State of Ad Fraud Q4 2018

November 2018

Augustine Fou, PhD.
acfou [at] mktsci.com
212. 203 .7239

What is Ad Fraud?

Who Am I?

What is digital ad fraud ?

Ad Fraud = ad impressions caused by bots, not seen by humans

Impression Fraud

(CPM) Fraud

(includes mobile display, video ads)

Click Fraud

(CPC) Fraud

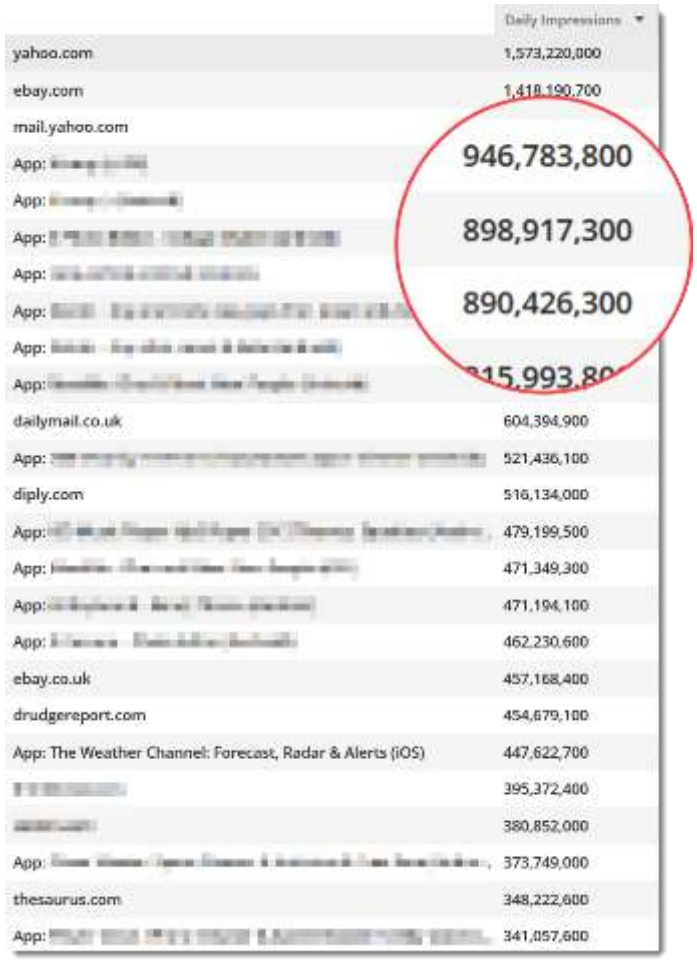
(includes mobile search ads)

How bad guys commit ad fraud

1. set up
FAKE SITES

2. buy
FAKE TRAFFIC

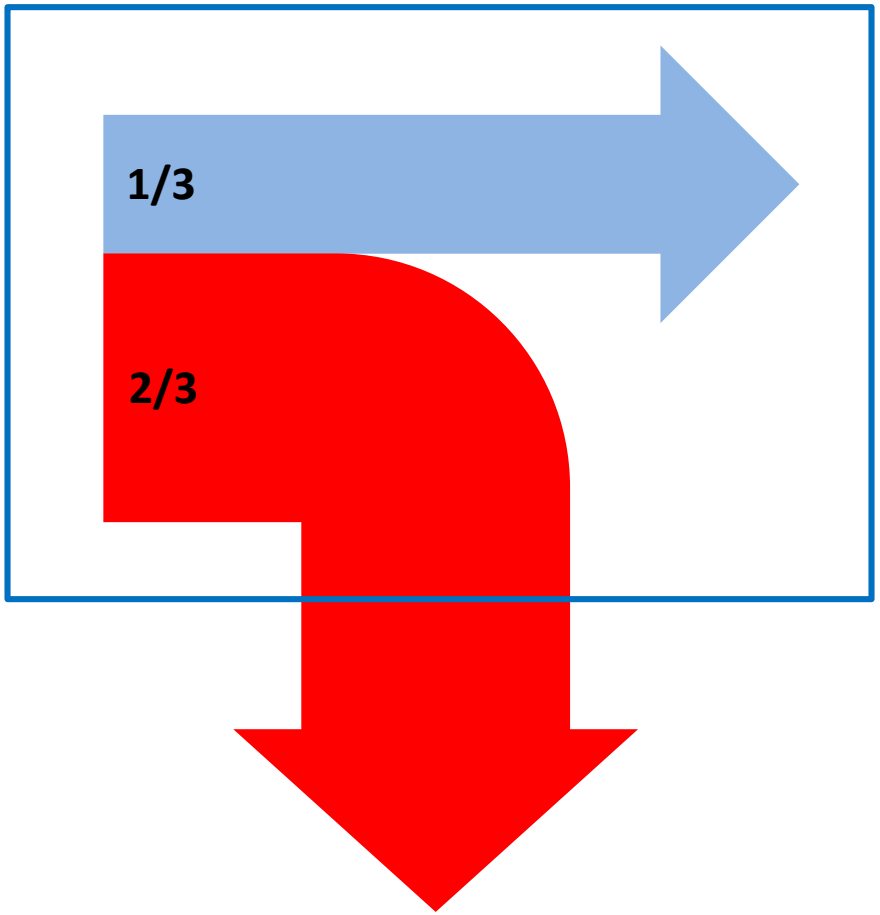
3. sell
FAKE ADS



Why is ad fraud bad?

Advertisers

Ads are not shown to humans, wasted ad dollars



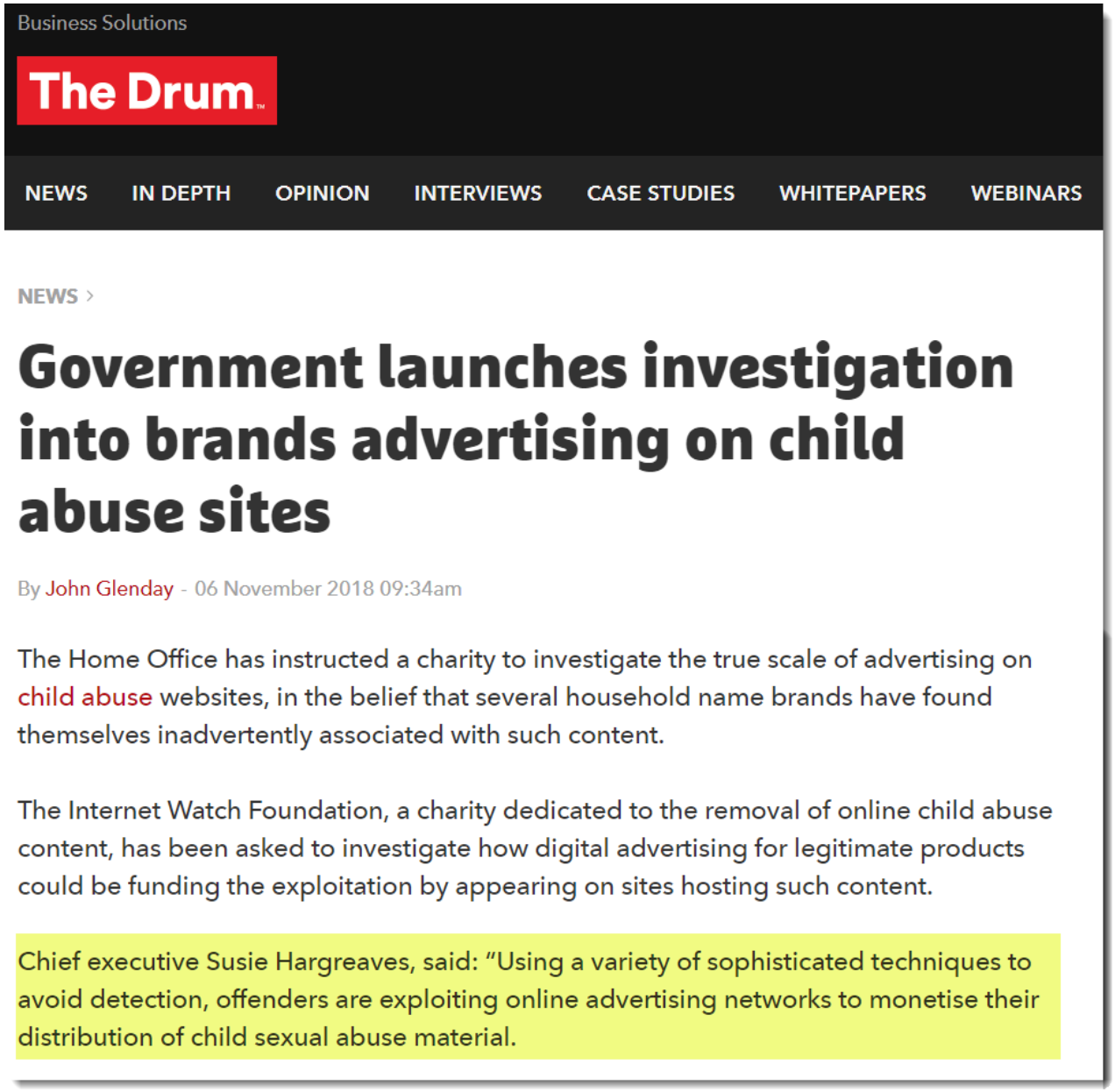
Publishers

Ad revenue declines because dollars are stolen by bad guys.

Bad Guys

Steal money using fake ads; siphon dollars out of ecosystem.

Ad dollars fund child abuse sites



Business Solutions

The Drum

NEWS IN DEPTH OPINION INTERVIEWS CASE STUDIES WHITEPAPERS WEBINARS

NEWS >

Government launches investigation into brands advertising on child abuse sites

By John Glenday - 06 November 2018 09:34am

The Home Office has instructed a charity to investigate the true scale of advertising on child abuse websites, in the belief that several household name brands have found themselves inadvertently associated with such content.

The Internet Watch Foundation, a charity dedicated to the removal of online child abuse content, has been asked to investigate how digital advertising for legitimate products could be funding the exploitation by appearing on sites hosting such content.

Chief executive Susie Hargreaves, said: "Using a variety of sophisticated techniques to avoid detection, offenders are exploiting online advertising networks to monetise their distribution of child sexual abuse material.

Source: The Drum Nov 6, 2018

"Using a variety of sophisticated techniques **to avoid detection**, offenders are exploiting online advertising networks to monetise their distribution of child sexual abuse material."

(2013) Ad dollars fund piracy sites

Segment	Ad Revenue	Margin
BitTorrent and Other P2P Portals		
Small	$2,079,334	85.9%
Medium	$3,227,159	84.5%
Large	$23,181,252	94.1%
Linking Sites		
Small	$3,690,915	79.9%
Medium	$8,351,446	89.8%
Large	$4,498,344	87.5%
Video Streaming Hosts		
Small	$529,480	79.9%
Medium	$1,681,477	
Large	$4,661,535	
Direct Download (DDL) Host Sites		
Small	$401,087	
Medium	$1,281,344	
Large	$3,084,123	

Table 1: Q3 Aggregate Ad Revenue, Margin for Ad-Supported Sites

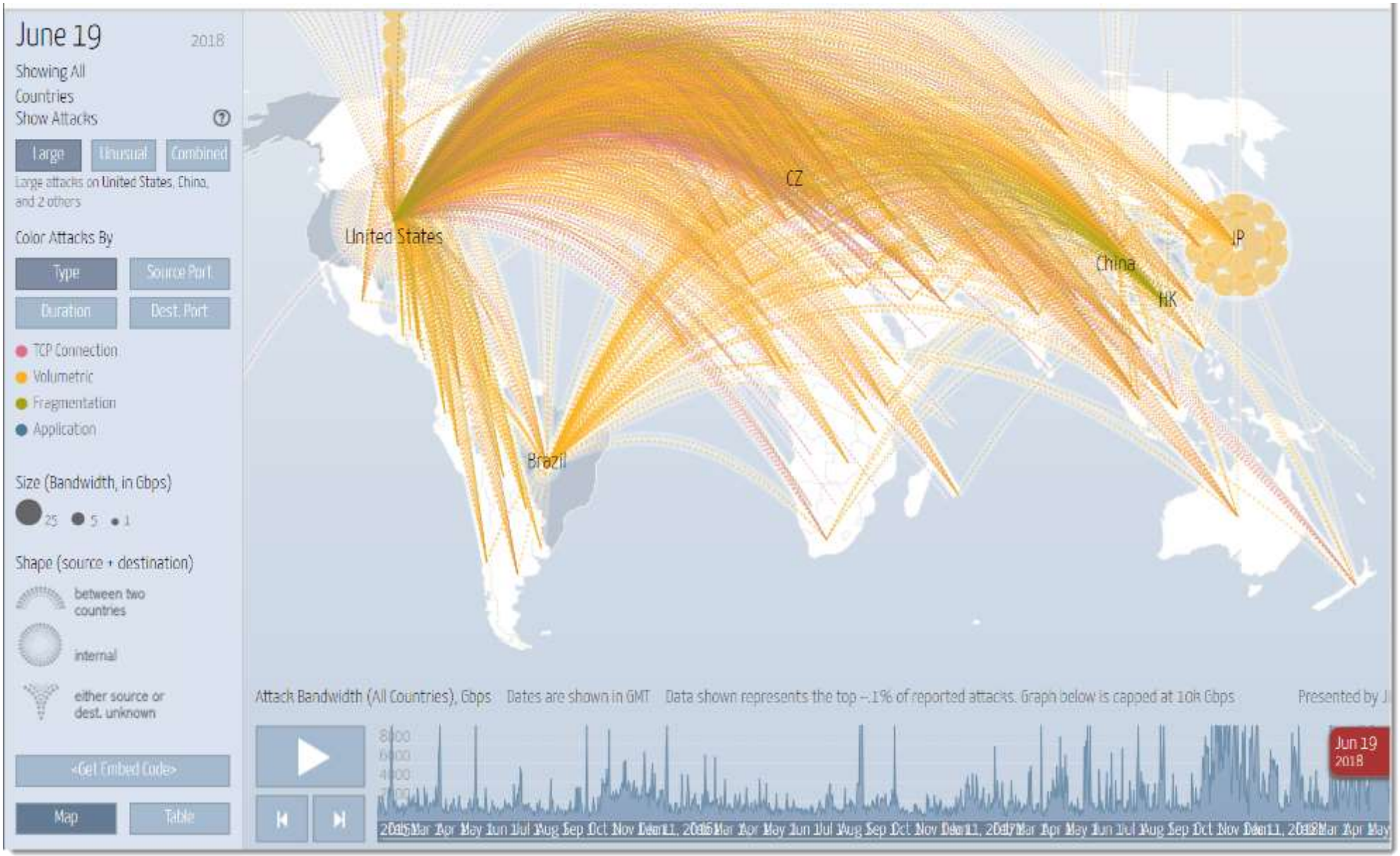
"Highly Lucrative, Profitable
The aggregate ad revenue for the sample of 596 sites was an estimated $56.7 million for Q3 of 2013, projecting out to **$226.7 million dollars annually**, with average profit margins of 83%, ranging from 80% to as high as 94%."

Source: Digital Citizens Alliance Study

https://thetrichordist.com/2013/01/28/over-50-major-brands-supporting-music-piracy-its-big-business/

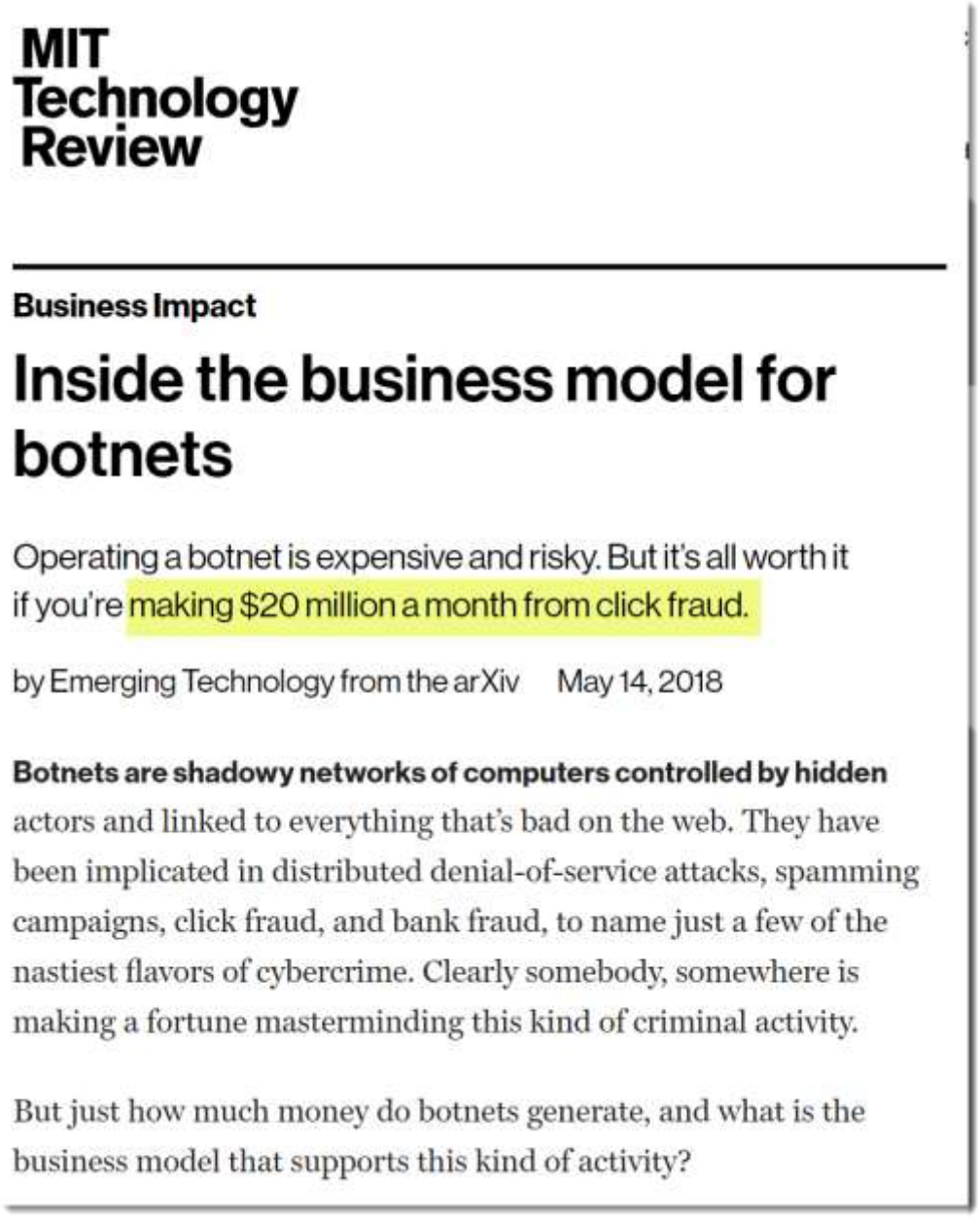
DDoS traffic for ad revenue

DDoS attacks overwhelm with traffic; now use traffic to make ad revenue



[Google Digital Attack Map]

Economics of botnets explained



MIT Technology Review

Business Impact

Inside the business model for botnets

Operating a botnet is expensive and risky. But it's all worth it if you're making $20 million a month from click fraud.

by Emerging Technology from the arXiv May 14, 2018

Botnets are shadowy networks of computers controlled by hidden actors and linked to everything that's bad on the web. They have been implicated in distributed denial-of-service attacks, spamming campaigns, click fraud, and bank fraud, to name just a few of the nastiest flavors of cybercrime. Clearly somebody, somewhere is making a fortune masterminding this kind of criminal activity.

But just how much money do botnets generate, and what is the business model that supports this kind of activity?

