TODAY

1. tracking mechanisms
2. prevalence: web
3. prevalence: mobile
4. consumer choice
5. existing incentives
6. what to do
BROWSERS
PRIVACY BY DESIGN

NCSA Mosaic™ for Microsoft Windows

Welcome to the Mosaic for Microsoft Windows Home Page. Mosaic is a World Wide Web client that was developed at the National Center for Supercomputing Applications on the campus of The University of Illinois in Urbana-Champaign.

Search Our Space

News and Announcements

- Version 2.0.0
- New! Wm32s Information
- World Wide Web Software Information
Google Chrome, Firefox Adding 'Do Not Track' Tools

DANA WOLLMAN | 01/24/11 05:20 PM

NEW YORK — The Firefox and Google Chrome browsers are getting tools to help users block advertisers from collecting information about them.

Fedor Gevcik, a technology and privacy officer for browser maker Mozilla, said the "Do Not Track" tool will be the first in a series of steps designed to give users privacy. He didn't say when the tool will be available.

Google Chrome users can now download a browser plug-in that blocks advertisers — but only from ad networks that already let people decline personalized, targeted ads. According to Google Inc., these include the top 15 advertising networks, as rated by the research group comScore, a group that includes AOL Inc., Yahoo Inc. and Google itself.

The next version of Microsoft Corp.'s Internet Explorer browser, which is still being developed, will include a similar feature, though people will have to go into options to find their own list of sites to block.
Google Chrome, Firefox Adding 'Do Not Track' Tools

DANA WOLLMAN | 01/24/11 05:20 PM

Google Chrome and Firefox are getting tools to help users block advertisers from collecting information about them. Alex Fowler, a technology and privacy officer for Firefox maker Mozilla, said the "Do Not Track" tool will be the first in a series of steps designed to guard privacy. He didn't say when the tool will be available.

Chrome users can now download a browser plug-in that blocks advertisers — but only from ad networks that already let people decline personalized, targeted ads. According to Google Inc., these include the top 15 advertising networks, as rated by the research group comScore, a group that includes AOL Inc., Yahoo Inc. and Google itself.

The next version of Microsoft Corp.'s Internet Explorer browser, which is still being developed, will include a similar feature, though people will have to opt in.
http://pixel.quantserve.com/seg/p–6fTutip1SMLM2.js

GET /seg/p–6fTutip1SMLM2.js HTTP/1.1
Host: pixel.quantserve.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: mc=4d441f48–a100a–1f66c–277f6; d=EM0BPAGBB0HxBi6IlgwALhQnyAAiCD8sQmnDMQLEAC_UA
HTTP

observer

identifier

activity

http://pixel.quantserve.com/seg/p-6fTutip1SMLM2.js

GET /seg/p-6fTutip1SMLM2.js HTTP/1.1
Host: pixel.quantserve.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Accept: */*
Accept-Language: en-us.en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: mc=4d441f48-a100a-1f66c-277f6; d=EM0BPAGBBoHxBi6llgwALhQnyAAiCD8sQmnDMQLEAC_UA
PROFILE

observer + identifier + activity =

AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0.782.107 Safari/535.1"


http://www.google.com/search?sourceid=chrome&ie=UTF-8&q=spearment+rhino" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0.782.107 Safari/535.1"

http://static.huluim.com/system/hulu_108321_0729114110_1.css HTTP/1.1" - - "http://www.hulu.com/the-big-gay-sketch-show" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0.782.107 Safari/535.1"


# PROFILES

<table>
<thead>
<tr>
<th>Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Styles</strong></td>
</tr>
</tbody>
</table>
| - Affluent Baby Boomers  
| - Auto Enthusiasts  
| - Corporate Execs  
| - Fashionistas  
| - Female Small Appliance Shoppers  
| - Foodies  
| - Frequent Travelers*  
| - Gadget Geeks  
| - Green & Eco-Friendly  
| - Healthy & Fit  
| - High Spenders  
| - Luxury Sports New Parents  
| - Outdoor Enthusiasts  
| - Seniors  
| - Shopping Addicts  
| - Soccer Moms  
| - Sportsmen  
| - Trendy Homemakers  
| - Young & Hip  
| **Demographics** |  
| - Age*  
| - Education*  
| - Estimated Credit Utilization*  
| - Estimated Household Income*  
| - Estimated Net Worth*  
| - Family Member Age*  
| - Gender*  
| - Home Owner or Renter*  
| - Length of Residence*  
| - Median Home Value*  
| - Number of Adults in Household  
| - Occupation*  
| - Presence of Children*  
| - Type of Dwelling*  
| - User Hobbies & Interests* |
ECOSYSTEM
• 2009 study at Berkeley

