TASSONE is completing her doctorate in human factors at Stevens Institute of Technology. The authors thank Tom W. Smith, Diane Duffy, Richard Clayton, Ed Pinnes, Bob Kraut, and Oscar H. Gandy, Jr., for their help. Maritz survey data appear in Gandy, 1990.

1. Unlike many other topics of research, surveys of privacy concerns are by their nature likely not to include members of the population who would be most concerned about

Public Opinion Quarterly Volume 54:125–143 © 1990 by the American Association for Public Opinion Research
Published by The University of Chicago Press / 0033-362X/90/0054-01\$2.50

THE POLLS—TRENDS

PRIVACY IN THE INFORMATION AGE

SAMUEL J. BEST
BRIAN S. KRUEGER
JEFFREY LADEWIG

Abstract In recent years, surveillance has become an increasingly salient political issue in the United States. In this article we present data on public opinion about privacy invasions and surveillance techniques since 1990. Generally speaking, the polls show that concern about threats to personal privacy has been growing in recent years. Although the public was temporarily willing to expand the government’s investigative powers in the aftermath of the September 11, 2001, terrorist attacks, support for most forms of surveillance has declined.

Many policy debates in the United States involve a trade-off between institutional interests’ coveting citizens’ personal information and individual privacy. Government agencies want broader powers to investigate Americans suspected of crimes or terrorism. Businesses want to track consumer behavior to better understand purchasing habits. Employers want methods to reduce shirking and dysfunctional behavior among their employees. In each context, questions surface about the forms of surveillance that are acceptable, the types of abuses that may occur, and under what circumstances collective interests trump individual ones. Understanding where the public stands on these issues is a critical component of the debates (Sheehan 2004; U.S. House 2001).

Building on an article from 1990 (Katz and Tassone 1990), we present longitudinal data on public opinion about privacy over the last 15 years. Since 1990, there have been three major developments capable of shifting public opinion about privacy: (1) the emergence of the Internet as a new communication technology; (2) the commencement of the “war on terrorism”; and (3) the development of a wide array of new surveillance technologies. Together these events have spawned considerable polling on opinion toward different forms

SAMUEL J. BEST is the director of the Center for Survey Research and Analysis at the University of Connecticut. BRIAN S. KRUEGER is an associate professor in the Department of Political Science at the University of Rhode Island. JEFFREY LADEWIG is an assistant professor in the Department of Political Science at the University of Connecticut. Address correspondence to Samuel Best; e-mail: sam.best@uconn.edu.

doi:10.1093/poq/nf018

© The Author 2006. Published by Oxford University Press on behalf of the American Association for Public Opinion Research. All rights reserved. For permissions, please e-mail: journals.permissions@oxfordjournals.org.

Is RCT Tenable as a Model?

Westin's approach places a high value on individuals negotiating in the marketplace for privacy, but the knowledge gap we elucidate shows that many consumers already believe that privacy rights are enshrined in privacy policies and guaranteed by law. Laboring with this myopic view of their duties as consumers, individuals have no reason to bargain for privacy in the marketplace.

Is RCT Tenable as a Model?

Westin's approach places a high value on individuals negotiating in the marketplace for privacy, but the knowledge gap we elucidate shows that many consumers already believe that privacy rights are enshrined in privacy policies and guaranteed by law. **Laboring with this myopic view of their duties as consumers, individuals have no reason to bargain for privacy in the marketplace.**

When RCT Fails, Move the Goalposts



Myopia as Strategy?

- Thinking in terms of myopia also addresses a common rational choice explanation that consumers do not read privacy policies because it is rational to remain ignorant.

- “The point is not that transaction costs are particularly high, because it does not take long to process a privacy notice. Rather, processing privacy notices is a cost that most consumers apparently do not believe is worth incurring. The perceived benefits are simply too low...The reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy.” --Beales & Muris (2008)

Our research suggests a different conclusion:
Consumers they think they are protected, and so
they do not believe there is value to be had in
reading about those protections.

A Final Note About Westin

- This survey work should not overshadow Westin's seminal contribution to privacy
- Against tech determinism
- Privacy as liberal value



Implications for FTC practice

1. View Privacy Policies as Seals



2. A MAC for Privacy

- In the 1970s, the FTC embedded marketing professors in the BCP—the Marketing Academic Consultancy program (MAC)
- MAC helped the FTC jettison RCT approaches to understanding marketing, and fostered a more realistic interpretation of ads
- A MAC program for privacy could help the agency understand the limits of notice and choice