Source: MIT Tech Review, May 2018

Botnets can be used for a variety of things

"distributed denial-of-service attacks using a network of 30,000 bots can generate around $26,000 a month. Spam advertising with 10,000 bots generates around $300,000 a month, and bank fraud with 30,000 bots can generate over $18 million per month. ***But the most profitable undertaking is click fraud, which generates well over $20 million a month of profit****."*

Insane profits from ad fraud

Sample Campaign 1

- Amount spent to buy traffic – $183,000
- Traffic purchased – 37 million pageviews ($4.99 CPM)
- Clicks successfully sold – 3.8 million **(passed all fraud filters)**
- CPC earned $1.20, at 10% click through rate

$4.6 million payout

25X return

$15.9 billion
annualized fraud

Sample Campaign 2

- Amount spent to buy traffic – $24,000
- Traffic purchased – 23 million pageviews ($1.03 CPM)
- Clicks successfully sold – 2.5 million **(passed all fraud filters)**
- CPC earned $0.39, at 11% click through rate

$982k payout

41X return

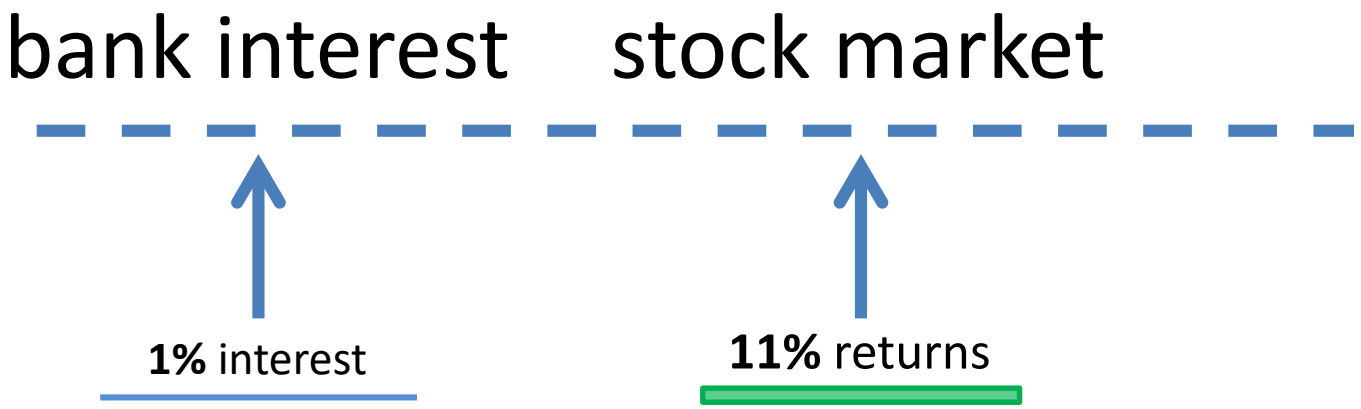
$5.5 billion
annualized fraud

The most profitable criminal activity

digital ad fraud

2,500 - 4,100% returns

"where else can I get multi-thousands percent returns on my money? Right. Nowhere."



Two main kinds of ad fraud

Impression Fraud

(CPM) Fraud

(includes mobile display, video ads)

Click Fraud

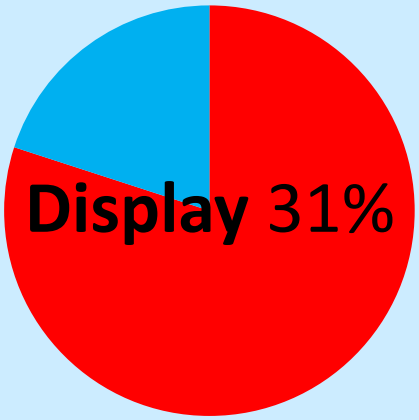
(CPC) Fraud

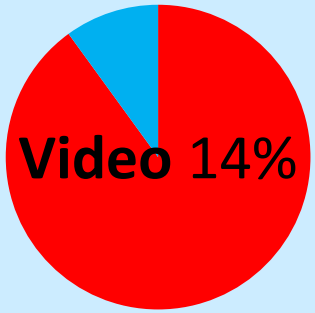
(includes mobile search ads)

*"Everything else is a **derivative of** (e.g. cost-per-install fraud), or **in support of** (e.g. tricking measurement, attribution, covering tracks) the above 2 forms of ad fraud."*

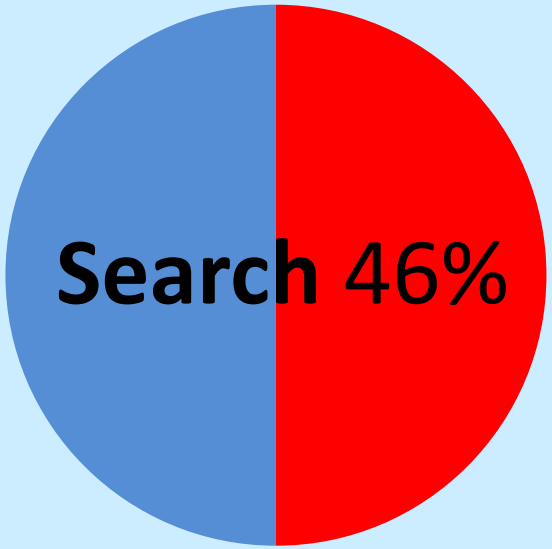
Why? Largest buckets of spend

Impressions
(CPM/CPV)



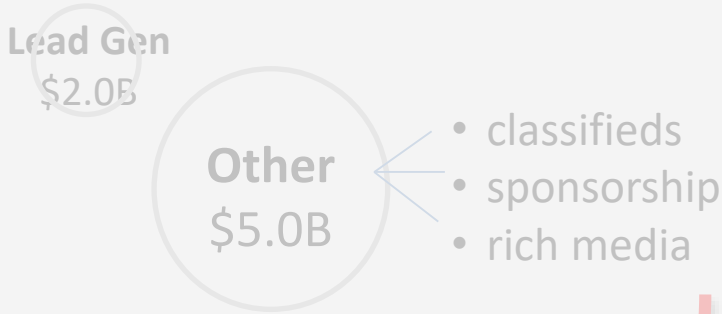


Clicks
(CPC)



Leads
(CPL)

Sales
(CPA)



9% spend

91% digital ad spend

Source: IAB **FY 2017** Report
Estimated >$300B in 2018

How Big is Ad Fraud?

Everyone has an opinion…

Ads fraud is
"non-existent"
– IAB Australia

Less than 4% of digital ads in Australia are fraudulent, claims IAB

March 2, 2017 10:03
by SIMON CANNING

…presenting Austr…
The industry…ed in a new report …ital
publishers h… …tal
advertising almost non-existent…ralia.
In a finding … …from other
parts of the w…pears to conflict …g Bureau of
Australia's first re… …claims that
more than 96% of ads …teractive…ops and mobiles are
served to real users.

"Ad fraud is $6.5 billion or 9% of display ad spend"
-- ANA/WhiteOps

"88% - 98% of clicks are generated by bots"
- Oxford Biochron

Quantifying Online Advertising Fraud:
Ad-Click Bots vs Humans

Adrian Neal, Sander Kouwenhoven

Oxford BioChronometrics SA

January 2015

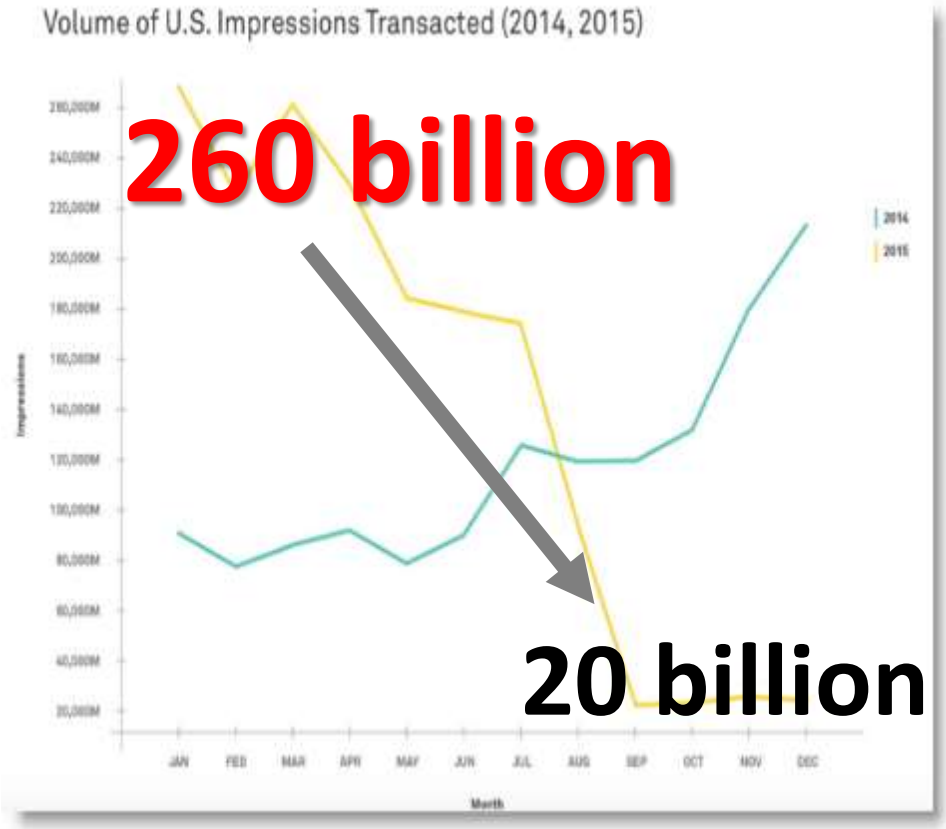
Abstract

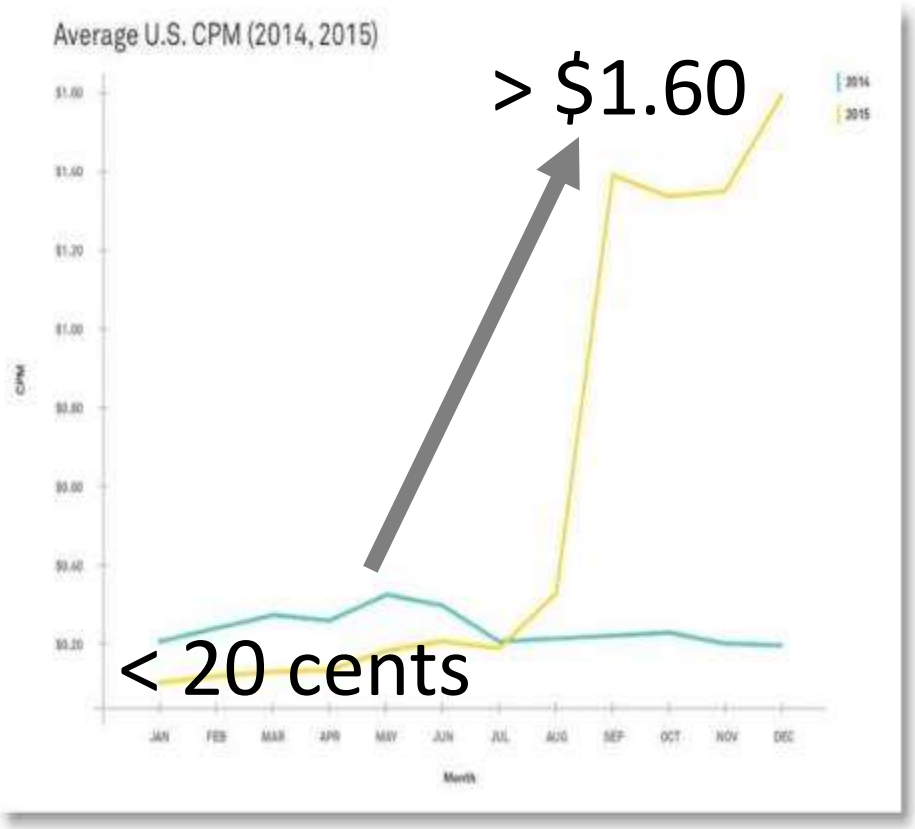
We present the results of research to determine the ratio of Ad-Clicks that are human initiated against those that are initiated by automated computer programmes, commonly known as ad-bots. The research was conducted over a 7 days period in early January 2015, using the advertising platforms of Google, Yahoo, LinkedIn and Facebook. The results showed that between 88 and 98 percent of all ad-clicks were by a bot of some kind, with over 10 per cent of these bots being of a highly advanced type, able to mimic human behaviour to an advanced extent, thus requiring highly advanced behavioural modelling to detect them.

(2015) Display ads …

Decreased impression volume **by 92%**

Increased CPM prices **by 800%**





Source: http://adexchanger.com/ad-exchange-news/6-months-after-fraud-cleanup-appnexus-shares-effect-on-its-exchange/

Methbot, Hyphbot (video fraud)

Vast botnets targeting high-value video ads, disguising/hiding

2016

*"**Methbot**, steals **$2 billion annualized;** and it avoided detection for years."*

- **Targeted video ad inventory**
  $13 average CPM, 10X higher than display ads
- **Disguised as residential**
  bots pretended to be from **residential IP addresses**

Source: Dec 2016 WhiteOps Discloses Methbot Research

2017

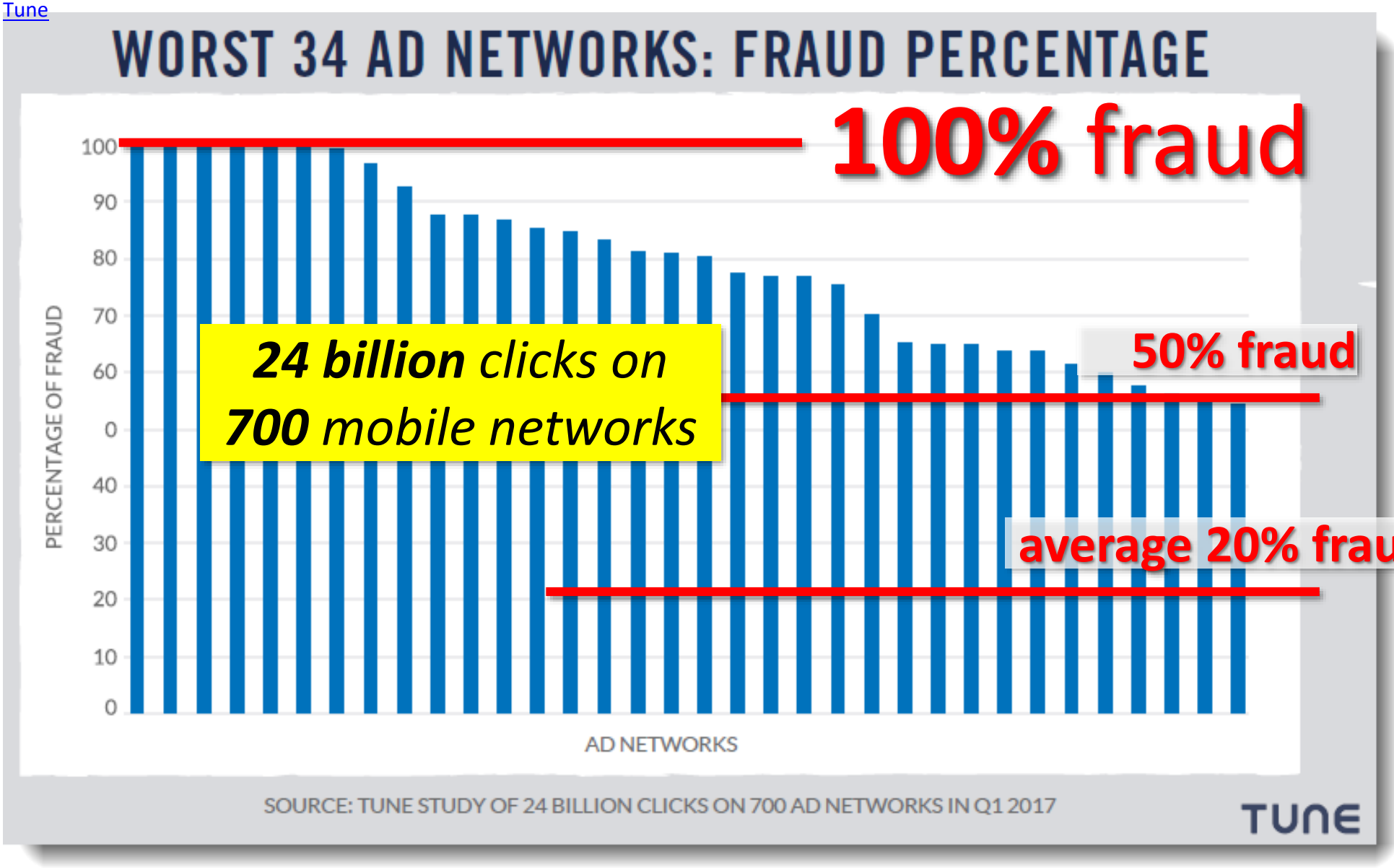
*"**Hyphbot**, targeted video ad inventory avoided detection."*

- active through at least 14 different exchanges and SSPs
- generating up to **1.5 billion requests per day**
- generated fake traffic on more than **34,000 different domains, 600k IP addresses**

Source: Adform, Nov 2017

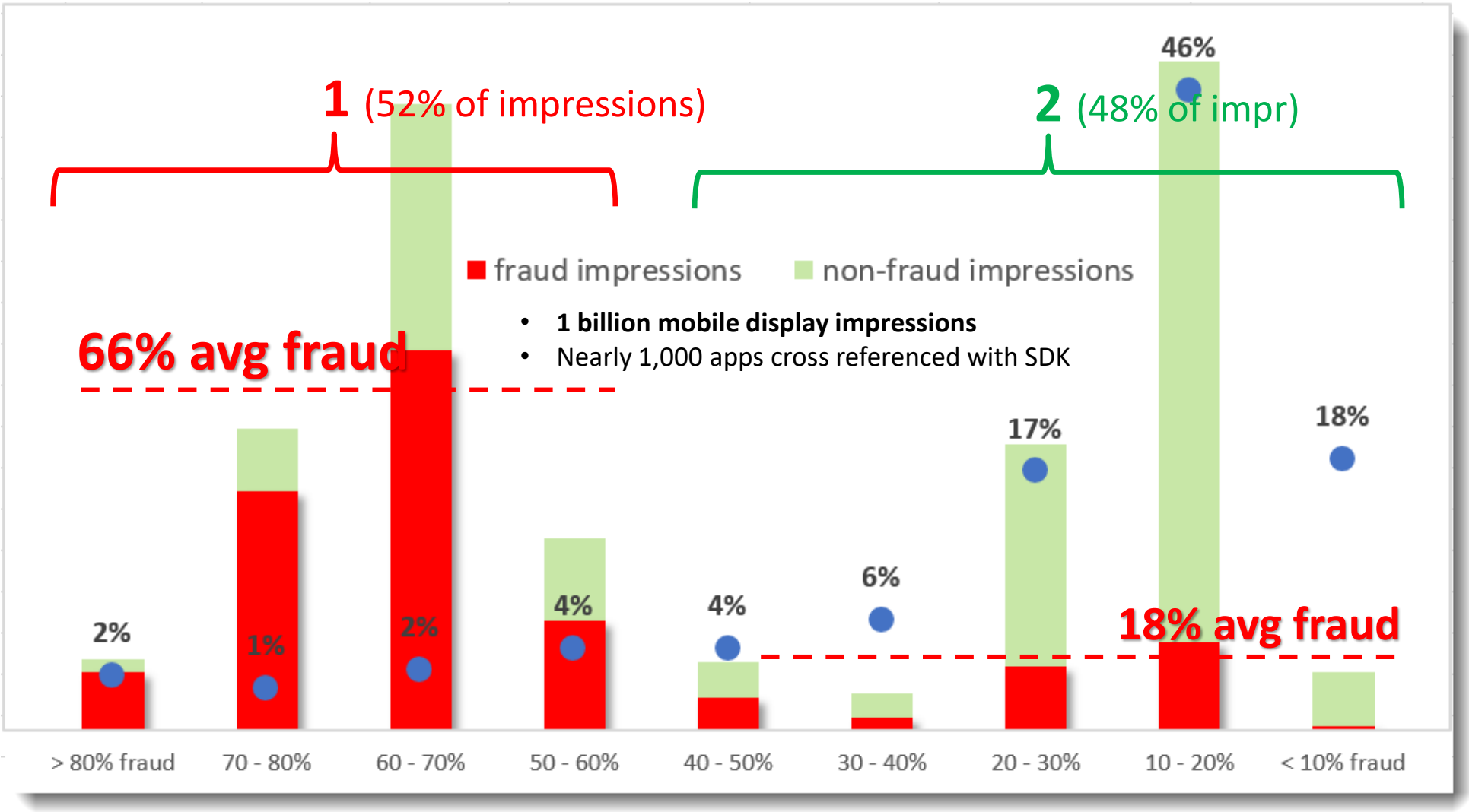
(2017) Mobile app install fraud

Source: October 2018, Tune



(2017) Handful of bad apps

1. **9% of the apps caused 52% of impressions; 66% outright fraud**
2. Remaining 91% of apps caused 48% of impressions, 18% outright fraud



Source: https://www.slideshare.net/augustinefou/mobile-display-fraud-case-study

Fake devices pass fake location

Houston, TX

Percent	HTTP_X_REQUESTED_WITH
38.2%	com.ji
20.6%	com.jl
19.7%	com.jl
11.4%	com.g
4.6%	com.jl
1.2%	com.jl
0.9%	mac.r
0.7%	com.a
0.6%	com.jl
0.5%	com.ji

percentage	
Houston	79.30%
Katy	3.91%
Spring	3.45%
Smithville	2.66%
Austin	2.36%
Cypress	2.32%
Pasadena	1.86%
Humble	1.62%
Pearland	1.47%
Missouri City	1.05%

Bozeman, MT

Percent	HTTP_X_REQUESTED_WITH
22.9%	com.g
19.2%	com.j
14%	com.j
9.2%	mac.r
7.4%	com.s
6.3%	com.l
5.9%	com.j
5.3%	com.j
4%	com.j
1.5%	com.j

percentage	
Bozeman	42.41%
Butte	17.67%
Anaconda	13.09%
Billings Metropolitan	8.25%
Belgrade	6.41%
Dillon	5.76%
West Yellowstone	2.62%
Missoula	1.57%
Townsend	1.57%
Columbus	0.65%

Fake devices declare fake locations to absorb higher ad spend

(2017) Mobile display ad fraud

"Judy Malware"

- **40 bad apps** to load ads
- **36 million fake devices** to load bad apps that load display ads
- e.g. 30 ads per device /minute
- 30 ads per minute = **1 billion fraud impressions per minute**

"Fireball Malware"

- **250 million** infected computers
- primary use = traffic for ad fraud
- 4 ads /pageview (2s load time)
- fraudulent impressions at the rate of **30 billion per minute**

Source: Forbes, May 2017

Forbes / Security / #CyberSecurity

MAY 16, 2017 @ 10:55 AM 179,527

The Little Black Book of Billions

Google Just Killed What Might Be The Biggest Android Ad Fraud Ever

Thomas Fox-Brewster, FORBES STAFF

FULL BIO

Google has thrown more than 40 apps out of its Play store after it emerged they were quietly forcing Android users to click on ads. As the apps been downloaded as many as 36 million times, security researchers said it appeared to be the biggest ever case of ad fraud perpetrated via Google Play and probably the most successful malware in terms of installs from the official store.