• examined top 100 most-visited websites

• sample from ~30,000-45,000 users

• examine prevalence of 3rd party cookies / beacons / etc

http://knowprivacy.org/
MANY OBSERVERS

Monthly Traffic
(In Millions of Users)

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>Number of Beacons Found on Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>blogspot.com</td>
<td></td>
</tr>
<tr>
<td>typepad.com</td>
<td></td>
</tr>
<tr>
<td>google.com</td>
<td></td>
</tr>
<tr>
<td>blogger.com</td>
<td></td>
</tr>
<tr>
<td>msn.com</td>
<td></td>
</tr>
<tr>
<td>aol.com</td>
<td></td>
</tr>
<tr>
<td>yahoo.com</td>
<td></td>
</tr>
<tr>
<td>huffingtonpost.com</td>
<td></td>
</tr>
<tr>
<td>photobucket.com</td>
<td></td>
</tr>
<tr>
<td>tripod.com</td>
<td></td>
</tr>
<tr>
<td>careerbuilder.com</td>
<td></td>
</tr>
<tr>
<td>nytimes.com</td>
<td></td>
</tr>
<tr>
<td>monster.com</td>
<td></td>
</tr>
<tr>
<td>time.com</td>
<td></td>
</tr>
<tr>
<td>reference.com</td>
<td></td>
</tr>
<tr>
<td>merriam-webster.com</td>
<td></td>
</tr>
<tr>
<td>cnn.com</td>
<td></td>
</tr>
<tr>
<td>comcast.net</td>
<td></td>
</tr>
<tr>
<td>answers.com</td>
<td></td>
</tr>
<tr>
<td>geocities.com</td>
<td></td>
</tr>
</tbody>
</table>

Many Observers
MANY OBSERVERS

100 different beacons reported on blogspot.com in Mar `09

Blogspot.com
Typepad.com
Google.com
Blogger.com
Msn.com
Aol.com
Yahoo.com
Huffingtonpost.com
Photobucket.com
Tripod.com
Careerbuilder.com
Nytimes.com
Monster.com
time.com
Reference.com
Merriam-webster.com
Cnn.com
Comcast.net
Answers.com
Geocities.com
Cnet.com
MANY OBSERVATIONS

Google beacons reported on 92 of Top100 in Mar `09
~2.15 Billion Unique Visits/Mo
MANY OBSERVATIONS

Google ‘trackers’ on 88% of websites we sampled

Google (348,059 Unique Domains in Mar '09)
MANY OBSERVATIONS

“10,000 new websites integrate with Facebook every day”
Sheryl Sandberg - Facebook COO - Oct 2010

“Users submit about 650,000 comments every minute”
Ken Deeter on Live Commenting - Jan 2011
ECOSYSTEM

Get your very own impossibly small iPod® nano FREE*!

Limited time only!

CLICK HERE NOW
MOBILE
SMARTPHONES
• 2010 study for the Wall Street Journal

• examined top 100 most popular ‘apps’ (50 iPhone / 50 Android)

• looked for leakage of ‘sensitive information’

• looked for transmission to 1st* and 3rd parties

• include SSL encrypted traffic*
SENSITIVE DATA

What we know on one

The iPhone version of music app Pandora sends eight tracker devices to send data to several phone ID to demographic...

Categories of data:
- Phone number
- Number, gender
- Location
- Phone ID
PROFILE

\[ \sum \text{observer} + \text{Phone ID} + \text{activity} = \text{persistent} \]
TRANSMISSION

• 47 apps sent location to 1 or more parties

• 56 transmit unique device id’s

• phone numbers, (entire) address books, sms messages sometimes sent to 1st/3rd parties
SURPRISING?