3. From Deception to Unfairness

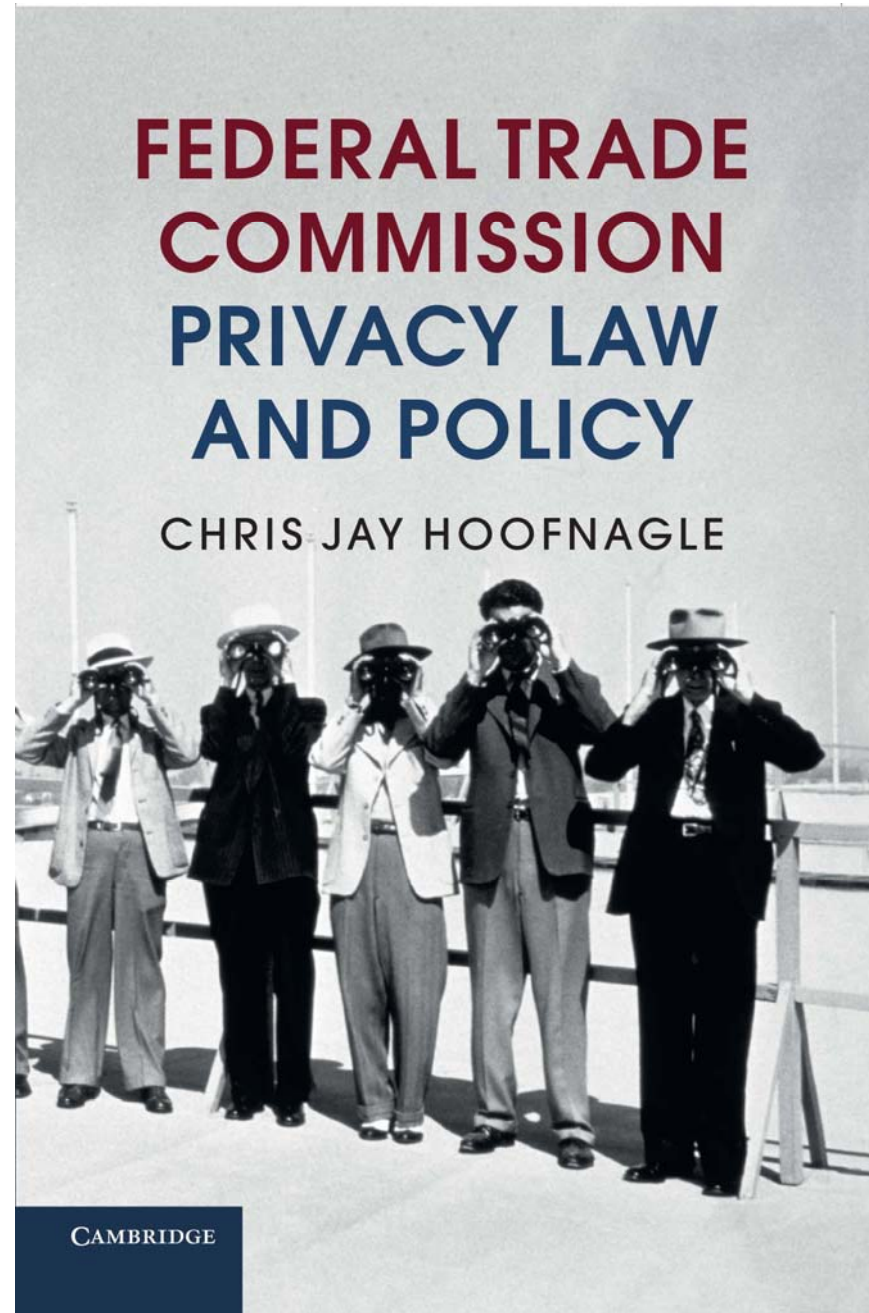
- How far can deception align practices with consumer expectations?
 - Notices can be “perfected”
 - Yet since consumers conceive of them as a seal, they go unread
- The FTC’s most important cases are those where the common law, contract, and tort, would offer no remedy or where consumers would lack standing (Sears, Nomi)

3. From Deception to Unfairness

- BE could develop a theory of substantial injury from privacy-invasive practices
- One source to draw from: transaction cost economics.
- Lock in, shifting practices, asset uniqueness make personal info transactions continuous ones. See e.g. Hoofnagle & Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. Rev. 606 (2014)

Thank you

My new book, Federal Trade Commission Privacy Law and Policy, is a 100-year history of the agency's consumer protection mission. It also discusses some findings presented today.



Joseph Turow

University of Pennsylvania

The Tradeoff Fallacy

Co-authors: Michael Hennessy (University of Pennsylvania); Nora Draper (University of New Hampshire)



A photograph of a large warehouse or retail store aisle. The aisle is long and narrow, with high shelves on both sides. The shelves are filled with various items, including boxes and bags. The floor is a light-colored concrete. The lighting is bright, coming from overhead fixtures. The perspective is from the end of the aisle, looking down its length.