Security firm Check Point revealed the campaign

Source: Checkpoint

Check Point

Home » Company » Check Point Blog » Threat Research » FIREBALL – The Chinese Malware of 250 Million Computers Infected

FIREBALL – The Chinese Malware of 250 Million Computers Infected

by Check Point Threat Intelligence Research Team posted 2017/06/01

Check Point Threat Intelligence and research teams recently discovered a high volume Chinese threat operation which has infected over 250 million computers worldwide. The installed malware, Fireball, takes over target browsers and turns them into zombies. Fireball has two main functionalities: the ability of running any code on victim computers–downloading any file or malware, and hijacking and manipulating infected users' web-traffic to generate ad-revenue. Currently, Fireball installs plug-ins and additional configurations to boost its advertisements, but just as easily it can turn into a prominent distributor for any additional malware.

(2018) Mobile app spoofing

BuzzFeed News

REPORTING TO YOU

TRENDING Pittsburgh Synagogue Shooting Soros Conspiracy Theories Pipe Bomb Scare

Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme

A BuzzFeed News investigation uncovered a sophisticated ad fraud scheme involving more than 125 Android apps and websites, some of which were targeted at kids.

Craig Silverman
BuzzFeed News Reporter

Posted on October 23, 2018, at 1:07 p.m. ET

Last April, Steven Schoen received an email from someone named Natalie Andrea who said she worked for a company called We Purchase Apps. She wanted to buy his Android app, Emoji Switcher. But right away, something seemed off.

"I did a little bit of digging because I was a little sketched out because I couldn't really find even that the company existed," Schoen told BuzzFeed News.

Source: [Buzzfeed News, Oct 2018]

The scheme reportedly involved 125 Android apps and websites. … the fraudsters buy legitimate Android apps with an established reputation and then … **blend bot- and human-generated traffic** to evade ad-fraud detection.

The **TechSnab malware is usually bundled with free, third-party apps** and is installed as a browser extension. Users would discover an infection if they see pop-ups, pop-unders and various other ads marked 'TechSnab'.

[Google] "confirmed the traffic from the apps "seems to be a blend of organic user traffic and artificially inflated ad traffic, including **traffic based on hidden ads**".

One example was an Android app called MegaCast, which was **found to be displaying the unique ID of others apps** to attract bids for ads.

(2015) Apps doing ad fraud

BUSINESS INSIDER

There are thousands of legitimate-looking apps in the Apple, Android, and Windows Phone app stores running a harmful type of ad fraud

Lara O'Reilly
Jul. 23, 2015, 9:00 AM 7,006

FACEBOOK LINKEDIN TWITTER

Researchers have discovered that thousands of apps in the app stores for Apple, Android, and Windows Phone are running a highly sophisticated and potentially harmful form of advertising fraud.

Forensiq predicts more than $1 billion in ad money could be wasted on in-app fraud by the end of this year.
FlickrCC/Christopher

Fraud detection company Forensiq claims in a report to have discovered a new type of ad fraud called "mobile device hijacking." A user downloads an app from the official app store — which may look legitimate and have hundreds of positive reviews — which then runs in the background, serving hundreds of ads at a rate as high as 20 ads per minute (most normal apps with ads in would only refresh an ad every 30 to 120-seconds.)

Known and documented for years – now mobile is majority of digital spend

"A user downloads an app from the official app store — which may look legitimate and have hundreds of positive reviews — which then **runs in the background, serving hundreds of ads** at a rate as high as 20 ads per minute"

Source: BusinessInsider, July 2015

Impressions offered (30 days)

	App/URL	Potential Impressions	Unique Cookies with Impressions	Potential Viewable Impressions
2	howstuffworks.com	13,331,755,008	37,539,240	4,652,153,856
3	Super-Bright LED Flashlight - Android (com.surpax.ledflashl	12,843,444,224	16,831,854	70,800,208
4	msn.com	9,140,699,136	9,998,644	3,960,017,920
5	dailymail.co.uk	8,998,725,632	14,726,014	1,593,495,680
6	xfinity.com	7,189,870,592	3,388,972	749,400,512
7	weather.com	6,685,053,952	10,182,312	23,404,652
8	GO Music Player PLUS - Android (com.jb.go.musicplayer.m	3,747,614,976	8,019,603	410,346
9	ranker.com	3,601,194,240	10,647,463	768,604,544
10	twentytwowords.com	3,501,990,400	3,342,428	907,051,264
11	m.ranker.com	3,233,506,048	8,696,249	631,613,824
12	Allrecipes Dinner Spinner - iOS (299515267)	3,093,926,400	2,806,602	231,658,128
13	S Photo Editor - Collage Maker - Android (com.steam.phot	2,897,		
14	screenrant.com	2,846,		
15	GO Keyboard - Emoji, Sticker - Android (com.jb.emoji.goke	2,649,		
16	drudgereport.com	2,354,		
17	boredomtherapy.com	2,277,		
18	people.com	2,138,		
19	allrecipes.com	2,089,		
20	accuweather.com	2,026,		
21	cnn.com	1,789,104,512	5,364,446	90,731,944
22	delish.com	1,261,016,704	3,560,009	23,222,630
23	TouchPal Emoji Keyboard - Android (com.emoji.keyboard.t	1,240,049,920	2,577,664	434,277
24	livestrong.com	1,183,711,360	2,667,744	213,508,592
25	Z Camera - Android (com.jb.zcamera)	1,117,740,544	2,953,365	356,455
26	goodhousekeeping.com	1,056,157,056	2,494,773	26,681,034
27	babygaga.com	1,050,812,992	1,015,785	196,136,800
28	buzznet.com	1,028,773,632	736,622	123,564,104
29	GO Music - Free Music, Equalizer, Themes - Android (com.	969,776,000	1,688,335	191,230
30	GO Launcher -Theme & Wallpaper - Android (com.gau.go.l	937,814,080	741,907	6,112,380
31	harpersbazaar.com	934,447,552	1,310,800	22,075,248
32	AppLock Pro - Privacy & Vault - Android (com.jiubang.alock	907,721,792	477,495	87,446
33	looper.com	900,943,680	3,291,817	144,069,184
34	Allrecipes Dinner Spinner - Android (com.allrecipes.spinner	786,078,976	1,668,915	33,476,448
35	thetalko.com	774,521,856	849,115	135,095,680
36	marieclaire.com	717,790,080	868,778	17,335,820
37	countryliving.com	662,211,584	2,017,750	17,131,218
38	cosmopolitan.com	603,556,416	2,118,915	20,746,424
39	rollingstone.com	590,455,936	3,373,262	54,689,056
40	elle.com	580,703,744	1,260,547	13,573,076

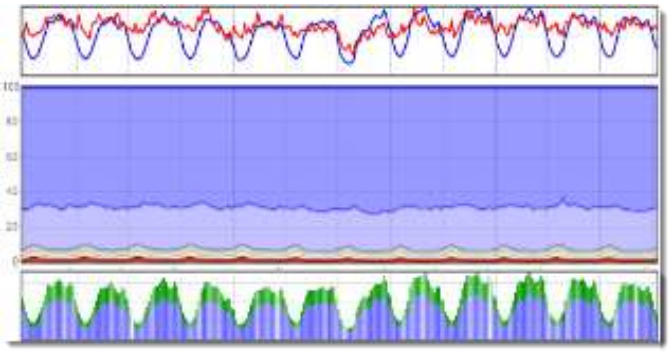
There's **160X** more "sites with ads"

(outside Google/Facebook)

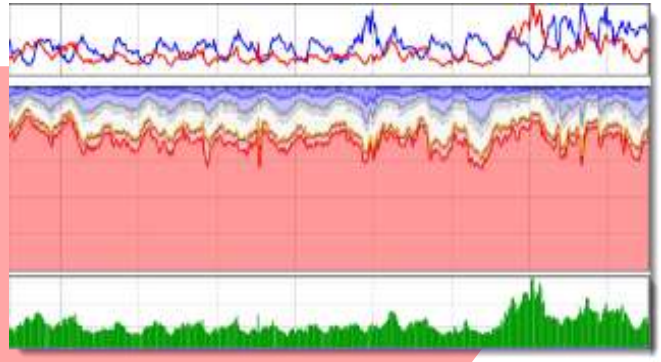
$23

78%
programmatic

Good Publishers



"sites with ads"



160X more

no ads

329M
Source: Verisign, Q4 2016
domains

carry ads

est. 1 million

"sites you've heard of"

WSJ Economist
ESPN Reuters
NYTimes Elle

0.3%

est. 164 million

"sites that carry ads"

000au000.com
000auction000.com
000audio000.com
000augusta000.com
000aurora000.com
000aus000.com
000austin000.com
000autoglass000.com
000autoinsurance000.com
000automobile000.com
000automotive000.com
000autoparts000.com
000autorenting000.com
000autorepair000.com

There's **700X** more fake apps

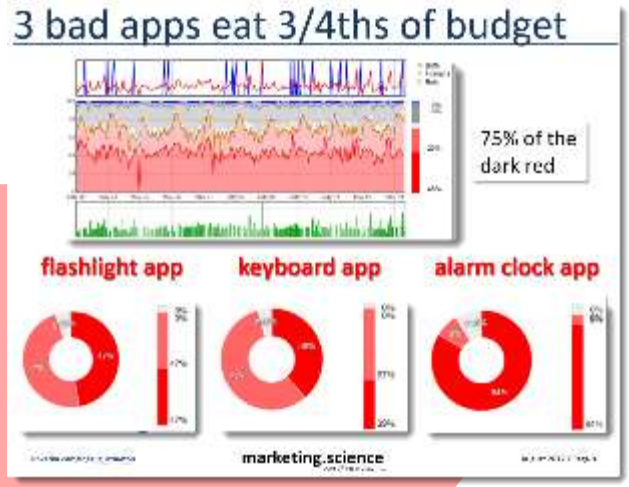
Facebook, 2015
Users use 8 – 15 apps on their phones.

Spotify, 2016
People have 25 apps on their phones, use 5-8 regularly

Forrester Research, May 2017
Humans "use 9 apps per day, 30 per month"

(outside Google/Facebook)
$23

78%
programmatic



7M
Source: Statista, March 2017
apps

700X more

10,000
"apps you've heard of"

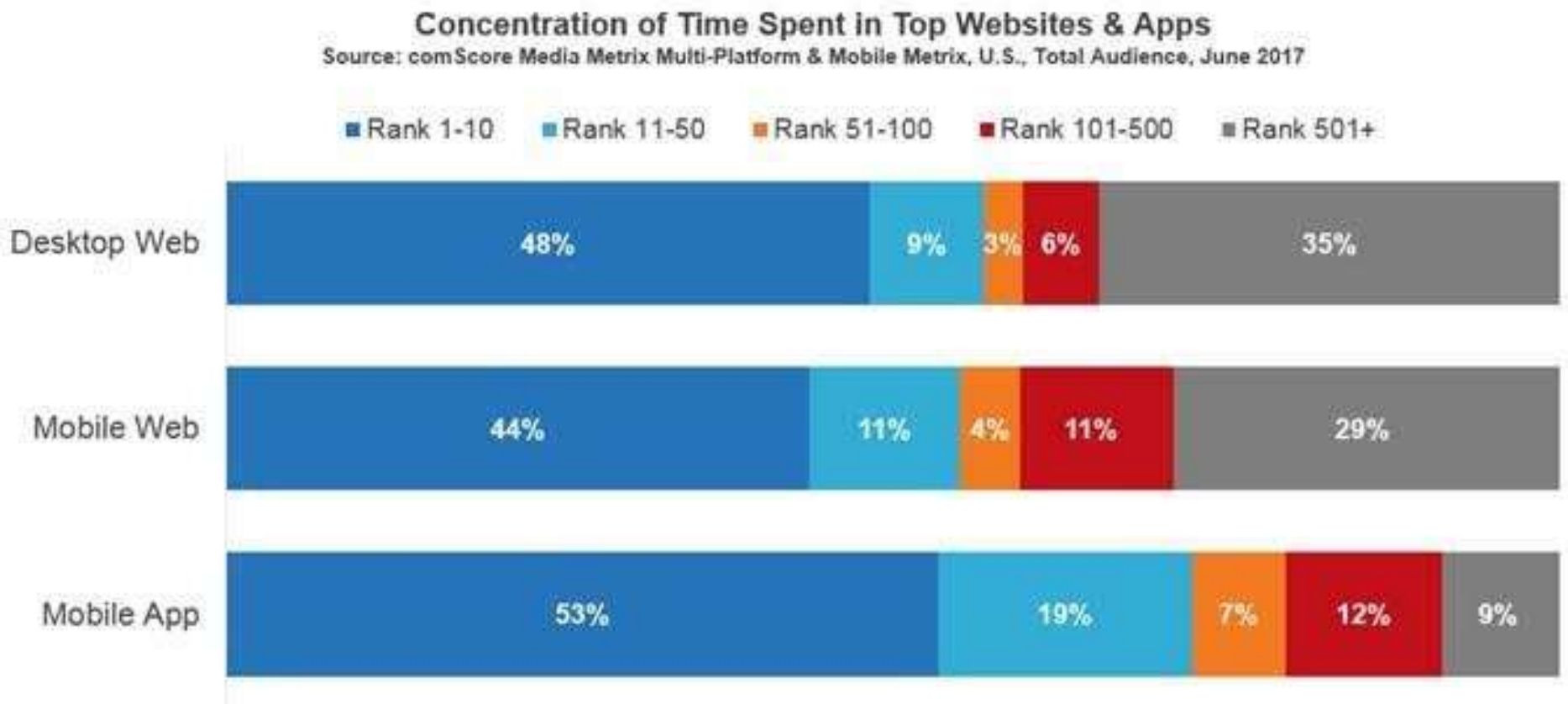
Facebook Zynga
Spotify Pokemon
Pandora YouTube

6.99 million
96% "apps that carry ads"

biz.western.dad.smooth.development
info.fence.everywhere.cry.cry
org.wore.favorite.whatever
ua.tool.muscle.fourth.muscle.desk
biz.win.model.likely.sad.flight
com.ann.clock.hung.immediately.handle

Myth of the long tail of sites

Most people visit sites they know most; occasionally long tail ones



"There are numerous pieces of research on how even as people accumulate hundreds of TV channels, ***they only watch seven****. It's rather commonly accepted that in a sea of millions of mobile apps, most people stick to* ***half a dozen."***

http://www.businessinsider.com/the-advertising-industry-has-been-living-a-lie-2017-10

Real billboards vs digital ads

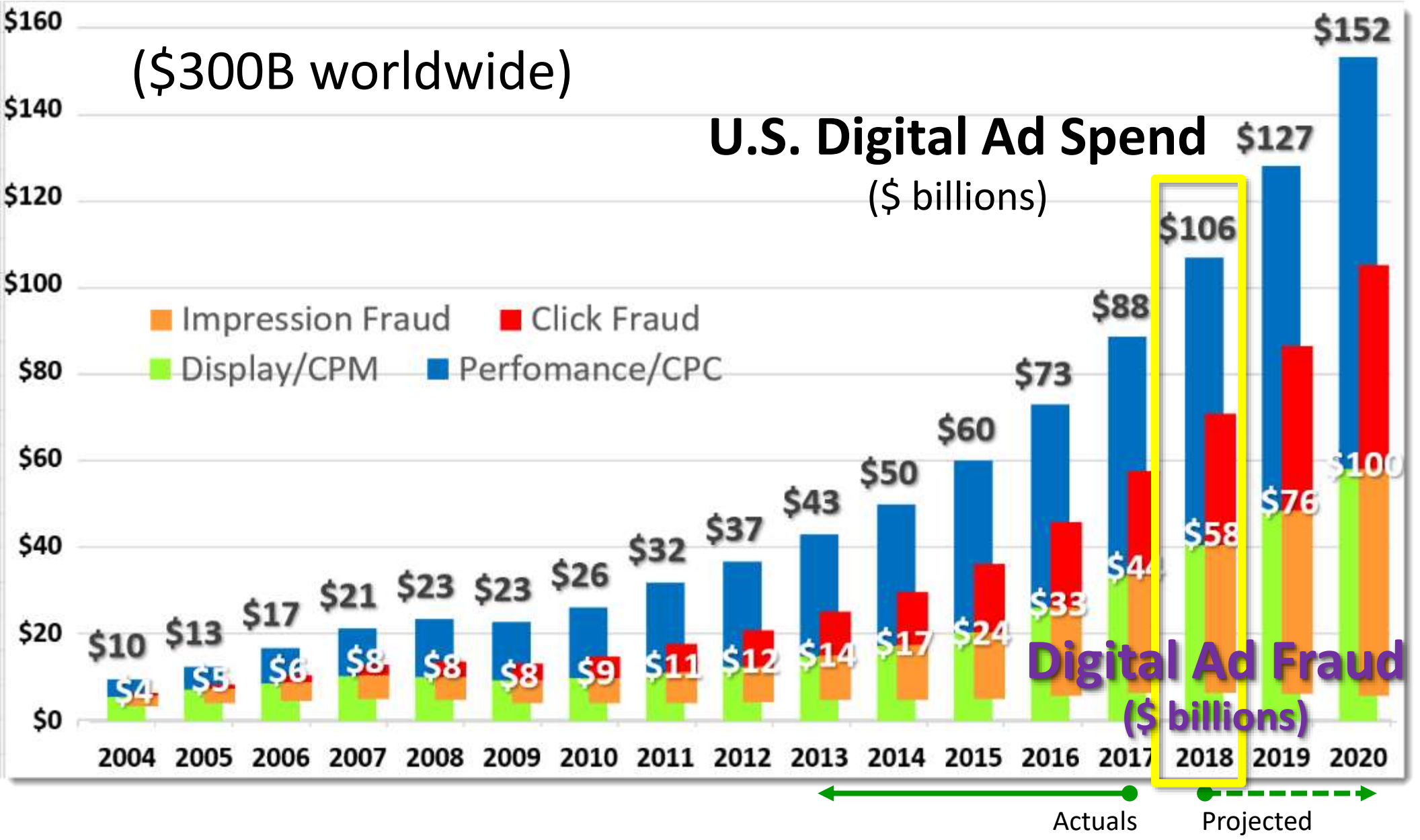
Infinite quantities of digital ads can be created on real or fake sites

Unlike real billboards that people actually drive by in the physical world …

Limitless quantities of digital ads can be created on fake sites that humans never visit.

Ad fraud is at all-time highs

There's $100B in digital ad spend to steal from, year after year



10 – 90

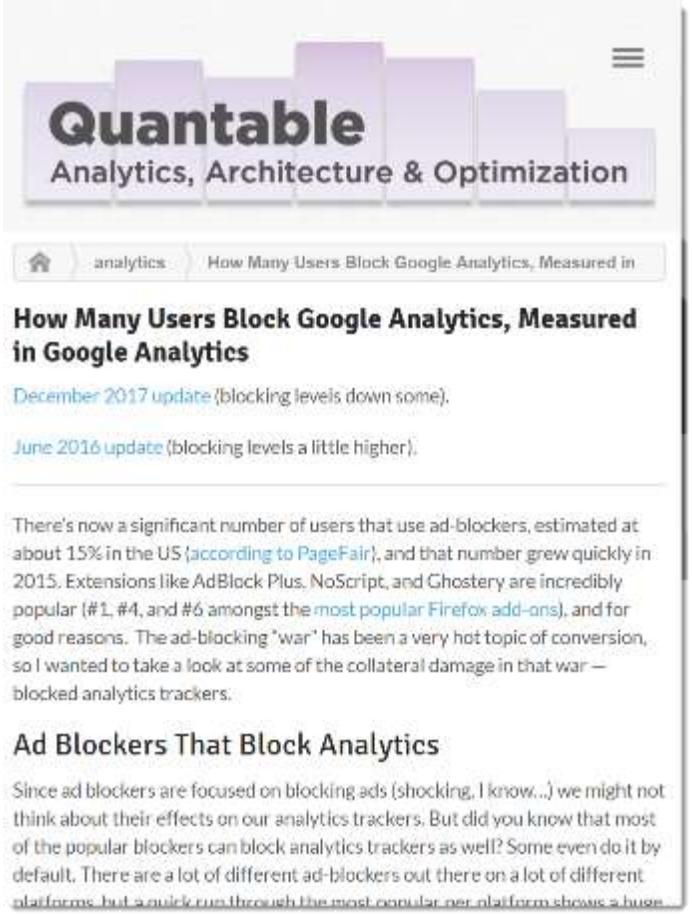
1 - 99

Why isn’t it detected?