<table>
<thead>
<tr>
<th>App name</th>
<th>Username, Password</th>
<th>Contacts</th>
<th>Age, Gender</th>
<th>Location</th>
<th>Phone ID</th>
<th>Phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.03 Seconds Pro</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age My Face</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angry Birds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angry Birds Lite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aurora Feint II: Lite</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barcode Scanner (BahnTech)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bejeweled 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best Alarm Clock Free</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SURPRISE ?!
CHOICE
## NAI OPT-OUT INTERFACE

<table>
<thead>
<tr>
<th>Member Company</th>
<th>Status</th>
<th>Opt-Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>aCerno</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AdBrite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AdChemistry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adconion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adara Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adify Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AdMeld</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertising.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregate Knowledge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Akamai</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**No Cookie**
You have not opted out and you have no cookie from this network.
Successfully Opted-Out

You have successfully opted-out.

A few things you should know:

- You may still see the same number of ads as before, but they may be less relevant because they will.
- You may still see ads related to the content in an application or based on other non-personal information.
- If you use more than one Apple mobile device, you will have to opt-out from each device individually.
- This opt-out applies only to Apple advertising services and does not affect interest-based advertising.

Notify me

Google AdMob Ads Preferences

Choose whether to receive interest-based ads from Google and AdMob in mobile apps on this device. Learn more

Receive interest-based ads

Copyright © 2010 Apple Inc. All rights reserved. Terms of Use | Privacy Policy
• consumers need to know about tracking
• opt-outs are brittle
• there’s no mechanism to opt out of tracking
NO CHOICE?

OPT-OUT of TARGETING ≠ OPT-OUT of TRACKING
CHOICE

Accept cookies from sites

Accept third-party cookies

Third-party Cookies
- Accept
- Block
- Prompt

Accept cookies:
- Always
- Never
- Only from sites I visit
Block cookies from third parties and advertisers.

Block all third-party cookies without exception
DELETE COOKIES?!
NO CHOICE?

• 2009 study at Berkeley on “Flash Cookies”

• identified 54 of the top 100 websites uses ‘flash cookies’

• tracking mechanism outside the control of most consumers

• 31 sites had matching cookies to enable ‘respawning’ (circumvention)

You Deleted Your Cookies? Think Again

By Ryan Singel · August 10, 2009 | 7:39 pm | Categories: Advertising

More than half of the internet's top websites use a little known capability of Adobe's Flash plug-in to track users and store information about them, but only four of them mention the so-called Flash cookies in their privacy policies, UC Berkeley researchers reported Monday.

Unlike traditional browser cookies, Flash cookies are relatively unknown to web users, and they are not controlled through the cookie privacy controls in a browser. That means even if a user thinks they have cleared their computer of tracking objects, they most likely have not.
NO CHOICE?

WTF is this?!?
NO CHOICE? (V2)

• 2011 followup Berkeley Study

• 37 of the top 100 websites uses ‘flash cookies’

• 15 of the top 100 uses HTML5 storage (ala ringleader)

• ~5000 third party cookies set from just using top100 websites

Researchers Expose Cunning Online Tracking Service That Can’t Be Dodged

By Ryan Singel | July 29, 2011 | 8:24 pm | Categories: Privacy
TECH
HULU RESPAWN

Initially using 3rd party Flash code from Quantcast

but...

Lawsuit Hits Companies Using 'Zombie' Flash Cookies

Posted by kdawson on Tuesday July 27 2010, @09:43PM from the brains-for-a-filling dept.

A privacy activist has filed a lawsuit targeting eight corporate users of Quantcast's "zombie" Flash cookies, in addition to Quantcast itself. The suit alleges that MTV, ESPN, MySpace, Hulu, ABC, Scribd, and others used Quantcast's Flash-based cookies to recreate browser tracking cookies that users had taken the trouble to delete.
function setComputerguidInFSO(value) {
    com.ns.utils.ConsoleLogger.getInstance().debug("setComputerguidInFSO: Start");
    _globalFSO = SharedObject.getLocal("BeaconService", "/");
    _globalFSO.data.computerguid = value;
    _globalFSO.flush();
    com.ns.utils.ConsoleLogger.getInstance().debug("setComputerguidInFSO: Done");
}

Via Flash in http://www.hulu.com/guid.swf?v2
Safari/Mozilla/Chrome

params = Object.extend(params, {
    user_id: Behaviors.getUserld(),
    history: UserHistory.get_history(),
    watched_history: UserHistory.get_watched_history(),
    guid: Beacon.computerGUID()
});

this.set = function(k, v) {
    if (store)
        store.setItem(k, v);
}

Internet Explorer

var userData = backend.create(function(
    return !! window.ActiveXObject &&
}, function() {

    var store = appendDiv(function(div) {
        div.id = '_cram_userData';
        div.style.display = 'none';
        div.addBehavior('#default#userData');
    });

    store.load("_cram");
Via Flash, HTML5, AND Cache ETag in
http://doug1izaerwt3.cloudfront.net/5a68d120b211c810289fc36493663648821d58aa.1.js

