AD FRAUD SUMMARY

OXFORD BIOCHRONOMETRICS analyzes millions of web interactions and ad views per day. Based on our advanced algorithms we can determine the behavior of each visitor and device to determine whether the interaction is a human or an automated script appearing to be a human (i.e., a bot). Our false positives and false negatives are under one percent despite the fact that bot technology is constantly evolving.

Bots are attracted to digital ads and websites for a variety of reasons. The biggest abuses are driven by financial gains for the players involved - the bot operator, the publisher of the website, the network, the ad agencies and other participants in the chain. The business model generally is quite simple across the board. Fees are charged per event and the more events that are logged the more money that can be charged. The following are some examples:

- **Publisher Fraud** occurs when a website publisher purchases bot to view their own site. This allows them to charge advertisers for each view or click even though they know that they created the interaction and that it did not come from a human. Other participants in the chain participate in the cash flow stream and nobody has an incentive to complain. The website now has significant revenue from fake views. They are financially motivated to continue this fraud because the revenue exceeds the expense of operating the bots and the risk of being prosecuted is thought to be low.

- **Social Network Fraud** occurs because networks (particularly a “closed garden” variety) are paid to reach a wide number of individual consumers. The more members there are in a social network (even if the operator of the network knows many are bots) the more advertising revenue it will attract. These networks also have the ability to command a premium because of the perceived quality of their user base.

- **Geo fraud** occurs when an advertiser wants to purchase a specific number of ads per day in a particular region. Unfortunately, the agency or network provider can’t find enough spots in that location to purchase. As a result, the ads are displayed, against the instructions of the client, in other parts of the world. This is a rapidly growing issue in many parts of the world, particularly in high income, low population areas. For example, a local car dealer might request that all ads be displayed within a 20-mile radius of the dealership. The problem is that the ads are deliberately shown to people (and bots) around the world and will never help the dealer sell more cars. Unfortunately, the dealer will never know about the wasted advertising money without the use of sophisticated analytics.

- **Viewability Fraud** occurs where an ad is shown improperly such as behind a webpage and is invisible to the person viewing the real website and include:
  - **stack fraud** where ads are placed one on top of the other making most invisible;
  - **1x1 fraud** where the ad is reduced to one pixel by one pixel;
  - and a variety of other forms with the goal of packing the most number of ads into a webpage, such that as each ad is reported as viewed, increasing the revenue of the bot operator.

Bot operators are attracted to ticket vendors, travel sites, news sites and many others to scrape data and resell services, provide price comparisons, purchase items and force delays, spam and commit credit card fraud.

Who pays for all this ad fraud?

The end consumer. And the Retail Investor.

Advertisers overpay for their digital ads by $16.4 billion per year according to a study commissioned by WPP. We believe this study may actually understate the costs that are ultimately passed on to consumers and retailers. As the problem grows it imposes a significant hidden business tax. Participants in the digital ad ecosystem have clear motivation to return higher revenue and exceed quarterly expectations. By utilizing non-human traffic to view, click, like, link or join it can become very easy for the unscrupulous to earn illegitimate revenues. If those revenues were used to promote and support public investment, then ad fraud quickly can become a securities fraud issue.

A common misperception is that ad fraud is committed only by criminal networks (and perhaps the Russians). However, ad fraud is much more widespread than that and is committed willingly by a large group of otherwise honest participants in the advertising ecosystem who fall into the non-human dependent trap.

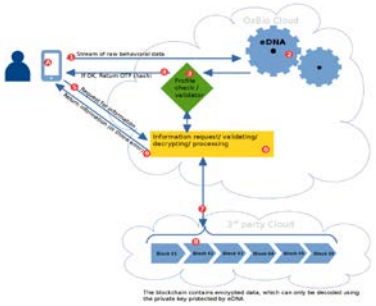
We believe that publishers and ad networks that charge advertisers for bots to view ads have defrauded the advertiser. We also believe that a social network or web operator that knowingly or willingly accepting non-human "members" has defrauded the public and their clients. While some percentage is due to faulty IP address lists, cookie misusages, bot created artificial cookies, VPN and ad blocker usage or errors in location services, the bulk is the result of intentional deception to produce additional revenue.

OXFORD UNIVERSITY INNOVATION

UNIVERSITY OF OXFORD

About Us

From our inception at the Oxford University Innovation Center OXFORD BIOCHRONOMETRICS has sought to provide the highest level of security without invading personal privacy. We will continue to build upon our proprietary technology to solve these problems, and to tackle related issues as they arise.