Bad guys easily avoid detection

Blocking of tags, altering measurement to avoid detection

Detection Tag Blocking — analytics tags/fraud detection tags are accidentally blocked or maliciously stripped out



Quantable
Analytics, Architecture & Optimization

analytics | How Many Users Block Google Analytics, Measured in

How Many Users Block Google Analytics, Measured in Google Analytics

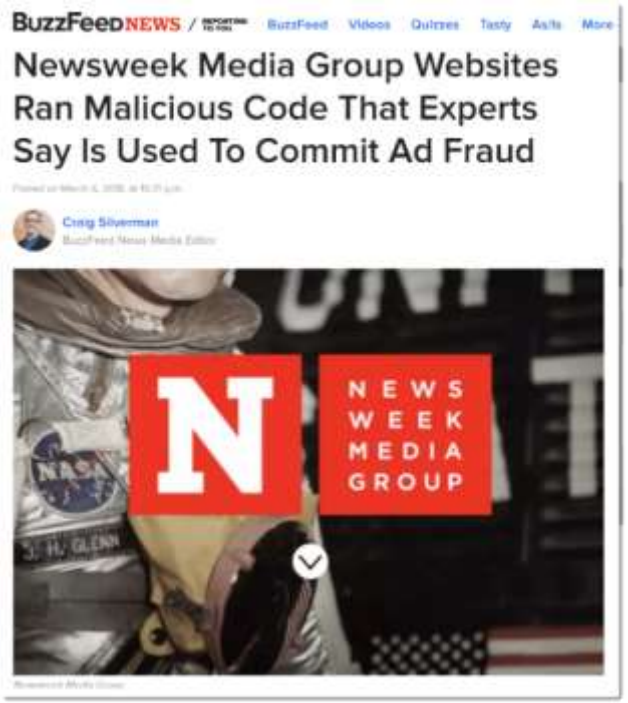
December 2017 update (blocking levels down some).

June 2016 update (blocking levels a little higher).

There's now a significant number of users that use ad-blockers, estimated at about 15% in the US (according to PageFair), and that number grew quickly in 2015. Extensions like AdBlock Plus, NoScript, and Ghostery are incredibly popular (#1, #4, and #6 amongst the most popular Firefox add-ons), and for good reasons. The ad-blocking "war" has been a very hot topic of conversion, so I wanted to take a look at some of the collateral damage in that war — blocked analytics trackers.

Ad Blockers That Block Analytics

Since ad blockers are focused on blocking ads (shocking, I know...) we might not think about their effects on our analytics trackers. But did you know that most of the popular blockers can block analytics trackers as well? Some even do it by default. There are a lot of different ad-blockers out there on a lot of different platforms, but a quick run through the most popular per platform shows a huge



BuzzFeed NEWS

Newsweek Media Group Websites Ran Malicious Code That Experts Say Is Used To Commit Ad Fraud

Craig Silverman

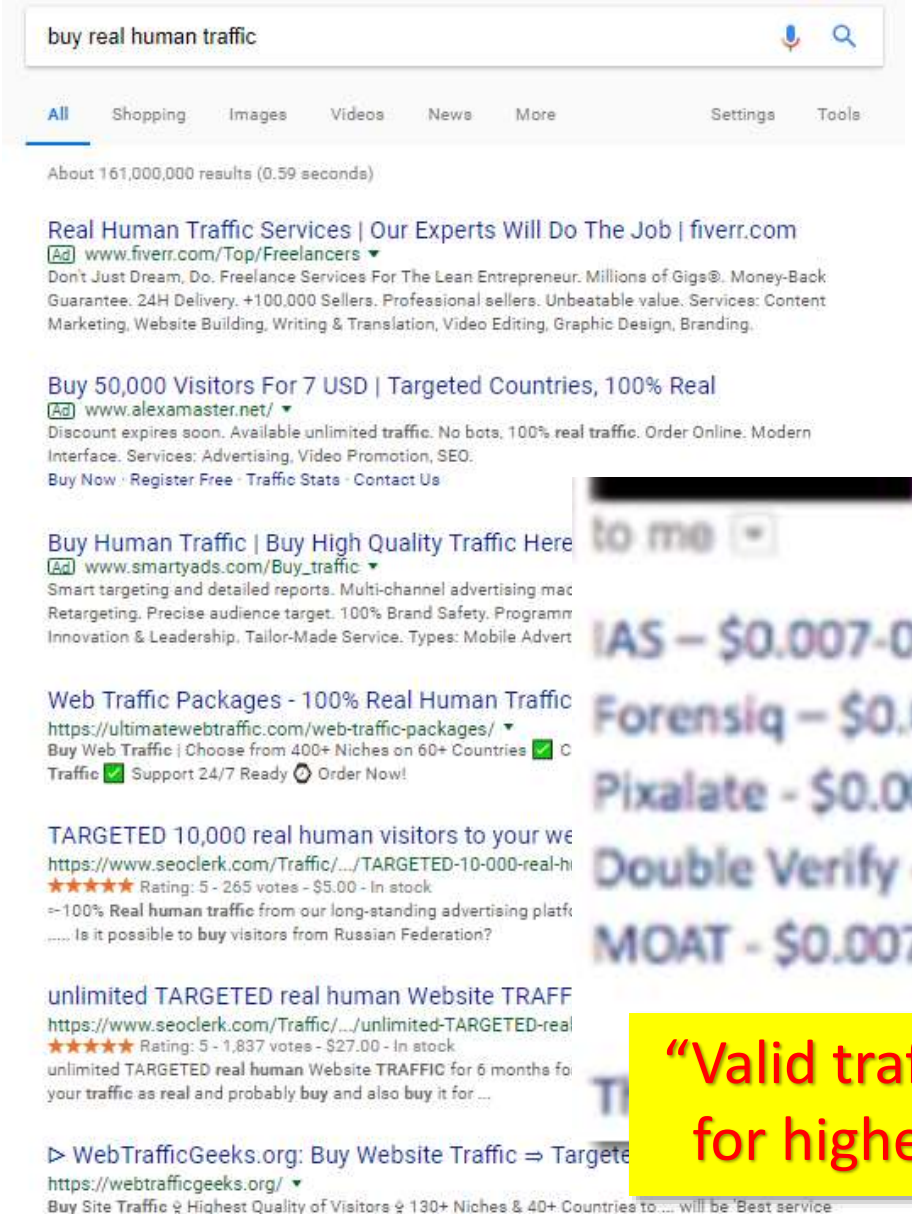
NEWS WEEK MEDIA GROUP

"malicious code **manipulated data** to ensure that otherwise unviewable ads showed up in measurement systems as valid impressions, which resulted in payment being made for the ad."

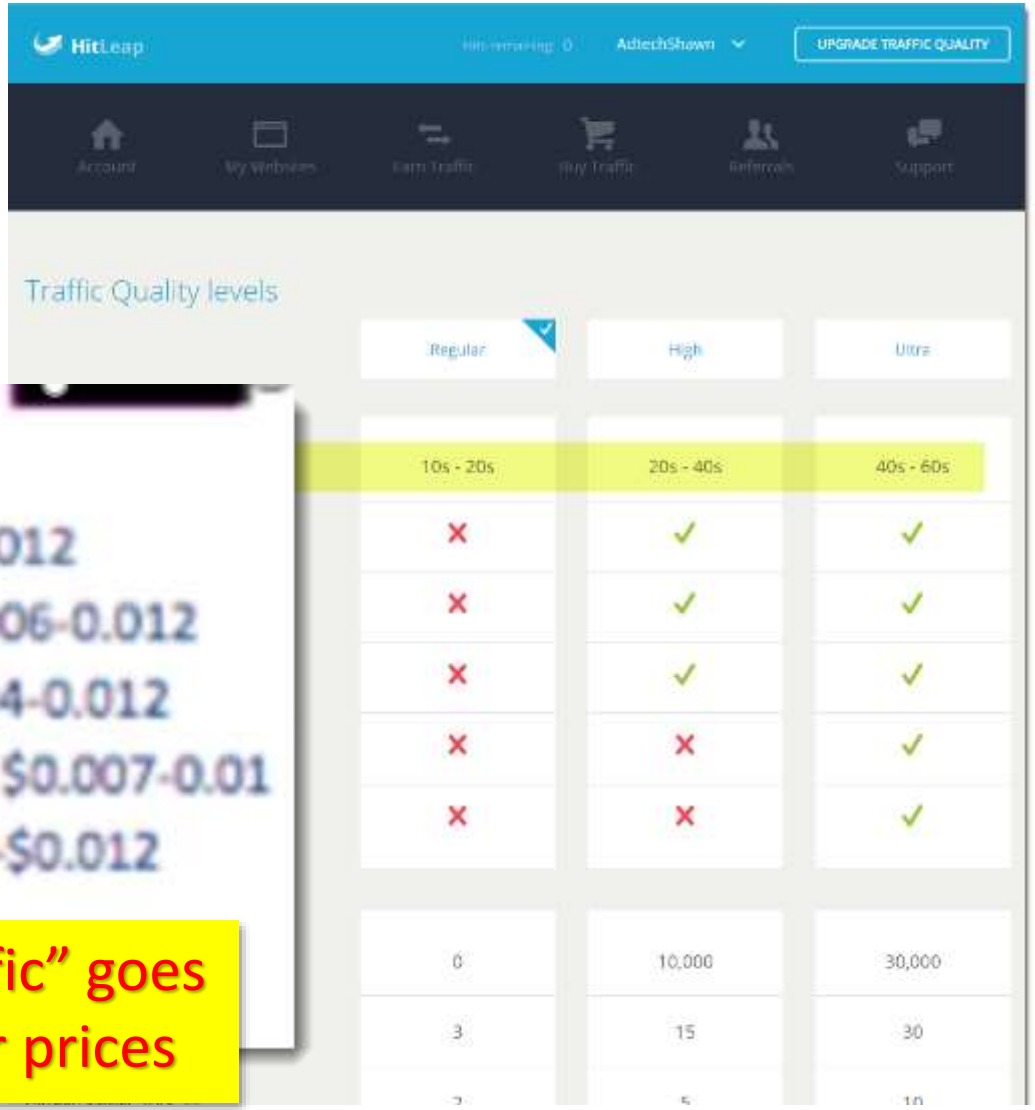
Source: Buzzfeed, March 2018

Traffic sellers' "high quality traffic"

Many sources to buy "traffic" and even tune "quality" level

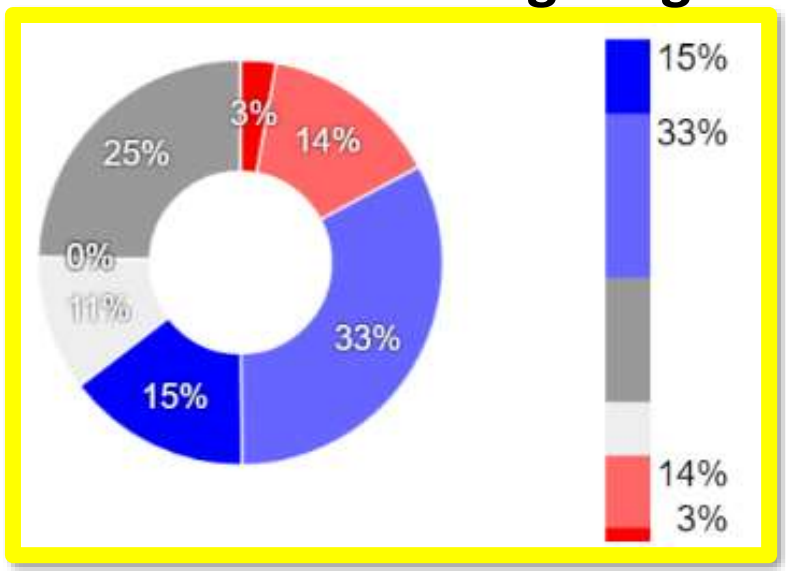


Choose Your "Traffic Quality Level"

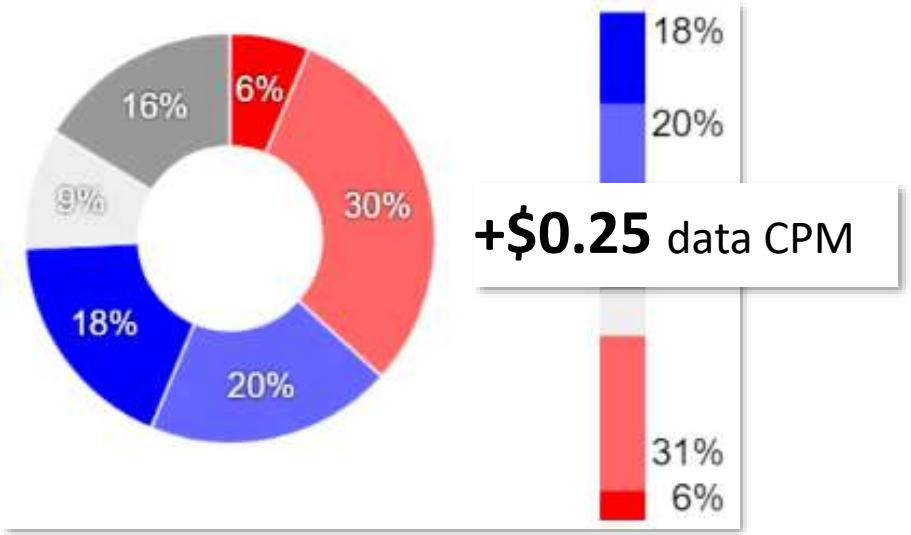


“Verified” no different than control

Control: No Targeting

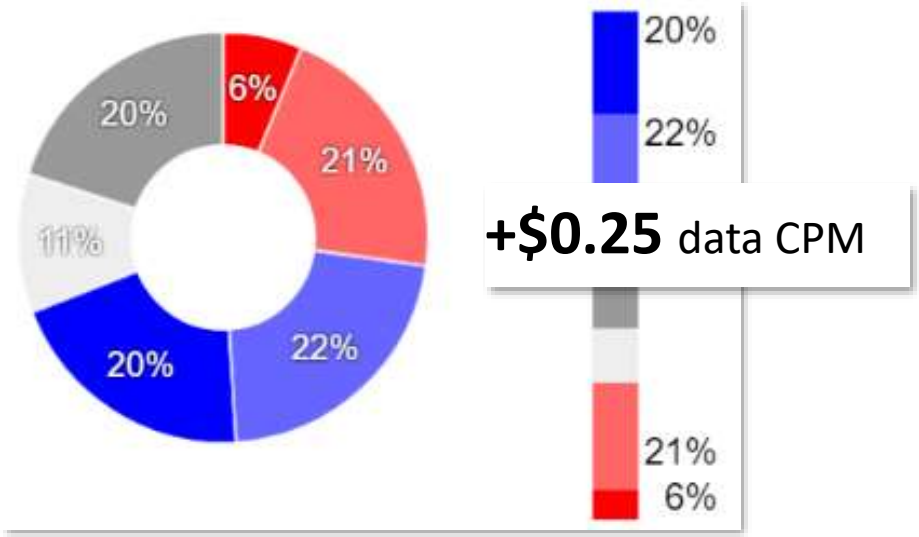


“Verified Bots”



+$0.25 data CPM

“Verified Humans”



+$0.25 data CPM

“verified bots” and “verified humans” showed no difference in quality to each other – AND both were **no different than the control where no targeting was used.**

They miss obvious botnets

Bots repeatedly loading ads and pages, 100% Android devices

Devices repeatedly load ads

Percent	Count	
2.5%	1000	d65dd04791dd2280bbbabdfada82f97b
1.5%	600	04fa879a518e246fef969d00036d4d14
1%	400	24ad77e19a9f4237f18fec203dfff0b2
1%	400	2dc45da50b08f3db7aeb1d0c20b031eb
1%	400	306c4302c342c7ab61eeef24eb28b319
1%	400	3951a18a64fc98e9c4a022b3f076091e
1%	400	4802ad3326f1163b7ddc68612ef2a67f
1%	400	a51cb46830687aac3dae78e43a40abf5
1%	400	ef2e2579db8812cfad27892749ea3d24
0.5%	200	0081a6d3e98a07124299c857d8048f00
0.5%	200	01dfcfd48b24db669861a2803d2a0136
0.5%	200	02b35a8c67beec1db6f670e5620cfaa9
0.5%	200	0356e61a33d6db997a665f450954934b
0.5%	200	041051869c2b525edf7087483678b227
0.5%	200	0598231c2d4aaf9135378459bc2b9781
0.5%	200	06021693af6b56b6464de20ed98aae36
0.5%	200	0637bf99a6b9c64cf301b9e7e8e666c2
0.5%	200	06493db32a544c6892544e98ef09b4df
0.5%	200	0d3da4e0ba74b9614e910f2bdad56fa6
0.5%	200	121ff80785daf933edf73d02d990b30b

100% Android 8.0.0 visitors

Percent	HTTP_USER_AGENT
13.1%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G950U Build/R16NW) AppleWebKit/537.36.
10.1%	Mozilla/5.0 (Linux; Android 8.0.0; SM-N950U Build/R16NW) AppleWebKit/537.36.
9.7%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G955U Build/R16NW) AppleWebKit/537.36.
8.7%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G960U Build/R16NW) AppleWebKit/537.36.
8.6%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G965U Build/R16NW) AppleWebKit/537.36.
3.4%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G930V Build/R16NW) AppleWebKit/537.36.
1.9%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935V Build/R16NW) AppleWebKit/537.36.
1.3%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G930T Build/R16NW) AppleWebKit/537.36.
1.2%	Mozilla/5.0 (Linux; Android 8.0.0; SAMSUNG-SM-G935A Build/R16NW) AppleW..
1.1%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G892A Build/R16NW) AppleWebKit/537.36.
1.1%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G950U Build/R16NW) AppleWebKit/537.36.
1.1%	Mozilla/5.0 (Linux; Android 8.0.0; XT1650 Build/OCLS27.76-69-6) AppleWebKit/...
1.1%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G960U Build/R16NW) AppleWebKit/537.36.
1.1%	Mozilla/5.0 (Linux; Android 8.0.0; SM-N950U Build/R16NW) AppleWebKit/537.36.
0.9%	Mozilla/5.0 (Linux; Android 8.0.0; SAMSUNG-SM-G891A Build/R16NW) AppleW..
0.9%	Mozilla/5.0 (Linux; Android 8.0.0; SAMSUNG-SM-G930A Build/R16NW) AppleW..
0.8%	Mozilla/5.0 (Linux; Android 8.0.0; LG-LS993 Build/OPR1.170623.032) AppleWeb..
0.8%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G950U Build/R16NW) AppleWebKit/537.36.
0.8%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G950U Build/R16NW) AppleWebKit/537.36.
0.8%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G955U Build/R16NW) AppleWebKit/537.36.
0.8%	Mozilla/5.0 (Linux; Android 8.0.0; SM-G960U Build/R16NW) AppleWebKit/537.36.