FLASH:
ifc = initializeFlashCookie
fsc = flashSaveCookie
fgc = flashGetCookie

HTML5 LocalStorage:
ils = initializeLocalStorage
lss = localStorageSave
lsg = localStorageGet

Cache ETags: KM_CID

IE UserData:
iud = initializeUserData
uds = userDataSave
udg = userDataGet

http://pastebin.com/FhUYuRsb
ETAGS

via http://i.kissmetrics.com/i.js

INITIAL REQUEST:
GET /i.js HTTP/1.1
Host: i.kissmetrics.com

RESPONSE:
Etag: "Z9iGGN1n1-zeVqbgzrlKkl39hiY"
Expires: Sun, 12 Dec 2038 01:19:31 GMT
Last-Modified: Wed, 27 Jul 2011 00:19:31 GMT
Set-Cookie: _km_cid=Z9iGGN1n1-zeVqbgzrlKkl39hiY; expires=Sun, 12 Dec 2038 01:19:31 GMT; path=/;

SUBSEQUENT REQUEST:
GET /i.js HTTP/1.1
Host: i.kissmetrics.com
If-None-Match: "Z9iGGN1n1-zeVqbgzrlKkl39hiY"

CONTENTS:
VAR KMCID='Z9iGGN1n1-zeVqbgzrlKkl39hiY'; if(typeof(_kmil) == 'function')_kmil();
Cache entry information

key: http://i.kissmetrics.com/i.js
fetch count: 8
last fetched: 2011-07-26 22:03:36
last modified: 2011-07-26 21:59:12
expires: 2038-12-11 20:19:31
Data size: 79
file on disk: none
Security: This document does not have any security info associated with it.

Client: HTTP
header: HTTP/1.1 200 OK
Cache-Control: max-age=864000000, public
Content-Type: application/x-javascript
Date: Wed, 27 Jul 2011 01:19:31 GMT
Etag: "29iGGNnl-zeVgbzrLKk139hY"
Expires: Sun, 12 Dec 2038 01:19:31 GMT
Last-Modified: Wed, 27 Jul 2011 00:19:31 GMT
P3P: CP="NOI CURa ADMa DEVa TAIa OUR IND UNI INT"
Server: nginx
Content-Length: 79
charset: ISO-8859-1

```javascript
var KMCID='29iGGNnl-zeVgbzrLKk139hY';if(typeof f(_km1) == 'function') _km1();
```
MATCHING 1ST PARTY COOKIES

<table>
<thead>
<tr>
<th>Site</th>
<th>Cookie Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>hulu.com</td>
<td>km_ai</td>
</tr>
<tr>
<td>i.kissmetrics.com</td>
<td>_km_cid</td>
</tr>
<tr>
<td>seomoz.org</td>
<td>km_ai</td>
</tr>
<tr>
<td>spotify.com</td>
<td>km_ai</td>
</tr>
<tr>
<td>spotify.com</td>
<td>km_uq</td>
</tr>
<tr>
<td>spokeo.com</td>
<td>km_ai</td>
</tr>
<tr>
<td>spokeo.com</td>
<td>km_uq</td>
</tr>
<tr>
<td>gigaom.com</td>
<td>km_ai</td>
</tr>
<tr>
<td>gigaom.com</td>
<td>km_uq</td>
</tr>
<tr>
<td>shoedazzle.com</td>
<td>km_uq</td>
</tr>
<tr>
<td>shoedazzle.com</td>
<td>km_uq</td>
</tr>
<tr>
<td>etsy.com</td>
<td>km_ai</td>
</tr>
<tr>
<td>etsy.com</td>
<td>km_uq</td>
</tr>
</tbody>
</table>

Name: km_ai
Content: GuTj890-_-xGvfgtGQG99dUqTPRA
Domain: .hulu.com
Path: /
Send For: Any type of connection
Expires: July 26, 2016 11:33:05 PM
PRIVATE
Multiple People/Same Computer (Advanced)