The Tradeoff Fallacy: Americans and The New Data-Gathering Environment

Joseph Turow &
Michael Hennessy
University of
Pennsylvania

Nora Draper
University of New
Hampshire

Summary

- Marketers justify their data-collection with the notion that **Americans want and understand benefits of data tradeoffs.**
- We challenge this assertion with results of a national (wireline/cell) telephone survey.
- Further, we present evidence that **what observers interpret as tradeoff behavior is really widespread resignation** among Americans regarding marketers' use of their data.

What is the issue?

- Polls repeatedly find that consumers are concerned about ways marketers access and use their data online.
- Annenberg, Pew, Bain & Company
- At the same time, observers concur people often release data about themselves that suggest much less concern.
- The privacy paradox.

**SOME MARKETERS READ THIS
PARADOX AS EVIDENCE PEOPLE PLACE
OTHER THINGS ABOVE PRIVACY—
WHICH LEADS TO THE NOTION OF
TRADEOFFS.**

- Yahoo (2014): Online Americans “demonstrate a willingness to share information, as more consumers begin to recognize the value and self-benefit of allowing advertisers to use data in the right way.”
- Mobiquity president (2012): “The average person is more than willing to share their information with companies if these organizations see the overall gain for end-users as a goal, not just for themselves.”

- A few corporate voices—Accenture, Bain, Brand Bond Loyalty—have put cautions around such generalizations.
- Bain: “Customers’ trust cannot be bought by companies offering compensation in exchange for selling or sharing personal data.”
- Others have urged transparency, without saying what that really should mean.

- Generally, firms argue that consumers understanding of tradeoffs along with increasing consumer power justifies consumer data collection and use.
- Marketers increasingly see personalization resulting from predictive analytics as a savior in our age of hyper-competition.
- Yahoo: “This concept of value exchange for personal data is starting to come to life through personalization...a pathway to advertising nirvana.”

The Tradeoff Logic Justifies 360° Tracking

- Gartner describes 4 stages toward “**cognizant computing**” that will unroll over the next 2-5 years, with the first two “well underway”
 - Sync me
 - See me
 - Know me
 - Be me

Alternative Explanations to Tradeoffs

- The public's **lack of knowledge** of what marketers are doing with their data behind the computer screen.
- Surveys show that lack.
- Cranor & McDonald on **privacy policies**
- Acquisti et al and others on the **difficulty of understanding the technological and institutional system.**

- This “knowledge failure” research explains the ease with which data retailers and advertisers retrieve information from individuals—though this proposition hasn’t been directly tested.
- But it may get marketers off the hook too easily – to blame schools and the media,
- And to institute Ad Choices,
- And to sound more optimistic about the public than advocates and policymakers.

Alternative Explanation:

- The privacy paradox is about far more than people's cost benefit analysis or lack of knowledge.
- It is about **citizens' belief they have no agency** in a central area of democratic society: commerce.
- **Americans have slid into resignation**—a sense that while they want control over their data world they will never achieve it.

Our Survey

- 20 minute average interviews
- February-March 2015
- English or Spanish speaking sample of 1,506 internet users living in the continental US
- Landline 750, wireless 756
- Conducted by Princeton Survey Research Associates International.

Americans Reject Tradeoffs as Unfair

Table 2: Americans' Responses to Tradeoff-Attitude Statements (N=1,506)

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Neither*
If companies give me a discount, it is a fair exchange for them to collect information about me without my knowing it. (91% disagree)	3	5	14	77	1
It's fair for an online or physical store to monitor what I'm doing online when I'm there, in exchange for letting me use the store's wireless internet, or Wi-Fi, without charge. (71% disagree)	9	18	18	53	2
It's OK if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me. (55% disagree)	12	30	17	38	3

*Neither was a volunteered answer.

- Only 4% agree or agree strongly with all three propositions.
- Using a broader interpretation of a belief in tradeoffs, we found that still a small proportion—21%--believes common tradeoffs with marketers amount to a fair deal.

Evaluating a Form of the Privacy Paradox

- “For the next few questions, please think about the supermarket you go to most often. Let’s say this supermarket says it will give you discounts in exchange for its collecting information about all your grocery purchases. Would you accept the offer or not?”

- 52% say no
- Of the 43% yes, this is twice the broad definition of tradeoff supporters.
- Seems to be similar in % to those who agreed with third statement in Table 2.
- But 40% who accept the supermarket discount don't agree that "It's OK if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me."
- This lack of correspondence even when the scenarios appear similar underscores that a small percentage consistently accepts the idea of tradeoffs.

- We wanted to know whether people who say they will accept the supermarket discount would still do it when presented with specific assumptions a supermarket might make about them from analyzing their grocery-purchasing habits.
- This is knowledge Americans almost never receive directly but may intuit from ads and coupons they think are targeted to them.