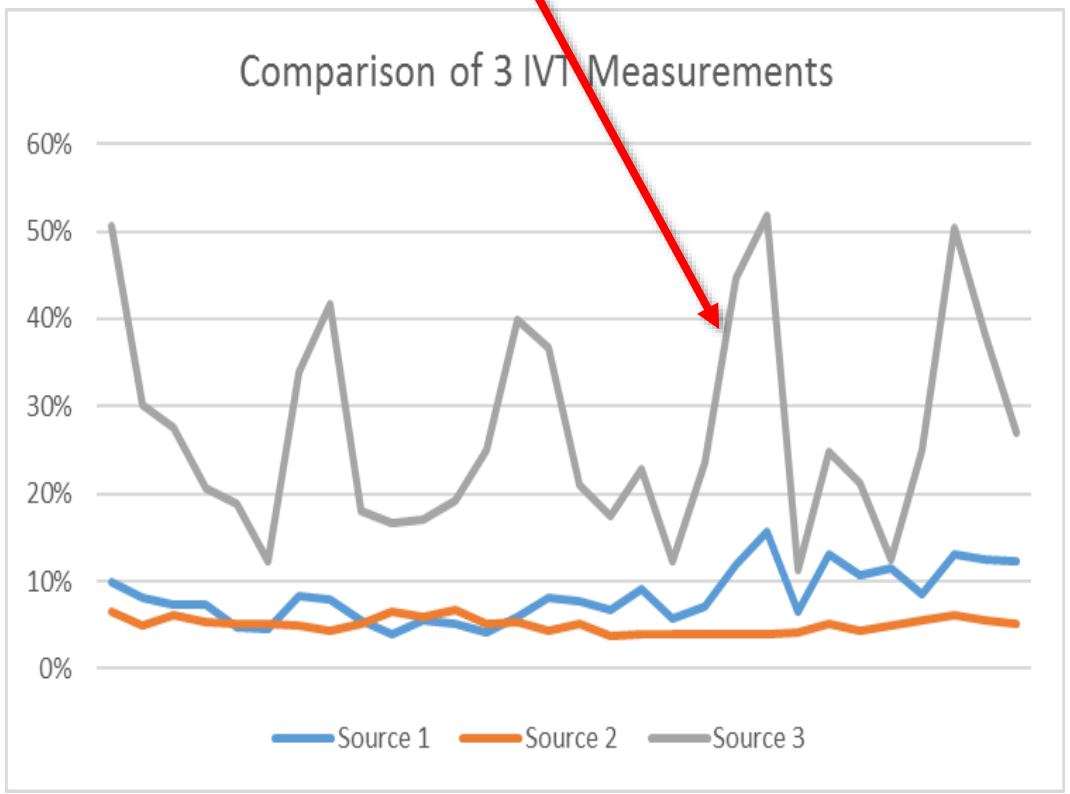
Sampling, Bad Measurement

Sampling can lead to large discrepancies and bad measurements

Date	Source 1 Data Points	Source 2 Data Points	Source 3 Data Points
7/1/2017	103,790	130,232	1,474
7/2/2017	107,568	144,841	2,179
7/3/2017	165,290	214,102	2,005
7/4/2017	192,128	243,528	2,012
7/5/2017	199,551	223,514	2,051
7/6/2017	211,443	278,472	2,414
7/7/2017	173,769	202,879	2,007
7/8/2017	128,740	159,063	1,560
7/9/2017	132,425	171,640	1,689
7/10/2017	209,714	263,933	2,420
7/11/2017	213,862	264,217	2,289
7/12/2017	221,638	274,139	2,458
7/13/2017	202,872	240,805	2,634
7/14/2017	170,528	197,712	2,141
7/15/2017	106,727	128,112	1,439
7/16/2017	118,995	157,384	1,521
7/17/2017	196,309	251,332	2,407
7/18/2017	232,390	309,020	1,877
7/19/2017	219,142	272,144	1,957
7/20/2017	203,270	253,838	1,891
7/21/2017	174,089	205,815	1,731
7/22/2017	119,673	143,404	1,231
7/23/2017	129,402	169,034	1,475
7/24/2017	209,837	272,166	2,350
7/25/2017	254,121	286,010	4,055
7/26/2017	240,000	286,274	2,042
7/27/2017	203,728	255,420	1,121
7/28/2017	176,055	196,615	1,012
7/29/2017	118,056	150,818	746
7/30/2017	128,526	171,599	686
7/31/2017	211,240	263,182	1,187
	5,474,878	6,781,244	58,061
			1 in 100

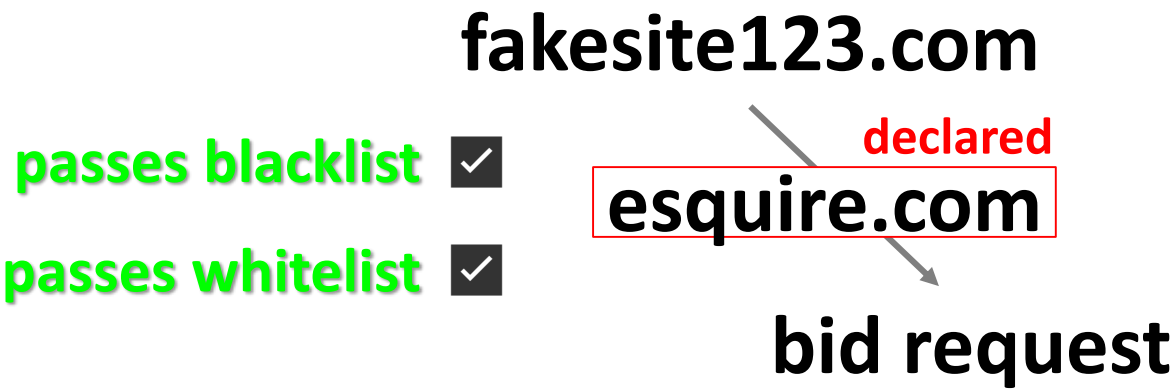
WRONG IVT Measurement

Source 3 - in ad iframe, badly sampled



Incorrect, due to sampling

Legit sites incorrectly marked



Domain (spoofed)	% SIVT
esquire.com	77%
travelchannel.com	76%
foodnetwork.com	76%
popularmechanics.com	74%
latimes.com	72%
reuters.com	71%

Bad measurement

1. fakesite123.com has to pretend to be esquire.com to get bids;
2. fraud measurement shows high IVT as it is measuring the fake site with fake traffic
3. Fake esquire.com gets mixed with real so average fraud rates appear high.
4. Real esquire.com gets backlisted; bad guy moves on to another domain.

Domain spoofing examples

Fake sites disguise themselves as good domains to sell inventory

2017

"bad actors intentionally disguise the nature of the ad space they're selling. … a marketer might believe they're paying for ads on FT.com."

2018

"more than 1,400 apps were found to have loaded ads under TV Guide's domain name"

(2017) Pop-Unders / Redirects

These forms of fraud typically get by current fraud detection tech

a.k.a. **"zero-click" "pop-under" "forced-view" "auto-nav"**

Source: https://www.buzzfeed.com/craigsilverman/remember-tom

Fake sites/apps NOT detected

Fake sites

1221e236c3f8703.com
62b70ac32d4614b.com
a6f845e6c37b2833148.com
da60995df247712.com
d869381a42af33b.com
a1b1ea8f418ca02ad4e.com
1de10ecf04779.com
2c0dad36bdb9eb859f0.com
a6be07586bc4a7.com
fe95a992e6afb.com
42eed1a0d9c129.com
da6fda11b2b0ba.com
afa9bdfa63bf7.com
739c49a8c68917.com
baa2e174884c9c0460e.com
d602196786e42d.com
153105c2f9564.com
8761f9f83613.com
20a840a14a0ef7d6.com
31a5610ce3a8a2.com
5726303d87522d05.com
3ac901bf5793b0fccff.com
b014381c95cb.com
2137dc12f9d8.com

Fake sites

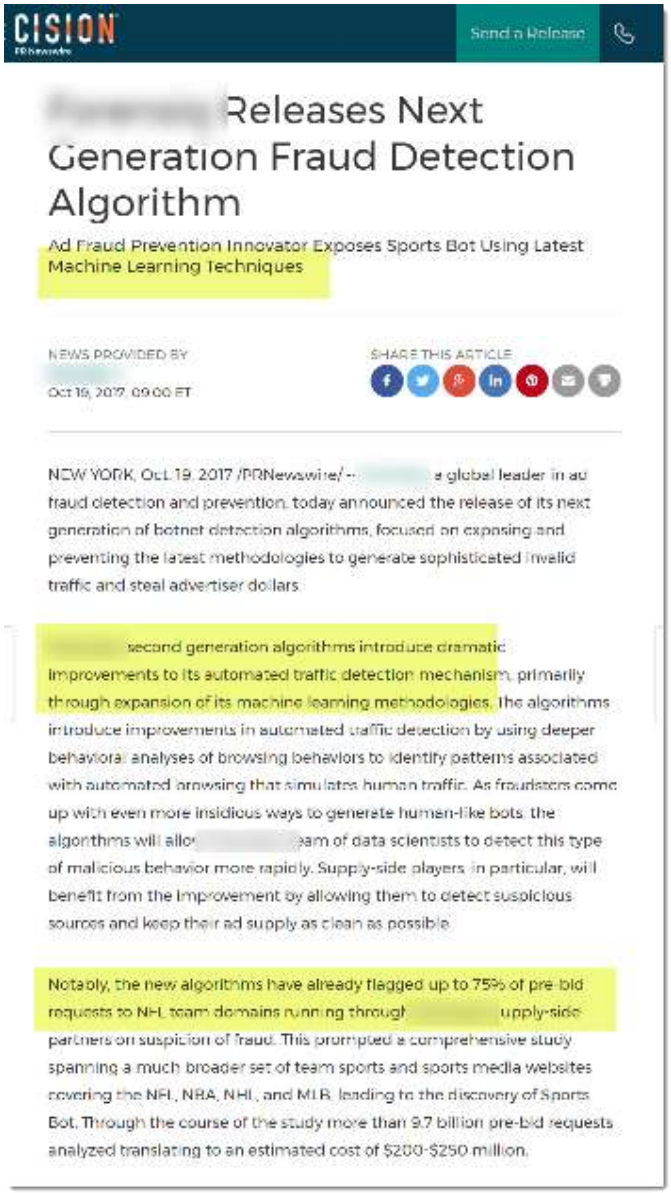
06f09b1008ae993a5a.com
fbfd396918c60838.com
97ff623306ff4c26996.com
b1f6fe5e3f0c3c8ba6.com
23205523023daea6.com
6068a17eed25.com
b1fe8a95ae27823.com
f4906b7c15ba.com
eac0823ca94e3c07.com
1f7de8569ea97f0614.com
21c9a53484951.com
24ad89fc2690ed9369.com
efd3b86a5fbddda.com
34c2f22e9503ace.com
0926a687679d337e9d.com
6a40194bef976cc.com
33ae985c0ea917.com
02aa19117f396e9.com
f8260adbf8558d6.com
9376ec23d50b1.com
pushedwebnews.com
a0675c1160de6c6.com
0f461325bf56c3e1b9.com
850a54dbd2398a2.com

Fake apps

com.dxnxbgj.mkridqxviiqaogw
com.obugniljhe.fptvznqwhmcjm
com.bpo.ksuhpsdkgvbtlsw
com.rlcznwgouw.vvtexstbfttngc
com.kasbgf.sbzwtgpcbjexi
com.bprlgbl.vbze
com.zka.lzhsoueilo
com.alxsavx.mizzucnlb
com.jxknvk.lrwfdfirdzpsw
com.tvwvqbt.wbshaguqy
com.iwnxtpahcu.leyuehdwdbb
com.okf.rhvemtykfibzpxj
com.obpmirzste.ldsjpv
com.zmm.shmxvjxnsagndui
com.nqzwr.leusrmpmsq
com.rced.zcdsglptpdlwpu
com.kerms.ehlsgnc
com.cmia.iabhheltm
com.skggynmtx.tyyjnwpefvqtll
com.kgdtltnuv.hayvfhob
com.ztzsiqg.dyojlxdscxws
com.xlwuqe.ddrdhsuosbn
com.rkrhmzee.wjcoznxu
com.ebhzb.hbzvomzpcctovj

Fake botnet fabricated for PR

Sportsbot was entirely fabricated for PR for fraud detection co.



CISION

Releases Next Generation Fraud Detection Algorithm

Ad Fraud Prevention Innovator Exposes Sports Bot Using Latest Machine Learning Techniques

NEWS PROVIDED BY

Oct 19, 2017, 09:00 ET

SHARE THIS ARTICLE

NEW YORK, Oct. 19, 2017 /PRNewswire/ -- a global leader in ad fraud detection and prevention, today announced the release of its next generation of botnet detection algorithms, focused on exposing and preventing the latest methodologies to generate sophisticated invalid traffic and steal advertiser dollars.

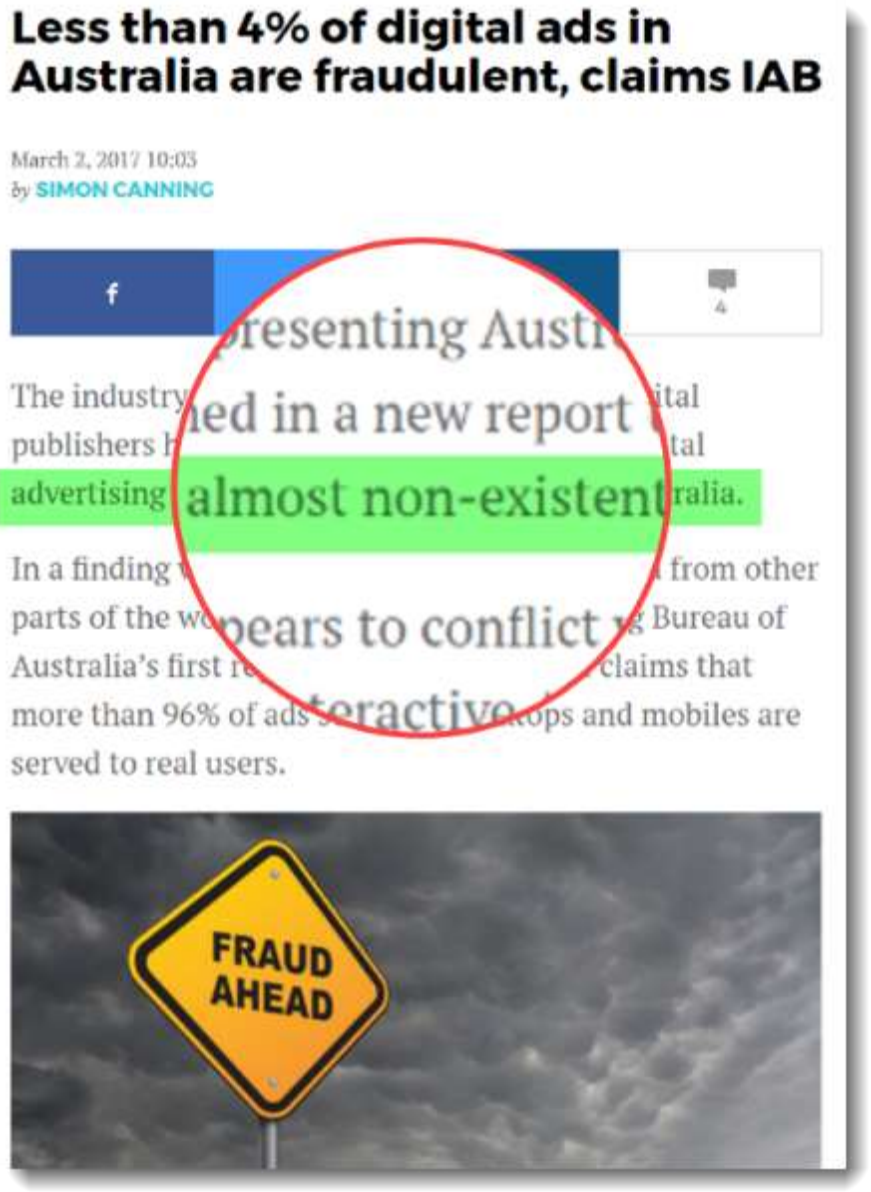
second generation algorithms introduce dramatic improvements to its automated traffic detection mechanism, primarily through expansion of its machine learning methodologies. The algorithms introduce improvements in automated traffic detection by using deeper behavioral analyses of browsing behaviors to identify patterns associated with automated browsing that simulates human traffic. As fraudsters come up with even more insidious ways to generate human-like bots, the algorithms will allo am of data scientists to detect this type of malicious behavior more rapidly. Supply-side players, in particular, will benefit from the improvement by allowing them to detect suspicious sources and keep their ad supply as clean as possible.

Notably, the new algorithms have already flagged up to 75% of pre-bid requests to NHL team domains running through upply-side partners on suspicion of fraud. This prompted a comprehensive study spanning a much broader set of team sports and sports media websites covering the NFL, NBA, NHL, and MLB, leading to the discovery of Sports Bot. Through the course of the study more than 9.7 billion pre-bid requests analyzed translating to an estimated cost of $200-$250 million.

PRESS RELEASE:
"used highly sophisticated techniques to fraudulently load ads on the affected sites without the site owners' consent, ***leveraging a new methodology*** *that allows it to monetize inventory on premium domains."*

"The botnet was **completely fabricated for the press release** announcing their new algo. None of this actually happened; **no ads were injected** into any of the sites they named in the press release. This was confirmed by direct measurement on the good publishers' sites. They were falsely accused and their reputation was harmed by this publicity stunt.

Just because you can't measure it



Less than 4% of digital ads in Australia are fraudulent, claims IAB

March 2, 2017 10:03
by SIMON CANNING

f 4

presenting Austr

The industry ed in a new report ital publishers h tal advertising almost non-existent ralia.

In a finding from other parts of the wo pears to conflict g Bureau of Australia's first re claims that more than 96% of ads teractive ops and mobiles are served to real users.

FRAUD AHEAD

… doesn't mean it's not there.

MRC, TAG

Media Ratings Council

"MRC accredits companies for measuring what they say they will measure and to standards; MRC cannot ascertain whether the measurements are correct"

GIVT

Bots that self-declare

SIVT

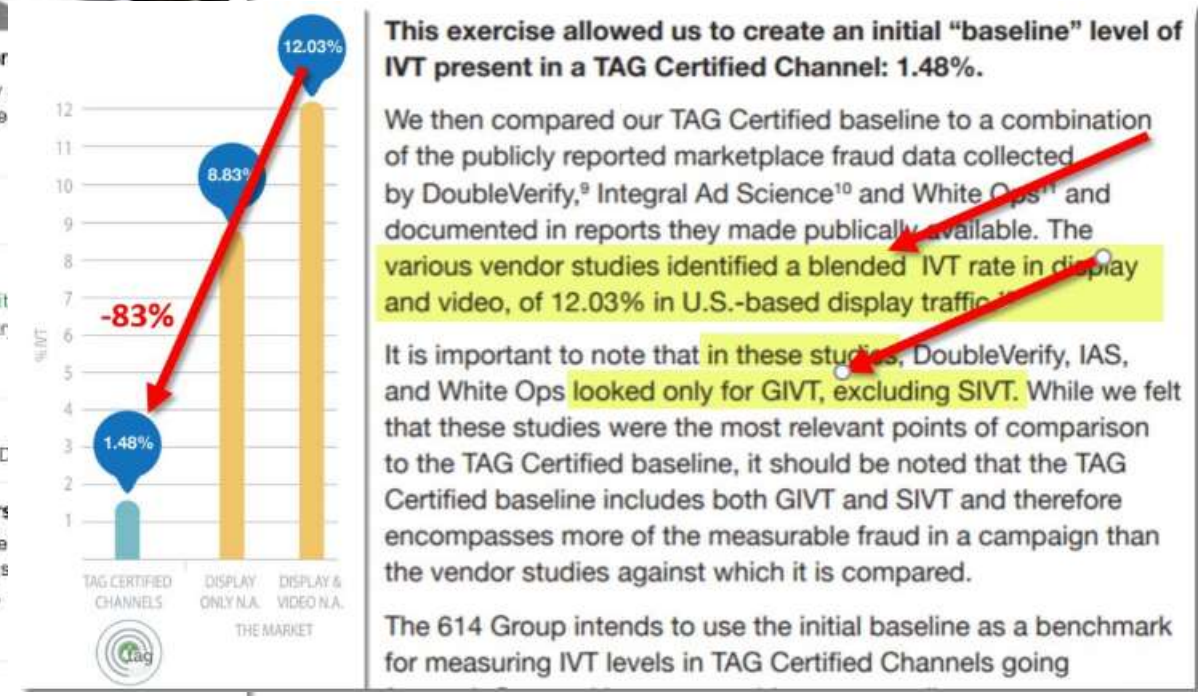
Blackbox, secret sauce

Trustworthy Accountability Group

TAG certification allows companies to self-declare they are trustworthy and clean.