What happens if someone in the same household uses the same computer and you call `identify` again? KISSmetrics will automatically detect this and **will not** alias the two named identities together (it will recognize them as separate people). However, it should be noted that any activity before you call `identify` for the second user will be attributed to the first user. Let’s see how this works:

1. Bob comes to your site and is assigned the anonymous identity `qFq2LweZugFNE4049hLhmRPBW34`
2. Bob then logs in and you call `identify` telling us that the identity is now `bob@site.com`. The activity from before Bob logs in (when we knew him as `qFq2LweZugFNE4049hLhmRPBW34`) is automatically tied to `bob@site.com`.
3. All activity continues to be attributed to `bob@site.com`, even after Bob logs out.
4. Now Bob’s brother Bill comes in to use the computer and visits your site. All activity will continue to be attributed to `bob@site.com`. KISSmetrics has no way to know that it is a different person sitting at the keyboard automatically.
5. Bill logs in and you call `identify` telling us that the identity is now `bill@site.com`. KISSmetrics **does not** alias `bill@site.com` and `bob@site.com` - it treats these as two separate people.
6. All activity from this point on is attributed to `bill@site.com` (until you call `identify` again)
Lawsuit Targets Mobile Advertiser Over Sneaky HTML5 Pseudo-Cookies

By David Kravets  September 16, 2010  6:18 pm  Categories: Surveillance, privacy

Facebook Like button tracks you, even if you don’t click

May. 19, 2011 (10:14 am) By: Lee Mathews

Race Is On to 'Fingerprint' Phones, PCs

By JULIA ANGWIN And JENNIFER VALENTINO-DEVRIES

IRVINE, Calif.—David Norris wants to collect the digital equivalent of fingerprints from every computer, cellphone and TV set-top box in the world.

He's off to a good start. So far, Mr. Norris's start-up company, BlueCava Inc., has identified 200 million devices. By the end of next year, BlueCava says it expects to have cataloged one billion of the world's estimated 10 billion devices.
**MANY ACTORS**

**Solution:** The Convertro Visitor Tracking Code completely eliminates the issues of cookie dependency. This means that a visitor can clear his/her browser cookies and cache or toggle between browsers and still appear as a unique visitor. We also have at least a 50% success rate tracking the same visitor across machines if they do end up converting. The result is a very rich set of conversion data that most accurately represents the true sources that drove any particular conversion.

2. **On average, visitors use 1.5 browsers to surf the internet.** Since cookies are browser specific, when the customer switches between browsers, conventional methods duplicate these visitors.

3. Increasingly strict browser default privacy and security settings can result in the blocking of third party cookies and, in some cases, first party cookies. Cookie-dependent methods would be ineffective under these scenarios.

4. **If a customer visits a site via two different machines prior to a conversion event, the visitor sessions will not be linked,** causing traditional analytics software to report two different visitors – one that purchased and one that didn’t.
Two major Web companies, Hulu and Spotify, have been sued by KISSmetrics because they were using 'ETag' technology to track visits to their website.

The case, filed by John Kim and Dan Schutzman, is the second major lawsuit stemming from KISSmetrics' technology, which relies on ETags for tracking. Last week, two different Web users sued KISSmetrics and Hulu for allegedly violating federal and state laws with ETags. The technology is controversial because ETags can be used to track consumers even when they delete their cookies.
CHOICE?
SURPRISE ?!
THE LOVESTORY
only browser that blocks 3rd party cookies by default
INCENTIVE$  
(PARTFORMS <3 ADS)
INCENTIVES

consumers
initial revenue from sale of phone (licensing/etc)

smartphone platforms = advertisers

admob

developers
ongoing revenue from app sales

iAd

ongoing revenue from advertising
# FACEBOOK: INCENTIVES

## Fields

The `User` object has the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Permissions</th>
<th>Returns</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The user's Facebook ID</td>
<td>No <code>access_token</code> required</td>
<td>string</td>
</tr>
<tr>
<td>name</td>
<td>The user's full name</td>
<td>No <code>access_token</code> required</td>
<td>string</td>
</tr>
<tr>
<td>first_name</td>
<td>The user's first name</td>
<td>No <code>access_token</code> required</td>
<td>string</td>
</tr>
<tr>
<td>middle_name</td>
<td>The user's middle name</td>
<td>No <code>access_token</code> required</td>
<td>string</td>
</tr>
<tr>
<td>last_name</td>
<td>The user's last name</td>
<td>No <code>access_token</code> required</td>
<td>string</td>
</tr>
<tr>
<td>gender</td>
<td>The user's gender</td>
<td>No <code>access_token</code> required</td>
<td>string</td>
</tr>
<tr>
<td>locale</td>
<td>The user's locale</td>
<td>No <code>access_token</code> required</td>
<td>string containing the ISO Language Code and ISO Country Code</td>
</tr>
</tbody>
</table>
PERCEPTIONS

