

DSTILLERY HYGIENE PATENTS

MINIMIZE WASTE WITH CLEAN AND ACCURATE AUDIENCES

“IT’S A CAPITAL MISTAKE TO THEORIZE BEFORE ONE HAS DATA.”

clean

Wasted money and misguided optimizations based on fraudulent traffic plague digital marketing. As high as 15% of ad traffic in the US is reported as fraudulent.

Dstillery invented multiple patented solutions to build audiences based on data an advertiser can trust. Our data-cleansing solutions work together to ensure advertisers do not waste money on non-humans or inaccurate data.

WHAT DO DSTILLERY’S HYGIENE PATENTS DO?



DYNAMIC FRAUD DETECTION

Patents Granted
[May 2014](#) | [Apr 2016](#)

Identifies websites with suspicious traffic



PENALTY BOX

Patents Granted
[Apr 2015](#) | [Aug 2015](#)

Quarantines suspicious IDs (bots) from audience building and ad delivery, even on legitimate sites



LOCATION AUTHENTICITY

Patents Granted
[Apr 2018](#) | [Feb 2019](#)

Identifies and eliminates inaccurate geospatial data infiltrating the mobile app ecosystem via fraud, sloppy app developers, or intentionally obfuscated locations

DSTILLERY HYGIENE PATENTS

MINIMIZE WASTE WITH CLEAN AND ACCURATE AUDIENCES

HOW DO WE DO IT AND WHAT MAKES IT SPECIAL?



DYNAMIC FRAUD DETECTION

We look at patterns in website co-visitation. We flag sites as compromised if many unrelated sites have high traffic overlap. And we do this continuously since ad fraud is dynamic.

Our method is agnostic to fraud type, detecting sites built for fraudulent purposes as well as legitimate sites temporarily compromised by forced traffic.



PENALTY BOX

A device that behaves like a bot is placed in a penalty box. If after some time the device proves its innocence with non-suspicious behavior, it can be released.

The standard broad brush approach permanently blocks suspicious IPs. While catching some fraud, this misses more complex schemes using residential IPs or temporarily compromised devices. Our nuanced approach eliminates fraud at the individual device level. Compromised devices stay out of our audiences and seed data for modeling.



LOCATION AUTHENTICITY

We evaluate the quality of data sets as a whole. We look at spatial distribution of data to identify signatures of inaccurate location data and also compare with web and app behavioral data.

Our location-based audiences reflect the reality of user locations for more effective targeted messaging and clearer insights. By cross referencing location data with related app and web behaviors, we develop and validate sophisticated lat/long filters that go beyond filtering out obvious geographic centers.