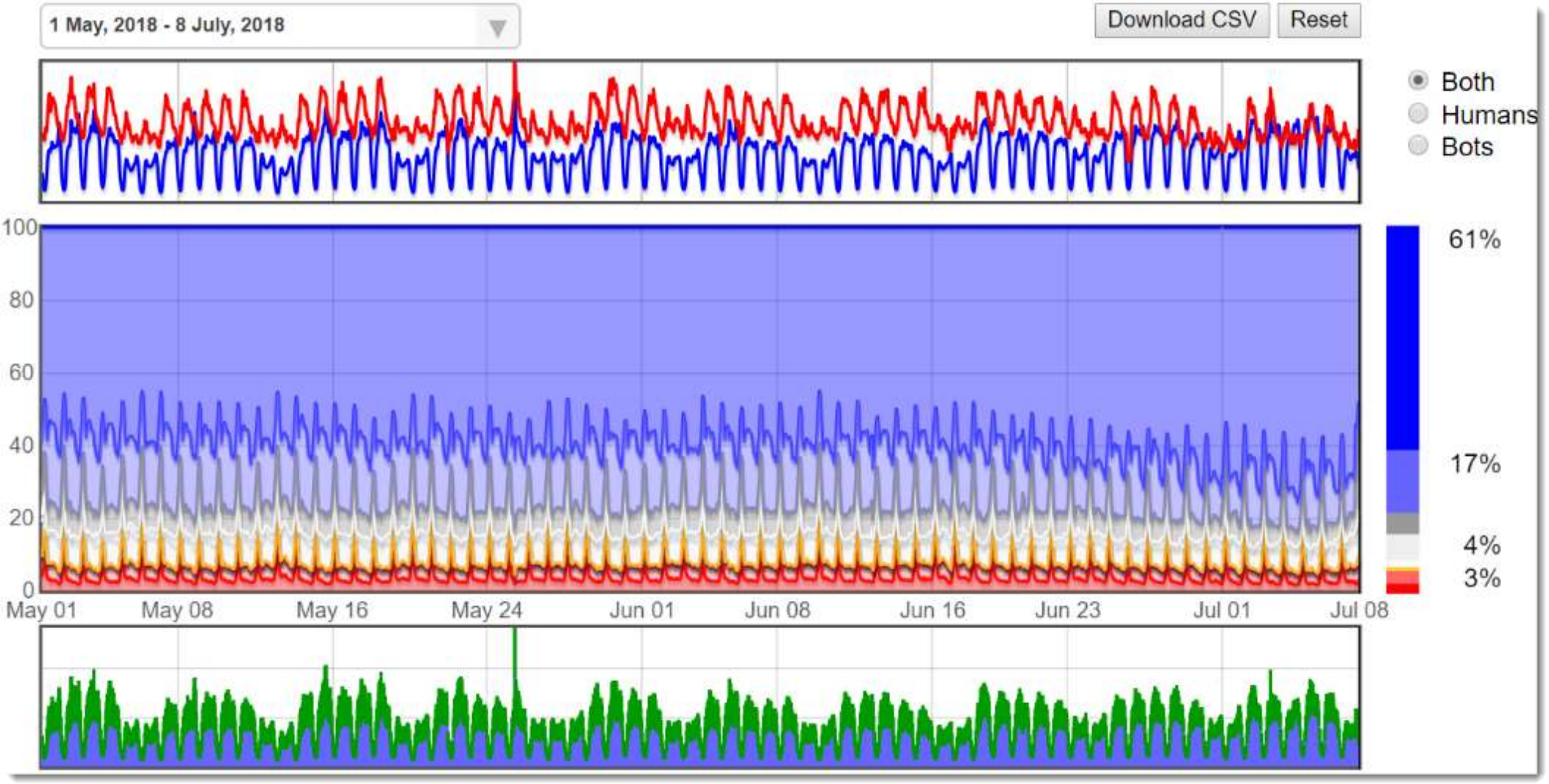
TAG claims credit for others' work

"@tag_today says it has a 'monumental' breakthrough on a method that can cut online fraud by more than 83%"



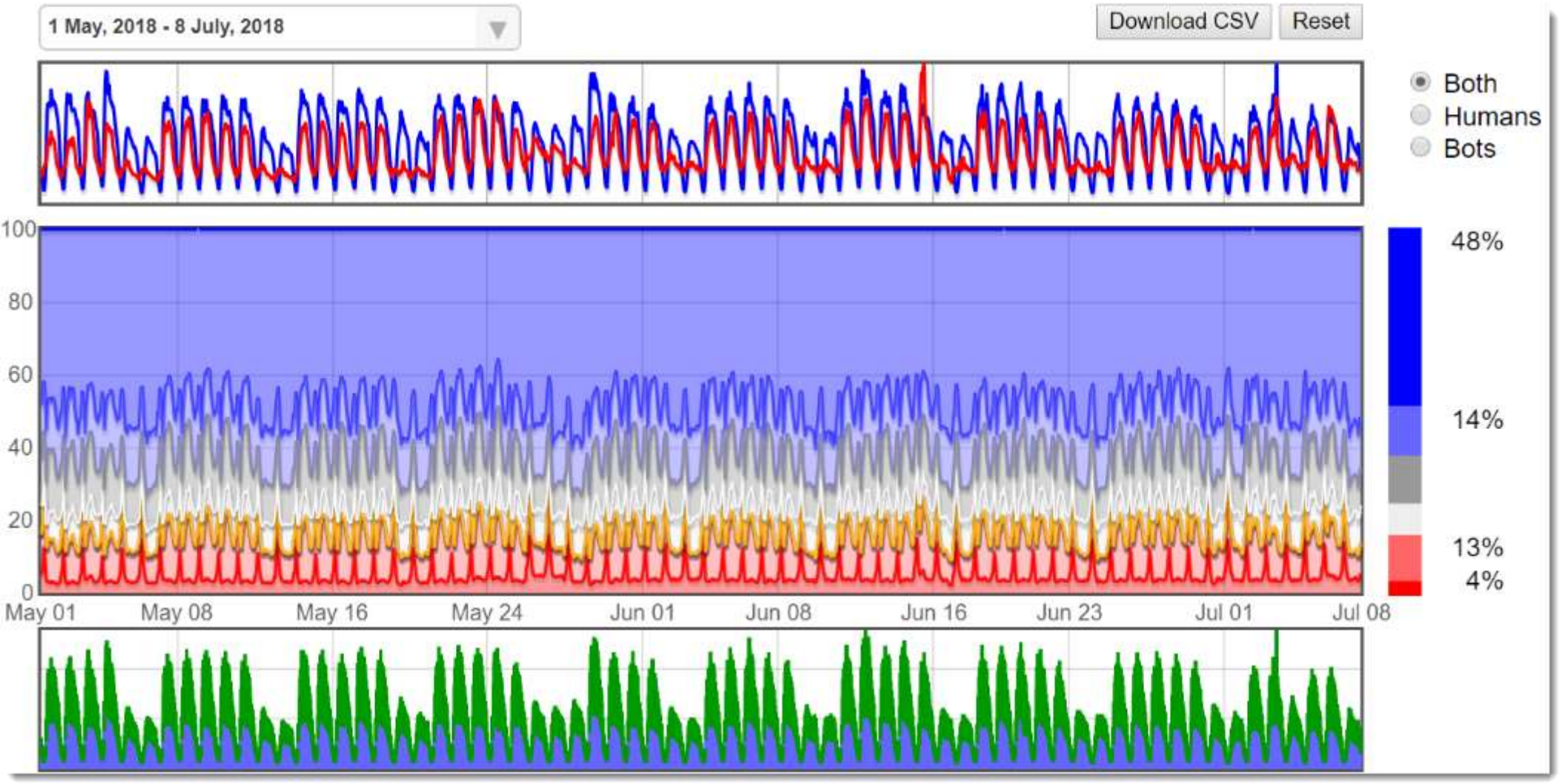
Local TV websites

Great consistency in the data over long periods of time



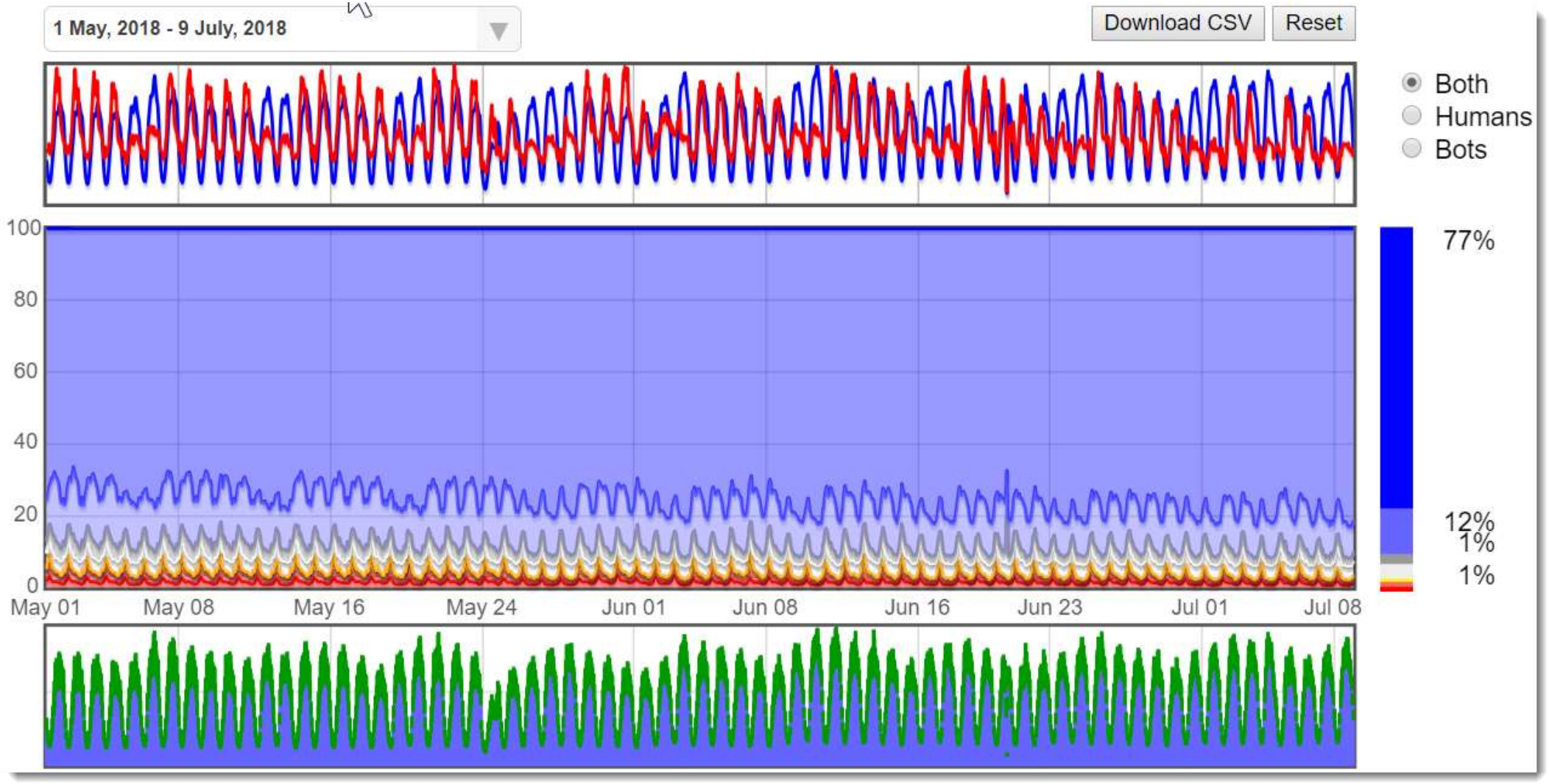
Local radio websites

Great consistency in the data over long periods of time



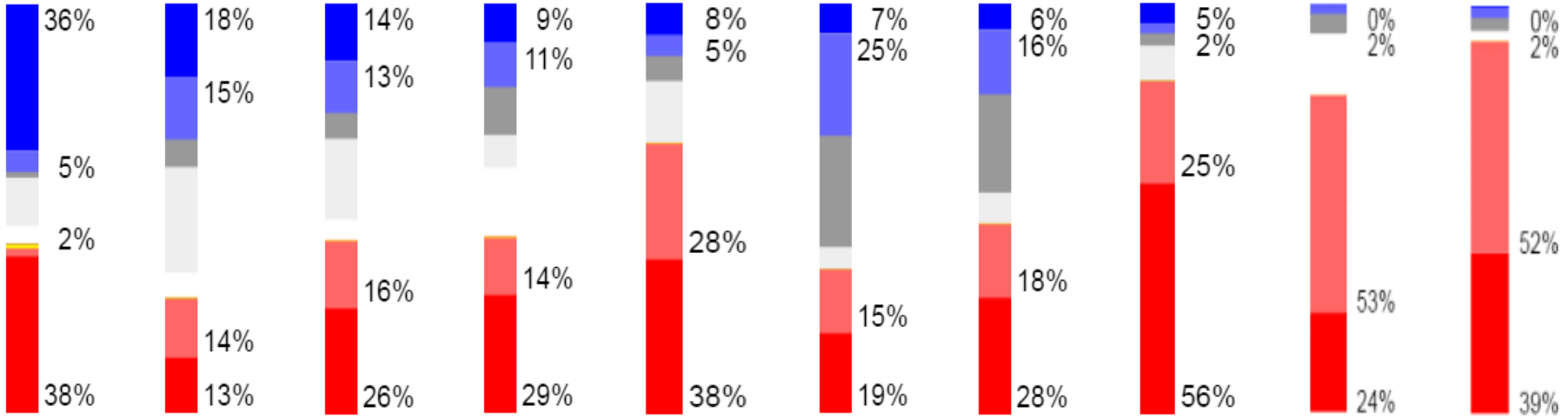
Magazine websites

Great consistency in the data over long periods of time

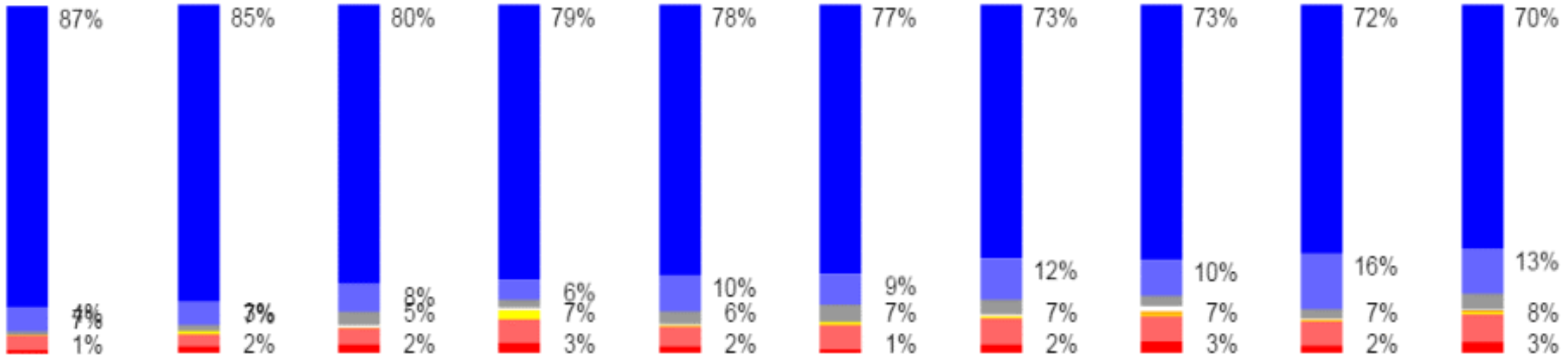


Humans (blue) on ad networks vs good publishers

Ad Networks



Publishers



Marketers are running their own experiments

Chase: **-99% reach**, no impact

"99% reduction in 'reach' … Same Results."

The New York Times

EDIA

Chase Had Ads on 400,000 Sites Then on Just 5,000. Same Result

SAPNA MAHESHWARI MARCH 29, 2017

"JPMorgan had already decided last year to oversee its own programmatic buying operation.

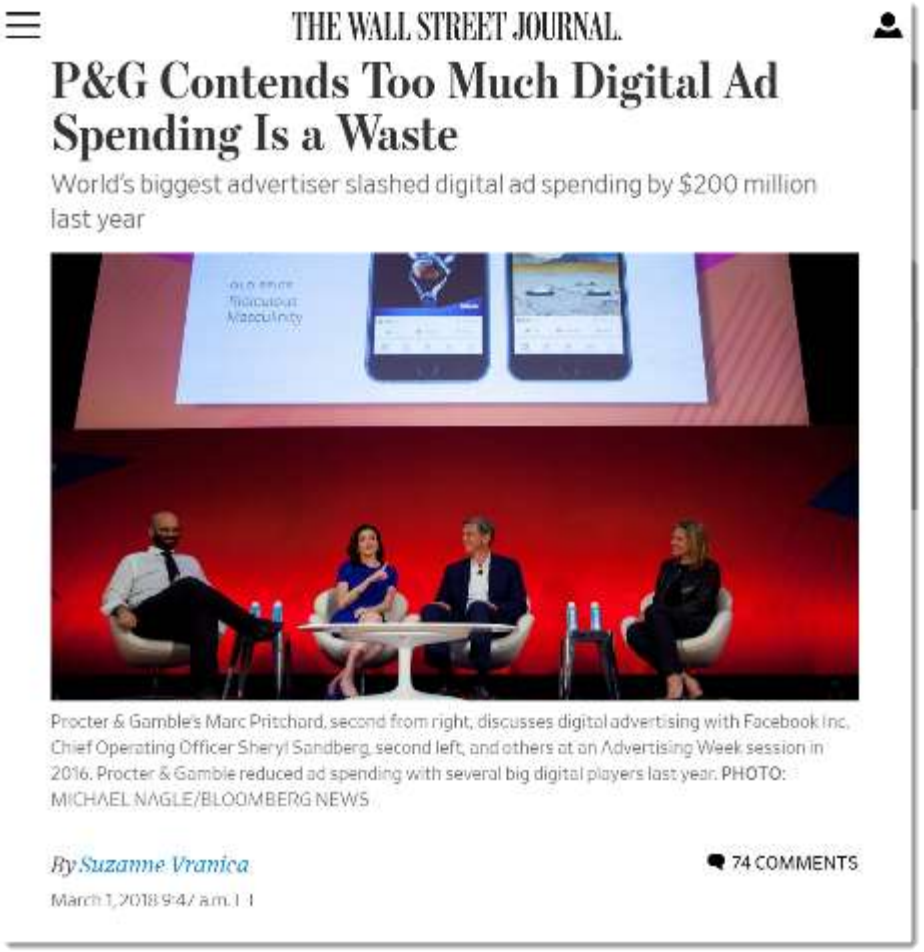
Advertisements for JPMorgan Chase were appearing on about 400,000 websites a month. [But] only 12,000, or 3 percent, led to activity beyond an impression.

[Then, Chase] limited its display ads to about 5,000 websites. We haven't seen any deterioration on our performance metrics," Ms. Lemkau said."

Source: NYTimes, March 29, 2017

(because it wasn't real, human reach)

P&G: cut $200M, no impact



THE WALL STREET JOURNAL.

P&G Contends Too Much Digital Ad Spending Is a Waste

World's biggest advertiser slashed digital ad spending by $200 million last year

Procter & Gamble's Marc Pritchard, second from right, discusses digital advertising with Facebook Inc. Chief Operating Officer Sheryl Sandberg, second left, and others at an Advertising Week session in 2016. Procter & Gamble reduced ad spending with several big digital players last year. PHOTO: MICHAEL NAGLE/BLOOMBERG NEWS

By Suzanne Vranica

74 COMMENTS

March 1, 2018 9:47 a.m. ET

"Once we got transparency, it illuminated what reality was," said Mr. Pritchard. P&G then took matters into its owns hands and voted with its dollars, he said."

"As we all chased the Holy Grail of digital, self-included, we were relinquishing too much control—blinded by shiny objects, overwhelmed by big data, and ceding power to algorithms," Mr. Pritchard said.