*our browsers are our ‘user agent’*

*we ‘buy’ our mobile devices*

*facebook is for us to connect to ‘our friends’*
“if you're not paying for it, you're the product being sold”
WHAT TO DO?
What Can You Do? Not Much

By JENNIFER VALENTINO-DEVRIES

It's nearly impossible to prevent cellphone "apps"—games and other software—from transmitting information about a phone and its owner.

Turning off the phone's location services can restrict tracking by location. But it can limit some phone features like maps.
An app that has requested your location within the last 24 hours will show the location services icon next to its name.
Use Google location

Google's location service provides applications with your approximate location without using GPS.

You can disable these features in Settings, under Location & Security and under Privacy.

- Allow Google's location service to collect anonymous location data. Collection will occur even when no applications are running.

- Use My Location for Google search results and other Google services.
Your messages
edit SMS or MMS, read SMS or MMS, receive MMS, receive SMS

Network communication
full Internet access

Phone calls
read phone state and identity

Storage
modify/delete SD card contents

Your personal information
read contact data, write contact data

This application has access to the following:

Network communication
full Internet access

Phone calls
read phone state and identity

Storage
modify/delete SD card contents

Your messages
edit SMS or MMS, read SMS or MMS, receive MMS, receive SMS

Services that cost you money
directly call phone numbers, send SMS messages

Storage
modify/delete SD card contents

Your personal information
read contact data, write contact data
Network security for Android.

WhisperMonitor provides a software firewall capable of dynamic egress filtering and real-time connection monitoring, giving you control over where your data is going and what your apps are doing.

Dynamic egress filtering.

When enabled, WhisperMonitor will monitor all outbound network traffic and issue dynamic prompts in order to determine egress filter rules.
MobileScope

Identifying Leaky Smartphone Apps

In the wake of the WSJ's "What They Know" inquiry it was obvious to us that for average smartphone users there is not much that can be done to prevent the leakage of sensitive information.

Technically savvy users can jailbreak their iPhones or root their Androids or create special network environments to gain visibility into their smartphone traffic. However, for normal people the phone is a black box they can't peer into.

Our MobileScope project aims to change that.

Project Goals

The primary goal of the MobileScope project is to provide a service whereby users of smartphones can quickly and easily see what information is emanating from their smartphone.
MobileScope: demo
MobileScope: primary concepts

• use handset agnostic network inspection to detect patterns

• applications for both security & privacy

• toggle on/off as needed to analyze new or suspect applications
mobilescope: current capability

• traffic inspection for any handset capable of PPTP VPN

• SSL inspection for iOS devices

• rudimentary self-service enrollment

• basic signatures for mobile malware and PII leaks
mobilescope: next steps

- bulletproof / easy self-enrollment
- optional auto-detection of unique identifiers
- SSL VPN: better NAT traversal
- SSL inspection for Android devices?
- autoconfiguration for Android?
- enhanced signatures for mobile malware and PII leaks
- better visualization / communication of results
mobilescope: technical concerns

- VPN API’s are private and/or immature
- proxy architecture creates latency
- storing “dossiers” on end users makes us a target
- egress filtering/fraud detection on our network
MobileScope

What is your smartphone leaking today?

Register

All we need is your email address and a password to get started

eMail Address
you@domain.ext

Your eMail address is your username

Password
Up to 50 characters

Confirm Password

Please re-enter your password to confirm

Device  ○ iOS  ○ Android
Choose the type of device you will be testing with this account

SSL Inspection  ○
Supported on iOS only presently.

Sign up
Install Profile

MobileScope
dev.mobiloscope.net

✔ Verified

Install

Description
This profile configures a VPN connection to the MobileScope cloud and also installs a private trusted root certificate that allows MobileScope to inspect SSL traffic sent to or from your device.