Our Technology

We believe that enormous opportunities in e-Commerce, digital advertising and publishing inevitably attracted nefarious players to the internet. Spam, "fake news," ad fraud, credit card theft and a corresponding loss of privacy have permeated the ecosystem on which we all rely. Policy questions include: how do you balance the good from the bad? What's the level of fraud or privacy invasion that's acceptable? We believe the answer is none.

We have developed proprietary Human Recognition Technology, (HRT) that creates a unique biometric authentication mechanism HRT+ for anyone – or *anything* – that interacts with our embedded code. OXFORD BIOCHRONOMETRICS' HRT determines definitively which interactions are human-derived and which are not, with independent studies having validated that our technology catches more fraud than alternatives that

represent the current standard. Our technology is so advanced that NATO announced OXFORD BIOCHRONOMETRICS as a winner of the agency's 2017 Defense Innovation Challenge, characterizing the technology as "transformational and state-of-the-art."

Our Solutions

Digital Media Solutions are OXFORD BIOCHRONOMETRICS products that identify non-human (bot) digital advertising fraud - these tools and services empower advertisers to ensure publisher traffic integrity and to pay only for traffic that matters.

- **SecureAd** Suite of products;
    - **SecureAd** Impressions
    - **SecureAd** for Search
    - **SecureAd** for Video
    - **SecureAd** for Agencies
    - **SecureAd** for Advertisers

Cyber Solutions are OXFORD BIOCHRONOMETRICS products that prevent fraud from happening.

- **SecureForm** (formerly **NoMoreCaptchas),** thousands of websites globally using this product to prevent spam and to block invalid user activity.
- **SecureLeads** uses Oxford BIOCHRONOMETRICS' Human Recognition Technology to verify that a human has filled out a lead/contact/signup form.
- **Secure Checkout** detects non-humans interacting with payments pages and blocks attempts at fraudulent credit card purchases.

Data

For the purpose of this report we will look at real data from a number of our clients that we have made anonymous. The selection covers the U.S., U.K., Norway, Belgium, Germany and Switzerland. All of the clients in the sample use at least one form of security to prevent bots and are targeted for distribution within the originating country.

Country		Bots	Humans	Total	%Bots
US		3,782,717	13,034,627	16,817,344	22.5%
UK		32,126,263	366,026,545	398,152,808	8.1%
Norway		1,049,077	6,603,516	7,652,593	13.7%
Germany		2,822,968	29,319,801	32,142,769	8.8%
Switzerland		1,314,620	26,989,945	28,304,565	4.6%
Belgium		7,538,878	39,879,307	47,418,185	15.9%

Our first pass shows the percentage of bots by the selected countries, but please note that as our business is largely based in Europe, that US data set is much smaller than the EU. OXFORD BIOCHRONOMETRICS will update the results as we get more US based data. In any event globally we see bot fraud at an average of 9.1 percent non-human traffic.

Next, we look at geo fraud

Country	In Target	Out of Target	Total	% Geo Fraud
US	14,572,400	2,244,944	16,817,344	13.3%
UK	391,338,470	6,814,338	398,152,808	1.7%
Norway	7,351,192	301,401	7,652,593	3.9%
Germany	31,138,234	1,004,535	32,142,769	3.1%
Switzerland	25,679,394	2,625,171	28,304,565	9.3%
Belgium	45,489,334	1,928,851	47,418,185	4.1%

The US again leads the way. These data show all activity, bot and human with the displayed ads and websites. The average geo fraud is 3%. For Switzerland, we included surrounding countries in the target calculation, thus potentially understating this fraud type.

Combining the two fraud types starts to show the bigger picture. Remember we are not yet calculating the other fraud types mentioned or hijacking.

Country	Bots and Geo Fraud	Relevant Humans	Total	Total Fraud
US	5,500,364	11,316,980	16,817,344	32.7%
UK	38,073,030	360,079,778	398,152,808	9.6%
Norway	1,126,311	6,526,282	7,652,593	14.7%
Germany	3,722,277	28,420,492	32,142,769	11.6%
Switzerland	3,701,305	24,603,260	28,304,565	13.1%
Belgium	9,090,290	38,327,895	47,418,185	19.2%

12% of all views are considered to be fraud, which easily supports the independent studies claiming the loss of $16.4 billion to ad fraud, with Statista claiming the 2018 total ad spend of $268 billion.[i] However, based on this small sampling, just these two simple frauds can claim up to $32.16 billion per year.