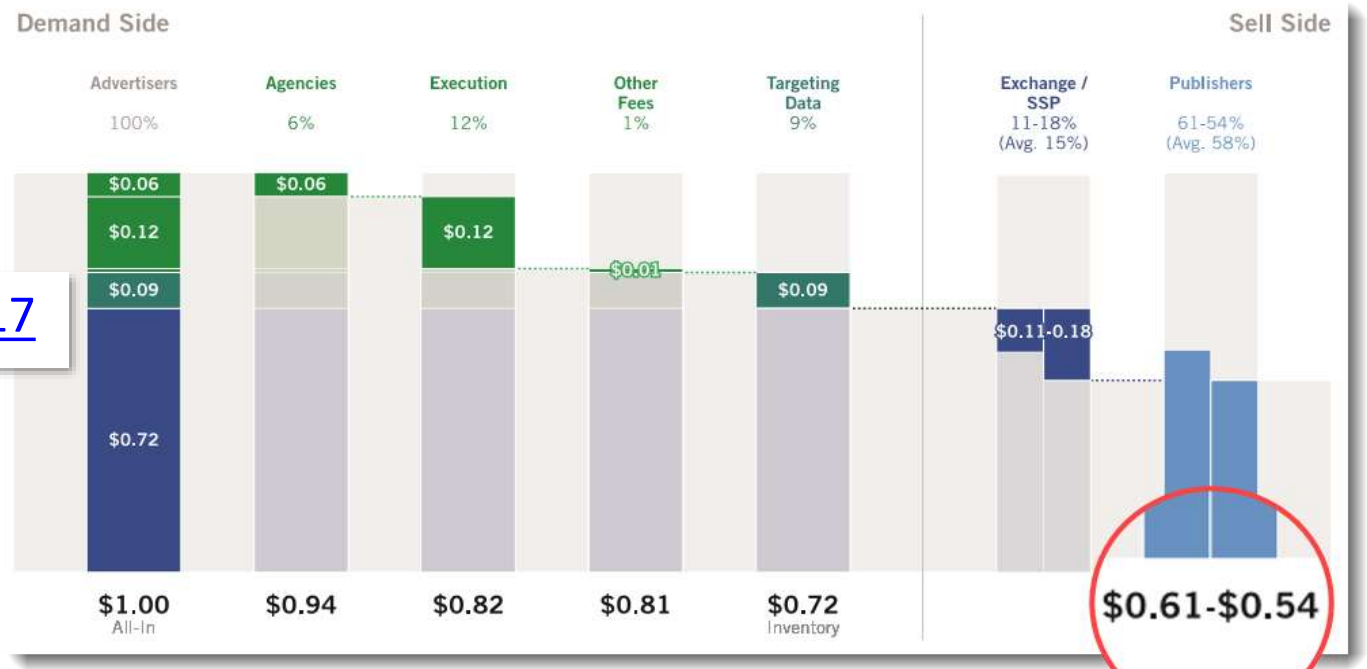
Source: WSJ, March 2018

Ad Fraud is NOT a Tech Problem …

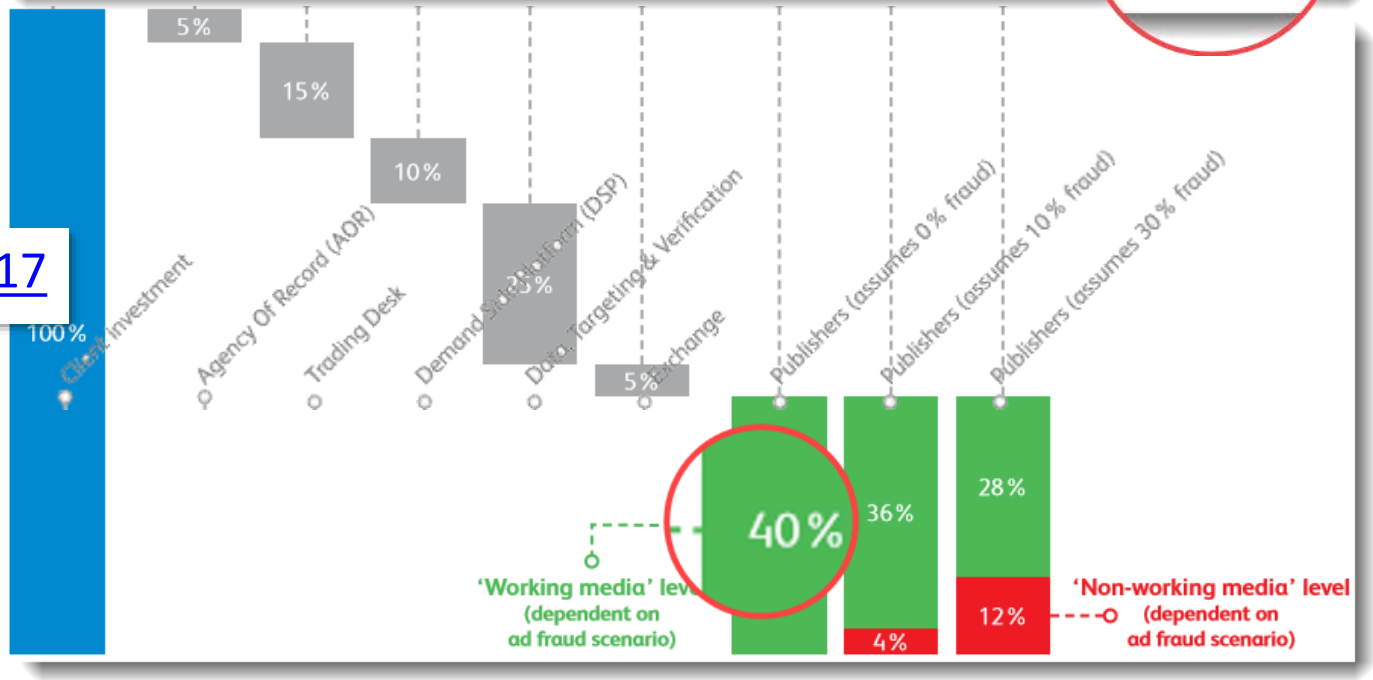
Ad Fraud IS an Incentives Problem…

“Ad Tech Tax” Middlemen Profits

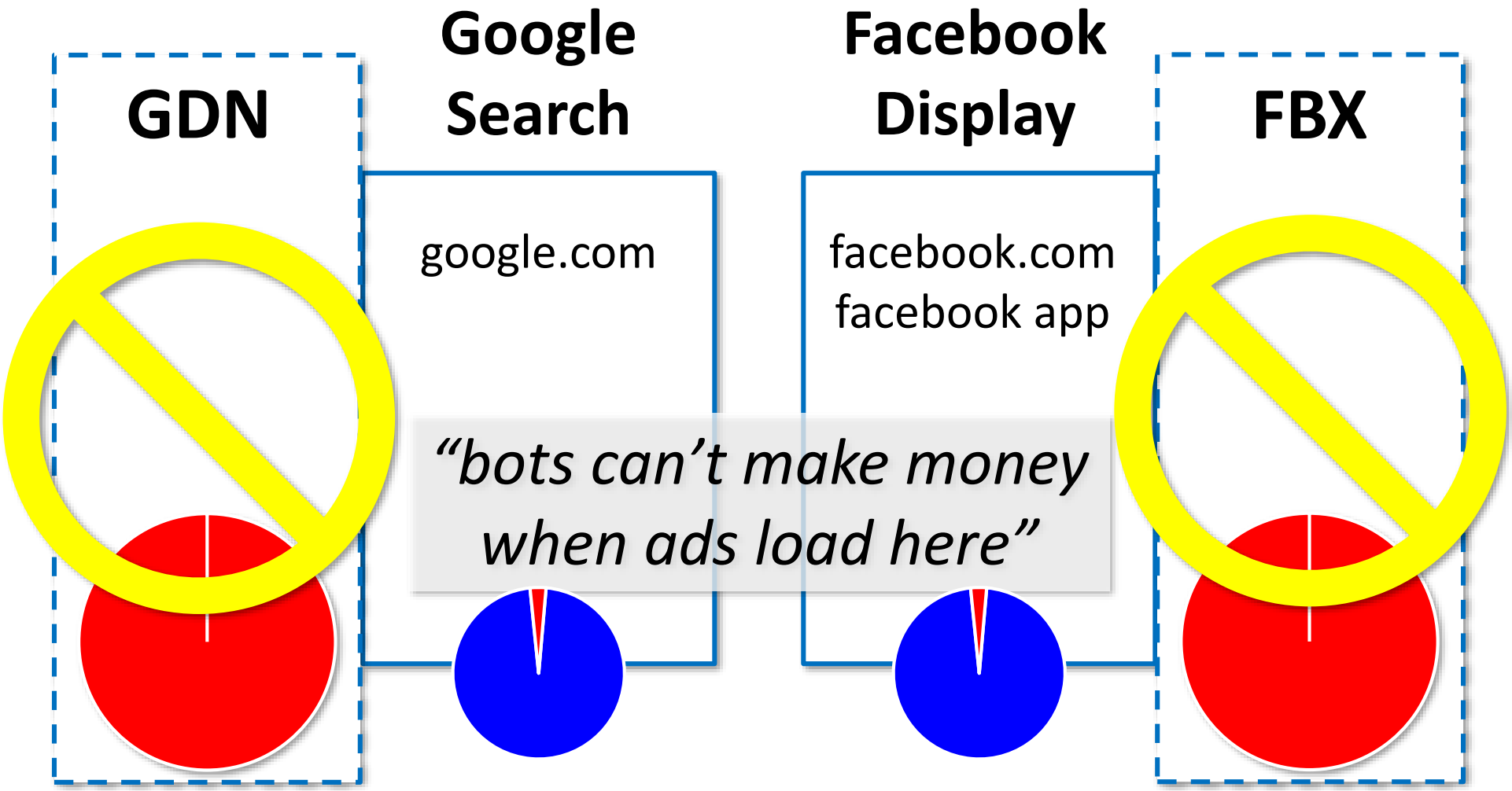
Source: ANA, May 2017



Source: WFA, April 2017



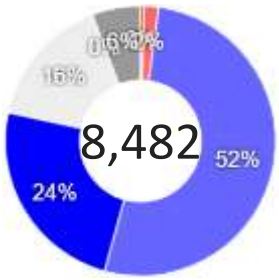
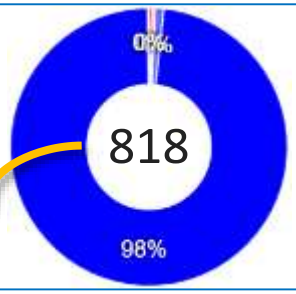
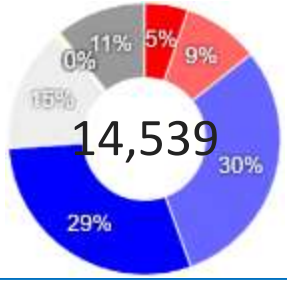
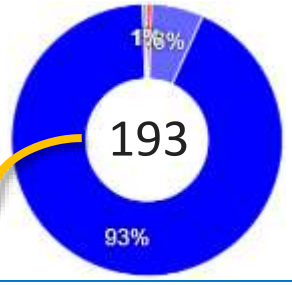
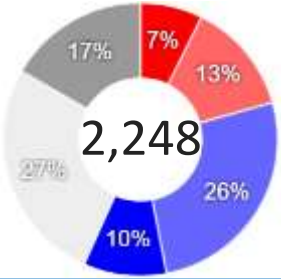
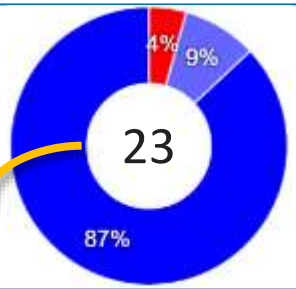
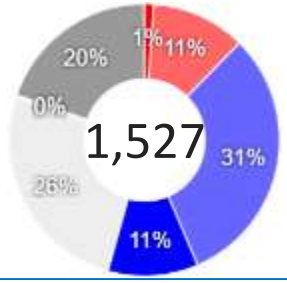
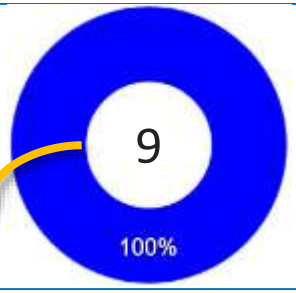
Walled gardens are fine, on-site …



less bots | more humans

first-party IDs, people-based marketing

Compare actual outcomes

	Site **Traffic**	**Humans**	**Conversions**
Display 1		2,036 humans human conversion rate 40%	
Display 2		4,216 humans human conversion rate 5%	
Display 3		225 humans human conversion rate 9%	
Display 4		168 humans human conversion rate 5%	

Small businesses found/killed fraud

Small Business A

- Noticed a 118,600% increase in Android devices hitting her site during campaign – AND no additional goal completions
- Compiled additional data that corroborated it was fraud; presented to ad network and **got refund for entire campaign**

Small Business B

- Year over year, marketer noticed the discrepancy between counts reported by ad network versus his own Google Analytics shot up dramatically (even though cost-per-action remained similar).
- Conversions also dropped dramatically. With deeper digging, he found the ratio of audience network inventory grew from 5% to 65% of total impressions. **Solved by turning off audience network**.

"Both of these small businesses used their own analytics and gut instinct; they resolved ad fraud without using any expensive tech."

How do we actually solve ad fraud?

- Digital assurance
- Publisher audits
- Continuous assurance

Stop buying poop water (bad ads)

"Which? 1) start with 'poop water' and filter it before you drink it?, or 2) start with fresh water?"

"fraud detection can't filter it for you"

About 376,000 results (0.53 seconds)

This Ingenious Machine Turns Feces Into Drinking Water | Bill Gates
https://www.**gates**notes.com/Development/Omniprocessor-From-Poop-to-Potabl
Jan 5, 2015 - **Bill Gates** recently got to check out the Omniprocessor, an ingenious ... Janicki Bioenergy, which turns human waste into **water** and ...

Watch Bill Gates Sip Water Made From Sewer Sludge [Update
www.forbes.com/sites/amitchowdhry/2015/01/10/janicki-omniprocessor/
Jan 10, 2015 - The goal of the **Gates** Foundation is to improve the quality of life for pe world. Over 2.5 billion people around the world do not ...

Bill Gates' poop water machine gets a test run - Aug. 13, 2015
money.cnn.com/2015/08/13/technology/**bill-gates**-poop-**water**/
Aug 13, 2015 - **Bill Gates** is backing a machine that turns poop into **water**, electricity a third of whom have no access to the city's **sewer** system.

Water, Sanitation & Hygiene - Bill & Melinda Gates Foundation
www.**gates**foundation.org/What-We-Do/Global.../**Water**-Sanitation-and-Hygiene
Our **Water**, Sanitation & Hygiene strategy is led by Brian Arbogast, director, and ... other systems that discharge raw **sewage** into open drains or surface waters.

"fight ad fraud with common sense"

- stop wasting money on tech that doesn't work
- insist on detailed data and look at the analytics yourself

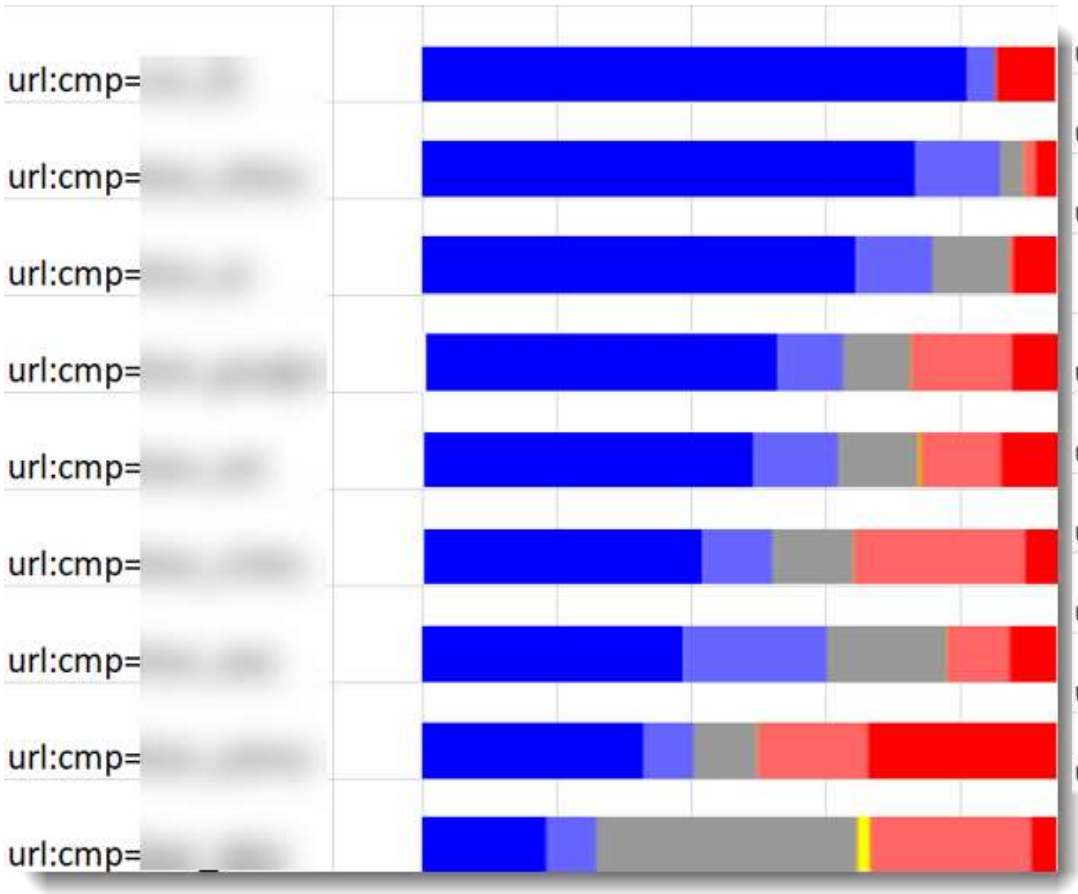
#FOMO or #FOFO (or both)

Tech + Technique

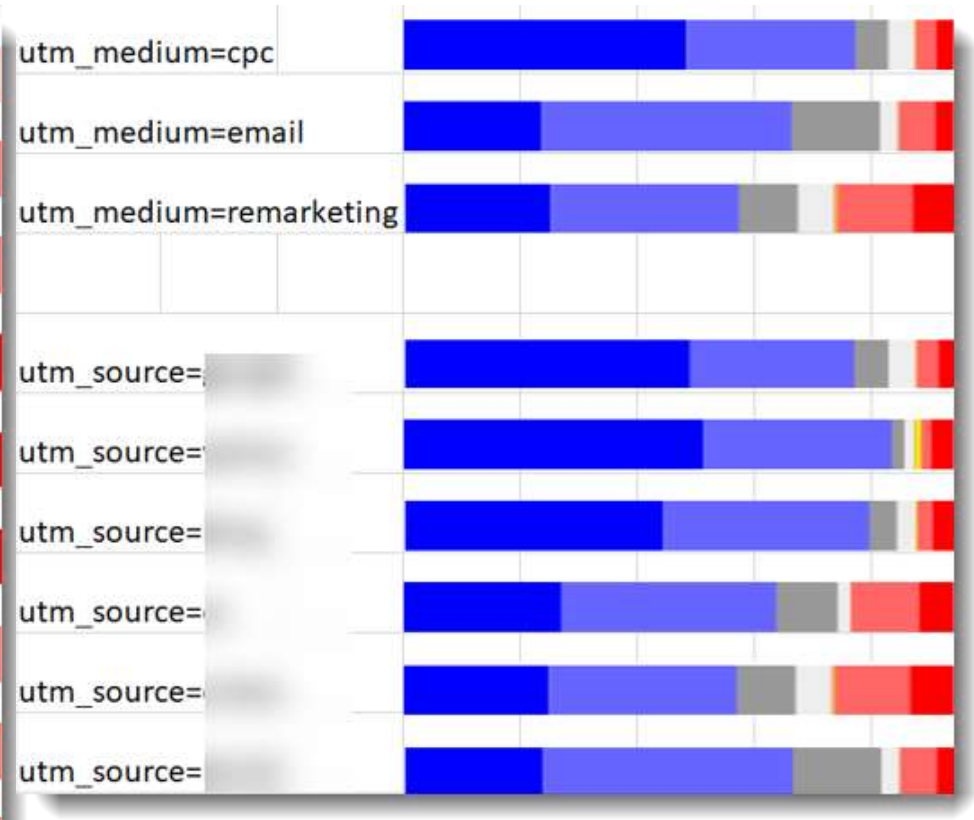
Tech to see relative quality

- **Blue** means humans
- **Red** means bots

Marketer 1



Marketer 2



"**increase spend** on sources driving more humans (blue); **reduce spend** on sources with more bots (red)"

Technique to reduce fraud

For each "bid won," an "ad impression" should be served

DSP says

Adserver says

Domain	Bids won	Impressions served	% difference
Weather.com	346,071	360,000	4%
Spotify.com	554,682	524,000	-6%
zimbio	108,039	94,000	-13%
looper	101,288	84,000	-17%
standardnews	112,809	92,000	-18%
accuweather	120,586	96,000	-20%
tvtropes	98,099	72,000	-27%
easybib	141,276	102,000	-28%
Citationmachine	231,399	166,000	-28%
Howstuffworks	678,279	484,000	-29%
Definition	280,653	190,000	-32%
Wunderground	192,239	124,000	-35%
Centurylink	154,482	83,000	-46%
groovyhistory	78,844	40,000	-49%
Eternallifestyle	244,263	114,000	-53%
pogo	125,501	56,000	-55%
Zynga	144,829	64,000	-56%
Wildtangent	246,766	34,000	-86%
getitlove	126,768	-	-100%

Bad guys may not even wait till the ad is served since they are already paid based on the number of impressions won.

From the data, the more fraudulent the site, the greater the discrepancy

– e.g. 80 – 100%

Marketers' anti-fraud playbooks

"Plays" that marketers can run themselves, to assess ad fraud

- **Brand (B2C) Marketers' Anti-Fraud Playbook**
- **Performance (B2B) Marketers' Anti-Fraud Playbook**
- **Questions to Ask Verification Vendors**

"They sell fraud detection; I teach fraud prevention."

Buy from **Good Publishers**

How can we tell "good" from "other?"