Signed
dev.mobiloscope.net (466870-Q7WcHYC1368cFaK)

Received
Jul 21, 2011

Contains
Certificate
VPN Settings

More Details
MobileScope Collusion

Each dot represents an app or a website which has received a canary hit

data.flurry.com

The host data.flurry.com tracks your behavior across the following apps.

- CBS News
- Grindr
- Shazam
- MyFitnessPal
- Bible
- NYTimes
- PaperToss
- YelpiPhone
# This Ruleset is Emerging Threats Open optimized for snort-2.8.4.

alert tcp HOME_NET any -> EXTERNAL_NET 8080 (msg:"ET MOBILE MALWARE Android Trojan Command and Control Communication"; flow:established,to_server; content:"POST "; nocase)

alert tcp HOME_NET any -> EXTERNAL_NET $HTTP_PORTS (msg:"ET MOBILE MALWARE Google Android Device HTTP Request"; flow:established,to_server; content:"|0d 0a|User-Agent|3

alert tcp HOME_NET any -> 184.105.245.17 8080 (msg:"ET MOBILE MALWARE DroidDream Android Trojan info upload"; flow:to_server,established; uri:content:"/GMServlet/GMServlet")

alert tcp HOME_NET any -> EXTERNAL_NET $HTTP_PORTS (msg:"ET MOBILE MALWARE Android Trojan HongTouTou Command and Control Communication"; flow:established,to_server; content:"POST "; nocase)

alert tcp HOME_NET any -> EXTERNAL_NET 8118 (msg:"ET MOBILE MALWARE Android Trojan MSO.PJApps checkin 1"; flow:established,to_server; content:"/push/androidxml/"; depth:

alert tcp HOME_NET any -> EXTERNAL_NET 9033 (msg:"ET MOBILE MALWARE Android Trojan MSO.PJApps checkin 2"; flow:established,to_server; content:"/log"; depth:100; nocase)

alert tcp HOME_NET any -> EXTERNAL_NET 8080 (msg:"ET MOBILE MALWARE Android Trojan DroidDream Command and Control Communication"; flow:established,to_server; content:"POST "; nocase; depth:5; content)

alert tcp HOME_NET any -> EXTERNAL_NET 81 (msg:"ET MOBILE MALWARE Android Trojan Fake10086 checkin 1"; flow:established,to_server; content:"POST "; nocase; depth:5; content)

alert tcp HOME_NET any -> EXTERNAL_NET 9033 (msg:"ET MOBILE MALWARE Android Trojan Fake10086 checkin 2"; flow:established,to_server; content:"req.php"; nocase; depth:200
The Zeus banking Trojan has jumped the bridge to the large and growing ecosystem of mobile devices powered by Google's Android operating system, according to security researchers at Fortinet.

Researchers say they have obtained a Zeus variant, dubbed "Zitmo," that can run on Android phones and that has the ability to intercept one time pass codes sent to mobile phones as an added, "two factor" security measure.
BUT
WHACK-A-MOLE?
we need policy AND technology working in tandem
DO NOT TRACK

IDEA: create a reliable signal to companies that a given user does not wish to be tracked
DEFINITION

observer event identifier

collect use identify
IMPLEMENTATIONS

header based signal

blocking collection
OPEN QUESTIONS
OPEN QUESTIONS

• what should the default be? (what’s the right balance?)

• can consumers reasonably judge risk?

• will control mechanism enable even more invasive collection? (affirmative consent = worse practices)

• does this paradigm favor certain players? (i.e those with 1st party relationships)

• how will international compliance be enforced?
OVERLOAD
OPT-IN?

cute
OVERLOAD

Opting in is the new way to consent to receive messages or offers from businesses. It's a voluntary choice, allowing you to decide whether you want to receive communications from a particular company.

The Wall Street Journal

Most Popular

ESPN

TV
REASONABLE RISK?

BACKUPS?
BEHAVIORAL ECONOMICS

hyperbolic discounting / availability heuristic
• what should the default be? (what’s the right balance?)

• can consumers reasonably judge risk?

• will control mechanism enable even more invasive collection? (affirmative consent = worse practices)

• does this paradigm favor certain players? (i.e those with 1st party relationships)

• how will international compliance be enforced?
QUESTIONS?

ashkan.soltani@gmail.com
twitter: ashk4n

http://knowprivacy.org
http://blogs.wsj.com/wtk-mobile/
http://ashkansoltani.org/img/location_ecosystem.jpg