**Table 3: Percentage of people who accept the supermarket offer and know supermarket will analyze grocery their purchases to make particular assumptions about them—
N=1506**

	<i>Yes</i> (%)
Accept the discounts without any specific assumptions added	43
Accept the discount knowing supermarket will make assumptions about	
Whether you tend to buy low-fat foods	33
Whether you have children and how old they are	27
What activities you might do outside of work	25
When you take vacations	22
The health status of you or someone in your family	21
How much money you make	21
Whether you are going through a major life event	19
Your racial or ethnic background	19

- The table shows the **limits of cost-benefit analysis as a rationale** for marketers' claims that most people will provide personal data in exchange for store deals.
- The decline in acceptance from 43% to around 20% is **not consistent with marketers' assertions** that people are giving up their personal information because of cost-benefit analysis.
- **In the supermarket scenarios, they are doing just the opposite:** resisting the idea of giving data for discounts.

Most Americans are Resigned

“the acceptance of something undesirable but inevitable.”

Table 4: Americans’ Responses to the Resignation Attitude Statements (N=1,506)

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Neither*	DK (%)
I want to have control over what marketers can learn about me online. (84% agree)	61	23	8	7	1	1
I’ve come to accept that I have little control over what marketers can learn about me online. (65% agree)	31	34	16	18	1	1

*“Neither” was a volunteered answer.

58% agree with both statements.

- There is a strong positive statistical relationship between believing in tradeoffs and accepting or rejecting various kinds of supermarket's use of discounts.
- By contrast, there is no statistical relationship between being resigned to marketers' use of data and accepting or rejecting the discounts.

- Put another way, people who believe in tradeoffs give up their data predictably, while people who are resigned don't do it in a predictable manner. They do give up their data, though.
- We found 57% of those who took the supermarket deal were resigned. A much smaller 32% were tradeoff supporters even using the broader measure of tradeoff support.

- The larger percentages of people in the population who are resigned compared to those who believe in tradeoffs indicate that **in the real world people who exchange their data for benefits are more likely to do it while resigned rather than as a result of cost-benefit analysis.**
- Moreover, **resignation is widespread** across the US population, regardless of age, gender, education, and race.

Knowledge to Make Tradeoffs

- We found that Americans often don't have the basic knowledge to make informed cost-benefit choices.
- We found large gaps in knowledge about basic data-marketing rules among large percentages of Americans.
- We also found that 51% cannot recognize the possibility of “phishing.”
- Large percentages believe incorrectly that government laws protect them from price discrimination and certain forms of data collection.

- These widespread misconceptions suggest that even when Americans do weigh the costs and benefits of giving up their data, they frequently base those choices on **incorrect information**.
- But we also found that those who **know more** about the marketing laws and practices **are more likely to be resigned**.
- We found, too, that resigned people who accept supermarket discounts even as the supermarket collects increasingly personal information tend to have **more knowledge than others**.
- So having **more knowledge is not the protective feature** academics have suggested.

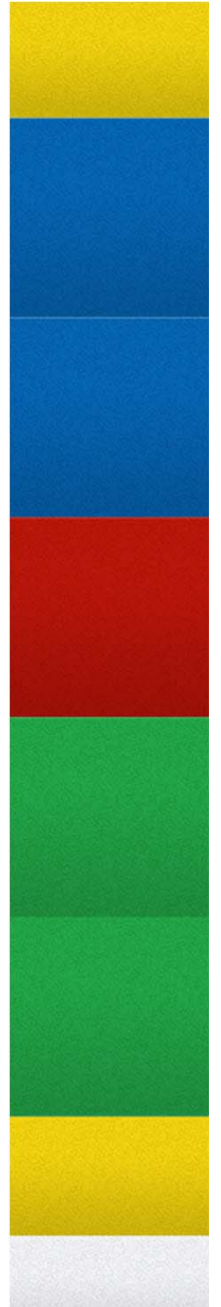
So What?

- The **rationale of tradeoffs** is a fig leaf used by marketers to justify a world of tracking and increasingly personalized profiling that people know is there, don't understand, and say they don't want.
- We haven't begun to **consider the social implications** of having a large population that is **resigned** about a key aspect of its everyday environment.

- We are **only at the beginning** of key aspects of this era, and there may be time for concerned parties to guide it.
- **Academics, journalists and advocates** have to translate they key issues for the public.
- Issues of **obfuscation and deception**
- The **public interest, convenience, and necessity**
- **Naming, praising, shaming**

THANKS FOR
LISTENING.

JosephTurow



Discussion of Session 1

Discussants:

- **Justin Brookman**, Federal Trade Commission
- **Omer Tene**, International Association of Privacy Professionals
- **Elana Zeide**, New York University School of Law

Presenters:

- **Ibrahim Altaweel**, University of California, Berkeley
- **Steven Englehardt**, Princeton University
- **Chris Jay Hoofnagle**, University of California, Berkeley Law
- **Joseph Turow**, University of Pennsylvania