Where are these bots coming from?

Country	In Target Bots	Out of Target Bots	Total	% Out of Target
US	3,255,420	527,297	3,782,717	14%
UK	31,258,692	867,571	32,126,263	2.7%
Norway	824,910	224,167	1,049,077	21.4%
Germany	2,717,742	105,226	2,822,968	3.7%
Switzerland	1,100,436	214,184	1,314,620	16.3%
Belgium	7,161,439	377,439	7,538,878	5.0%

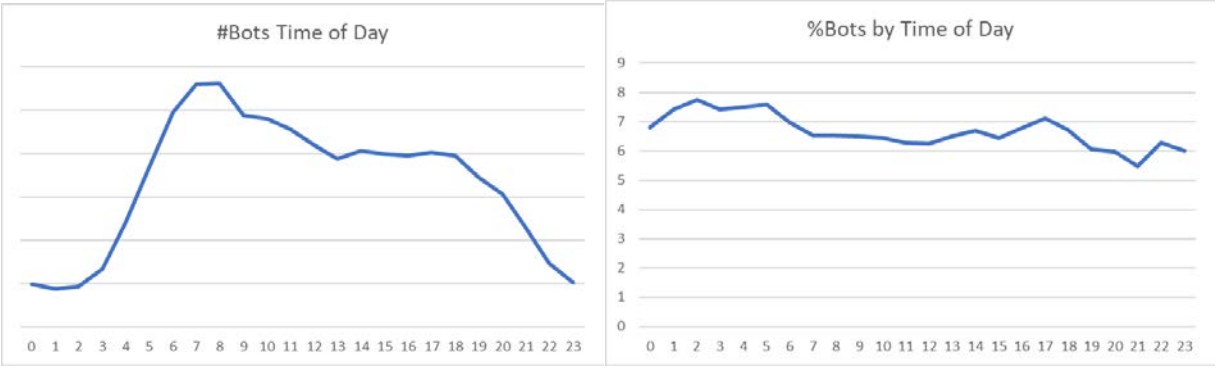
The vast majority of bots come from within country and are not external attacks.

How are these bots attacking?

device	Humans	Bots	total	
car	449	705	1,154	61.1%
desktop	131,332,627	6,966,538	138,299,165	5.0%
game console	32,613	2,671	35,284	7.6%
laptop	2,052,556	51,410	2,103,966	2.4%
phone	23,578,222	2,003,900	25,582,122	7.8%
smarttv	37,839	6,228	44,067	14.1%
tablet	13,503,425	770,846	14,274,271	5.4%

From the chart above you can see that desktops remain the most prevalent platform for the delivery of bots. However, phones have a higher percentage and mobile ad fraud is positioned to grow. It is interesting to note that bots claiming to be from cars and smart TVs have a growing percentage of activity (over 300 percent increase since the third quarter of 2017) and we can imagine it will only increase with the increase of the Internet of Things (IoT), it would be natural to speculate that IoT like smart coffee makers and refrigerators will make our list before too long.

When are these Bots attacking?



While the absolute number of Bots correlates to general human working hours, the percentage correlation is more evenly distributed.

Summary

The fraud reported here is just a small slice of the overall fraud. Policy makers should keep in mind that it generally comes from domestic sources rather than foreign agents and is distributed amongst a wide range of platforms. Ad fraud is constantly evolving.

In a future report, we will update our evolution of bots to show how the simple spam bots of the past, that are easily measured now by most ad fraud detection companies, are decreasing and more humanoid bots, that browse websites, create a history, are able to fill in forms and simulate mouse movements, are becoming more prevalent.

Older generation technology has moved from protecting the advertiser and consumer to protecting the networks, agencies and publishers. Nonetheless, these same companies and groups claim that fraud is decreasing. What is decreasing is their ability to detect the continually advancing threats. While our solutions cannot entirely prevent fraud, we can report and audit very effectively. In our experience, clients actively using our prevention techniques and use the data to remove outliers continually see improvements and reduce the price of the hidden tax.

Constant vigilance, best of class fraud detection and remediation will help to reduce ad fraud and associated costs to consumers and businesses. All players in the market need to be held accountable – networks, agencies, demand side and supply side platforms and publishers – but it must start with the advertisers themselves to demand accountability and proper auditing.

[i] Digital advertising spending worldwide from 2015 to 2020 (in billion U.S. dollars), statistica, https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/.