*"**Business practice review** by independent 3rd party provides the trust and assurance that distinguishes **good publishers** from 'sites that carry ads'."*

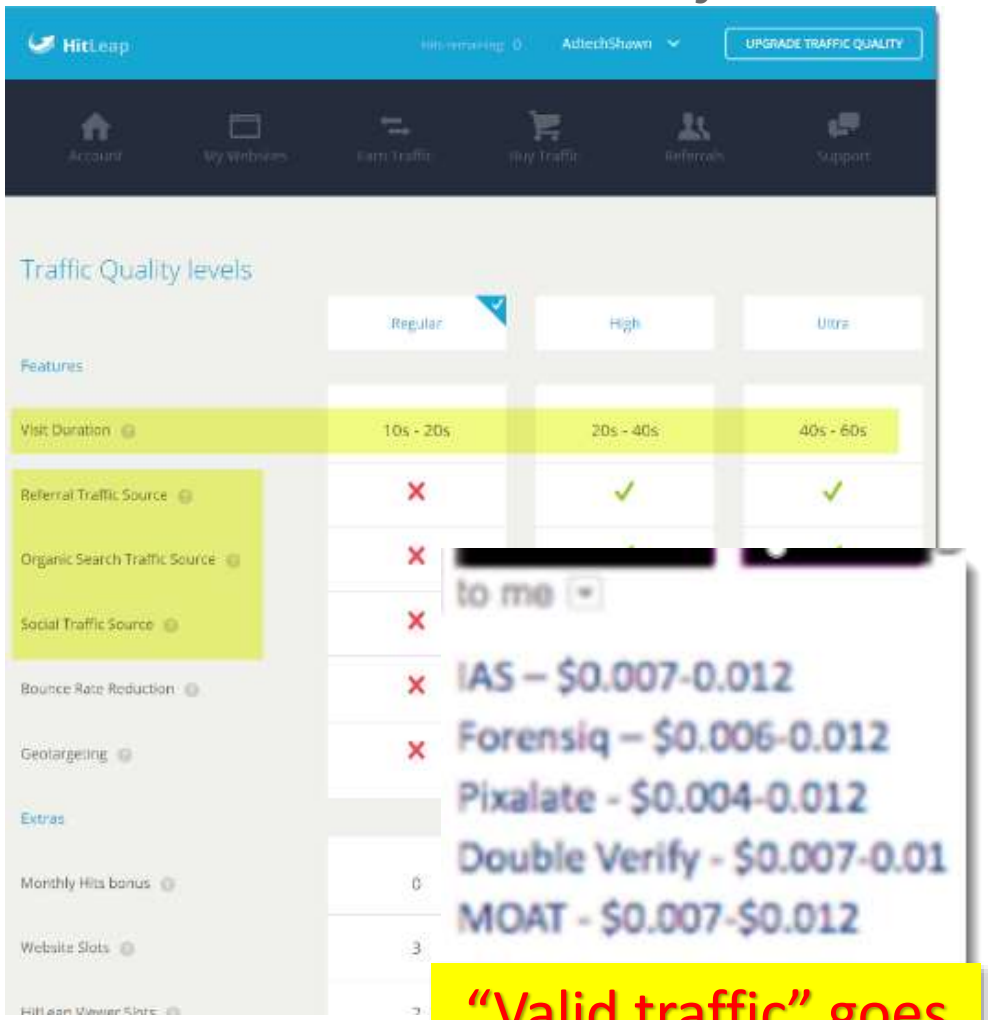
3-Step Publisher Certification Process

- **Business process** review to validate business practices used to manage audience traffic
- Technology employed to **validate quantities** of third-party website analytics
- Technology employed to validate that business practices are working properly to deliver **high-quality audience**

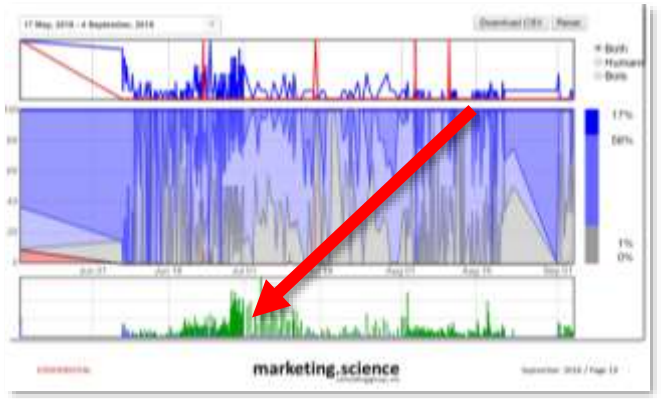
Don’t “source traffic”

Sourcing traffic (not digital marketing) exposes you to fraud

Choose Your “Traffic Quality Level”



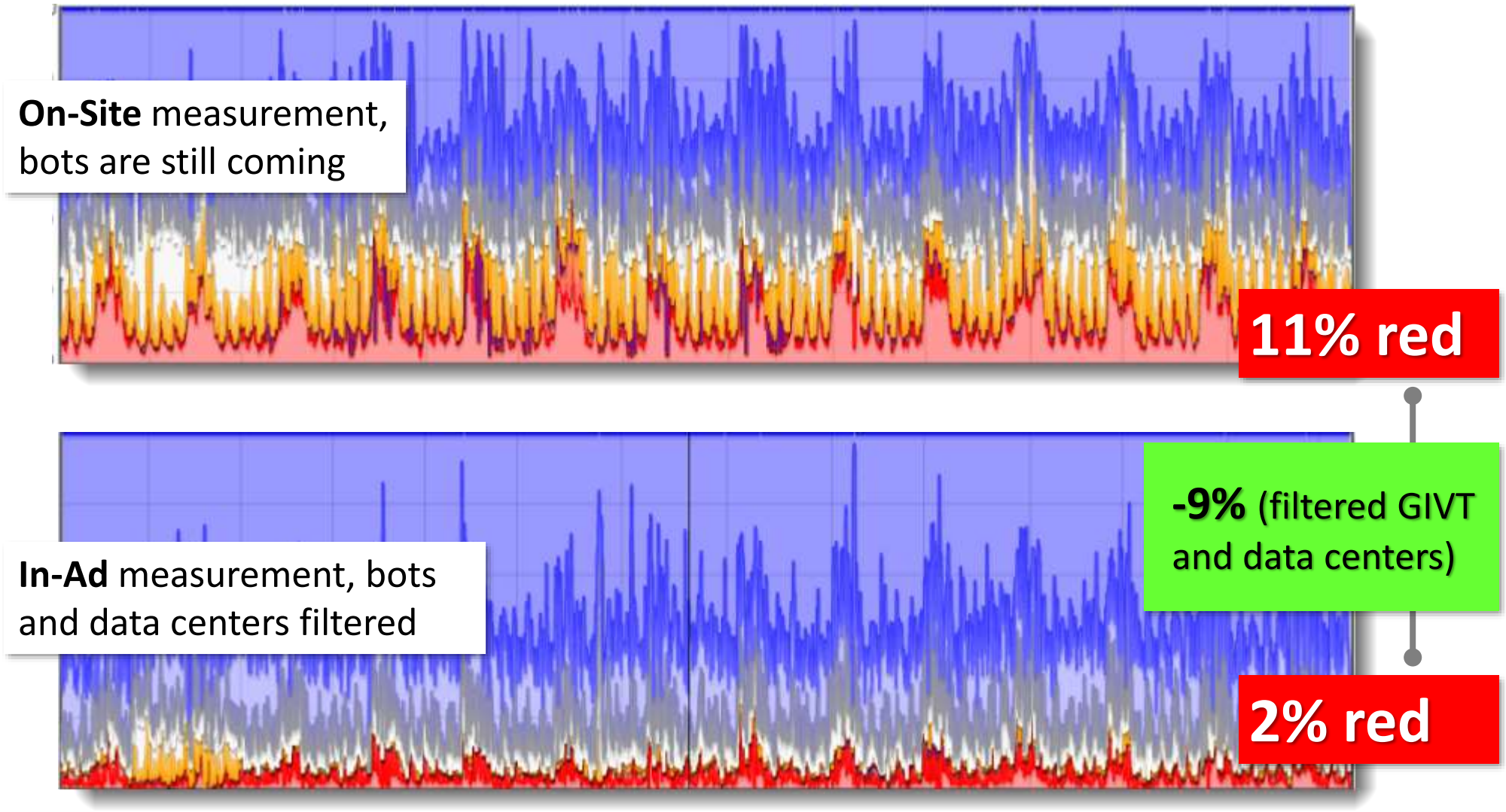
“Valid traffic” goes for higher prices



Good publishers act to reduce bots

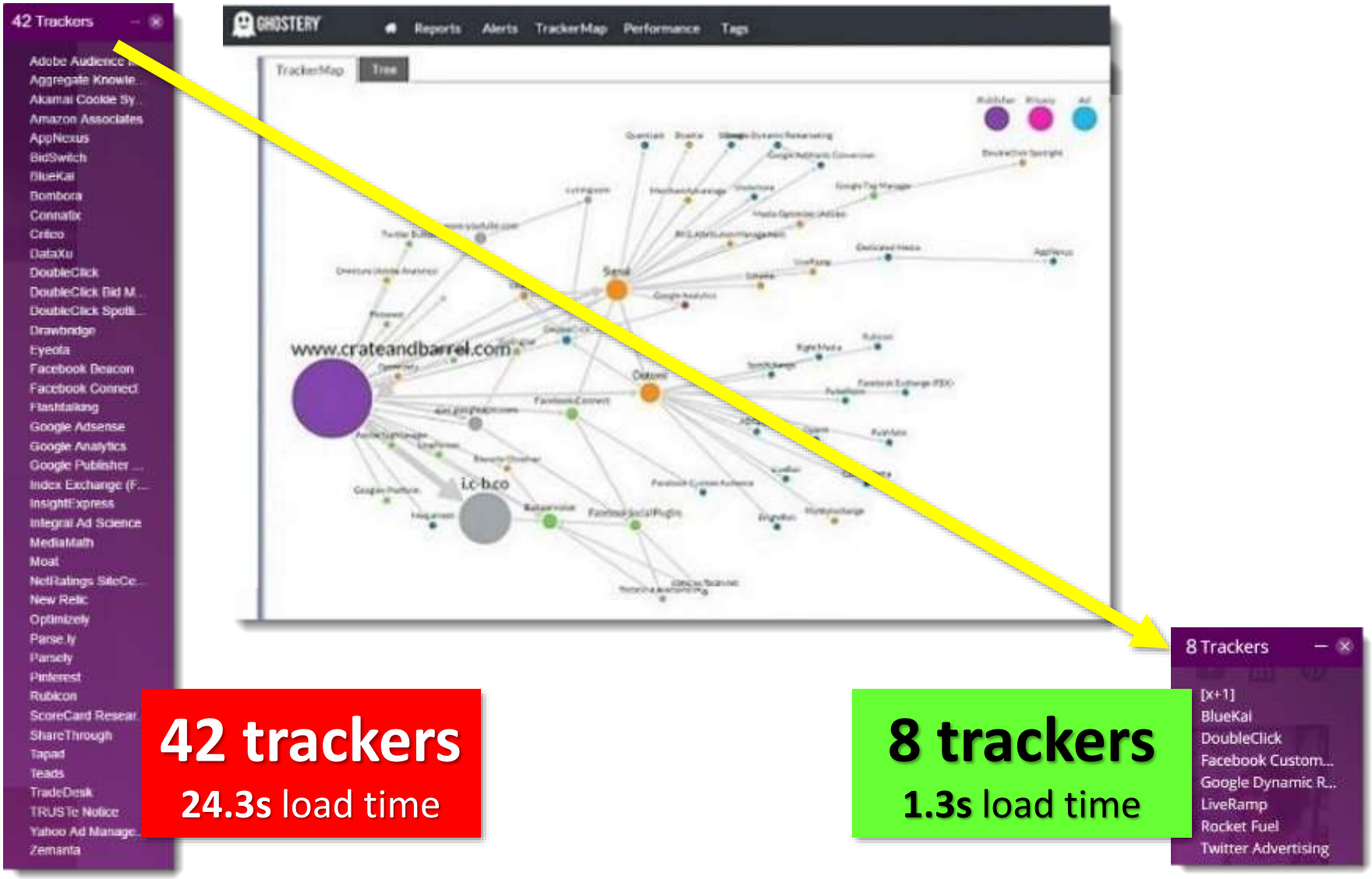
Good publishers protect **advertisers**

"Filter data center traffic and not call the ads"



Good publishers protect their **users**

"minimize 3rd party javascript trackers on pages"

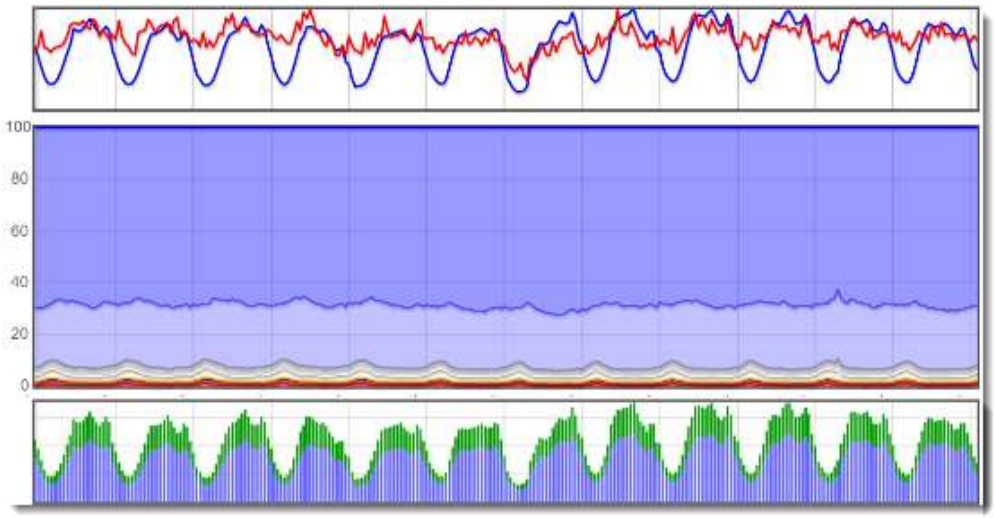


42 trackers
24.3s load time

8 trackers
1.3s load time

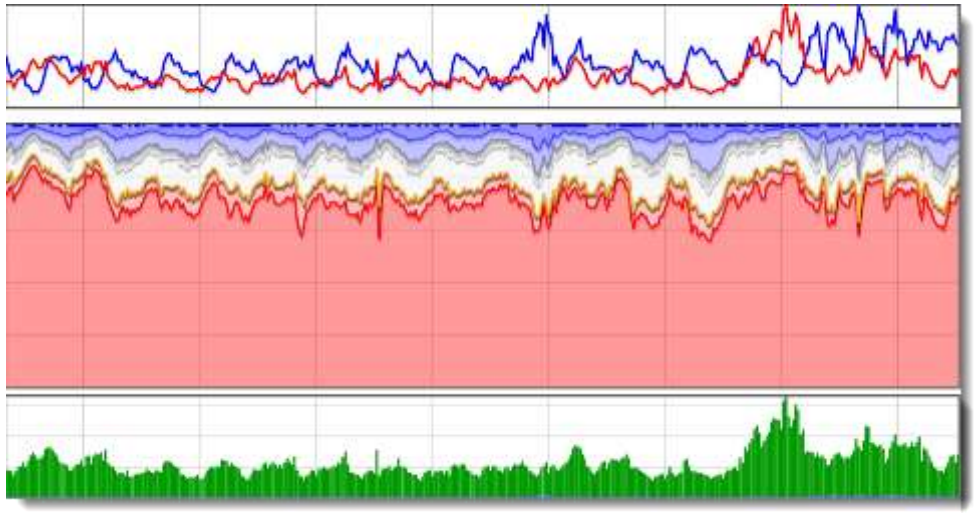
Good publishers have good practices

Good Publishers



- don‘t source traffic
- protect advertisers
- protect consumers

“sites that carry ads”

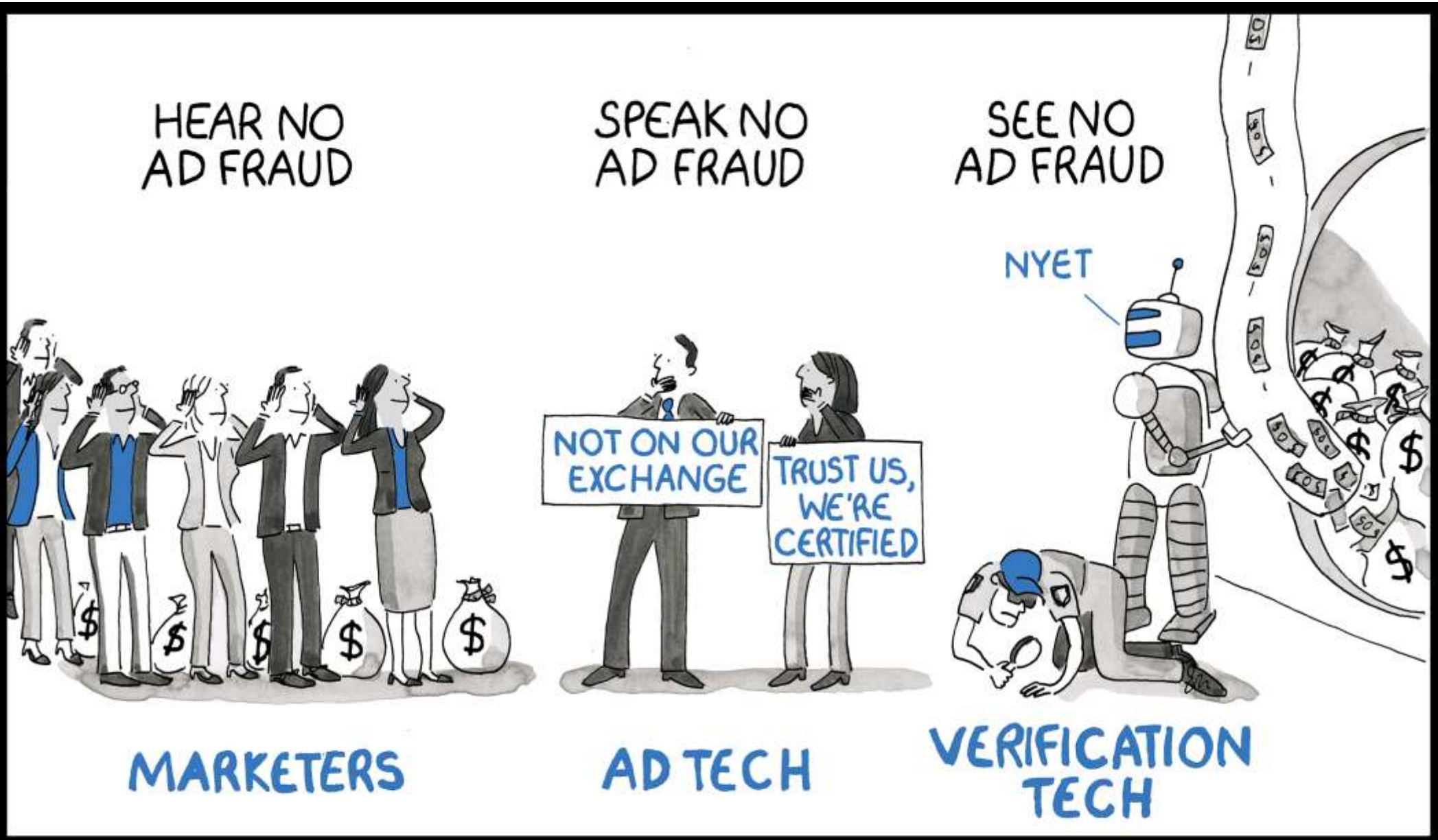


- source traffic
- audience extension
- auto-refresh
- traffic laundering

“good business practices lead to good looking data”

Buy from Quality Certified Publishers.

Opportunity
&
Obligation



Digital Marketing circa 2018

About the Author

Augustine Fou, PhD.
acfou [@] mktsci.com
212. 203 .7239

Dr. Augustine Fou – Independent Ad Fraud Researcher

Published slide decks and posts:
http://www.slideshare.net/augustinefou/presentations
https://www.linkedin.com/today/author/augustinefou

THE WALL STREET JOURNAL. **2015**

In the case of viewability trickery, these fraudsters are looking to make as much money as possible from this practice, and unlike legitimate websites, they aren't too concerned with guarding the integrity of editorial content. So they can just put ads wherever they need to go on Web pages to get a high score from the third parties that track Web ad viewability. They also know not to score so high that they look suspicious, said Dr. Augustine Fou, a former ad agency executive who has become a consultant specializing in non-human traffic.

ADWEEK **2013**

ıfriends and Dreammining, a gaming hub aimed at young girls, plus a variety of ıuently blacklisted by ad buyers. According to Augustine Fou, founder of the ıg Science Consulting Group, Dreammining raises many questions. Using Alexa ı found Dreammining's top search term to be "mining of selena," which exhibits ſic on Google, he points out. The site also has a high at-work audience that doesn't ; demo, while the second- and third-largest domains driving traffic to the site are

ExchangeWire **2016**

ExchangeWire invite Dr Augustine Fou (pictured below), a cybersecurity and ad fraud researcher, who advises advertisers, publishers, and agencies on the technical aspects of fighting digital ad fraud and improving the effectiveness of digital advertising, to explain the threats that javascript trackers pose to website owners (i.e. publishers) when installed on their sites. Dr Fou

Advertising Age **2014**

In the video below, ad fraud researcher and technical forensics expert Dr. Augustine Fou demonstrates how these scammers work their craft, narrating a simulation of a real bot script he ran on top of a dummy version of The New York Times' homepage. While these bots are

The Register® *Biting the hand that feeds IT* **2017**

For those buying online ads, it might just be both halves, due to fraud. "It's about 60 to 100 per cent fraud, with an average of 90 per cent, but it is not evenly distributed," said Augustine Fou, an independent ad fraud researcher, in a report published this month.