

Proposal:

Where discrepancies are found between 1st and 3rd party reporting, Canoe's internal reporting should be used as a "currency" to ensure that ad agencies do not lose faith in the cable operators delivery of managed services as a unique delivery ecosystem held apart from unmanaged internet based video services as OTT and CTV.

Background:

Starting in 2011, Canoe now provides DAI and service assurance for the QAM and IP based Set Top Box VOD ecosystems of Charter, Comcast, Cox, and Frontier.

Access to VOD on these systems is gained only by subscribers authenticating to the MVPDs' closed networks. Canoe's platform operates similar to a Server-Side Ad Insertion (SSAI) platform where the player itself (e.g., a set-top-box in a viewer's home) is not tasked with issuing beacons. Instead, the set-top-box forwards impression details to centralized platforms that are then responsible for firing any applicable impression or quartile beacons.

All beacons fired for the Canoe footprint purposely contain no PII, a requirement dictated by each of Canoe's Distributors Security Policies – that is the beacon cannot contain device, household, or user-specific data. Canoe's beacons, which are fired on behalf of Google Ad Manager (GAM) programmers, are always issued from the same IP address (208.42.224.132). FreeWheel (FW) also fires beacons for impressions that occur on the Canoe footprint, which originate from a consistent block of FW AWS IP's. For 2016, the MRC reviewed and provided accreditation for the Canoe QAM STB VOD/DAI system. During that audit process, Canoe provided an on-going review of traffic analysis used internally to detect IVT. At the time, the number of suspect events occurring which may have been invalid impression traffic was so significantly small that it was determined to be non-impactful. In the past, VOD delivered in the context of the MVPD's authenticated, Title 6 Video service has not been subject to any of the fraud claims that affected other OTT/CTV or non-authenticated streaming VOD services. Canoe's platform was built in accordance with the MVPD's obligations established in the Cable Act of 1992 which prioritized the integrity of consumer data by severely limiting what could be exposed outside the cable operators' network for Title 6, managed video and data services.

For the past 18 months, Canoe has worked with several companies (e.g., Innovid, Extreme Reach, Double Verify, IAS, MOAT) as recipients of beacons being transmitted for the Canoe VOD/DAI footprint. As agencies and advertisers have begun to rely more and more on reported beaconed events as reported by these companies, Canoe has become a member of both TAG and IAB in order to insure Canoe maintains a current and correct understanding and interpretation of their beacon-related specifications.

Occasionally, some but not all of these companies will flag Canoe traffic as Invalid Traffic, either designated as General Invalid Traffic or Sophisticated Invalid Traffic. As Canoe works through the details with each of these companies it is generally determined that this is due to the lack of PII in the received beacon by the reporting company.

Flagging of Canoe traffic as IVT has adverse effects on Canoe's programmers, many of which rely on the 3rd party reporting to invoice their customers. These programmers are seeing sporadic IVT rates of up to 24% per day for campaigns that are utilizing 3rd party vendor tags. Once flagged, the path to resolution has taken anywhere from one to four weeks depending on the responsiveness of the agency. During this period, the measurement agency continues to falsely flag valid impressions, despite confirming no fraud occurred and garner approval of the IPs or User Agents. The resolutions are never retroactive, and the programmer's revenue is therefore adversely impacted. In speaking with programmers on the Canoe footprint, their grievances can be summarized in three points:

1. Agencies unwillingness to pay invoices in full due to seeing variances in 3rd party reporting.
2. Programmers are not able to see they are not on track to fulfillment of campaigns at any point throughout flight window due to IVT. To reach stated goal they are forced to waste additional inventory to reach their campaign goal and proactively account for IVT.
3. Programmers understand the Canoe ecosystem is a fraud-free environment, but they can no longer utilize Canoe inventory as a fail-safe against under delivery of other platforms such as digital or mobile.

Canoe's hope is to respond to these pain points by moving forward with a fail-safe to 3rd party reporting: in cases where discrepancies are found between 1st and 3rd party reporting, Canoe's internal reporting should be used as a "currency" to ensure that ad agencies do not lose faith in the cable operators delivery of managed services as a unique delivery ecosystem held apart from unmanaged internet based video services as OTT and CTV.