Security Solutions

White Paper

neustar

Cracking Down on Password Sharing?

IP Intelligence and Human Insight Can Help

LIVE STREAMING
PLAY

Password sharing is costing providers of over-the-top (OTT) content big money—at least $2.3 billion a year for Netflix, according to a recent study by Cordcutting.com, and an estimated $1.5 billion in 2018 for Hulu, according to a CNBC report.

For content providers that want to limit password sharing, spotting—and then acting on—suspicious activity means making tough decisions, like how to balance customer experience with effective enforcement within constraints that are often set by external entities. For many forms of digital media, strict guidelines have been established that govern where, when, and how content can be legally consumed, and by whom. A live-streaming baseball game might be blacked out for certain markets, for example, and movies and TV shows may be licensed for viewing only in certain countries, while local broadcasts may be designated for viewing by city, ZIP code, or designated marketing area (DMA).

If your company decides to immediately block suspicious users until you can verify their locations and identities, this could have unintended negative consequences. An authorized user trying to sign in from an atypical location or network might react with concern—and make a costly call to customer service. Or worse, these frustrated users could take their business elsewhere.

Neustar is here to help with our IP Intelligence family of decisioning data that includes our IP GeoPoint and IP Reputation services:

- IP GeoPoint provides IPv4 and IPv6 geolocation data on over 99.99% of the world's routable IP addresses.

- IP Reputation equips content providers with two powerful scores to help determine whether an IP address is likely to be a human user or a bot, or if the address has previously been associated with risky behavior.

Supporting both data sets is a team of dedicated network geography analysts. These analysts are involved in every stage of the data collection and analysis processes, from researching location and network references and assuring quality post-data synthesis to reviewing "geo-feedback" from customers and partners.

For years now, Neustar has provided granular IP (internet protocol) geolocation and risk data to OTT and streaming media providers. Our data has enabled providers to identify and enforce content restrictions, flag suspicious logins, and track user connection characteristics, such as the use of a virtual private network (VPN) anonymizer. In this white paper, you'll find recommended best practices for using IP Intelligence decisioning data, analytics, and human insight to address password sharing in a way that achieves both regulatory compliance and customer retention.

1

LEARN LOGIN LOCATION

Strategic login oversight starts with IP geolocation data. This data connects a user's IP address with associated geographic location information: where they are logging in, how they are connecting to the internet, and more.

IP geolocation decisioning data helps you set your organization's rules for allowing access and establishing criteria for suspicious behavior—so the more granular this data is, the better. Neustar, for example, collects over 40 attributes* for each IP address, including country, state, city, postal/ZIP code, time zone, type of organization, and DMA. We're also able to identify whether the IP address is associated with anonymous proxy activity and whether the IP address is originating from a hosting facility or a residential location.

To enforce password sharing guidelines, you'll want to use the most robust IP geolocation data available. This ensures you can accurately locate your users and identify logins originating from alternative locations, which may indicate password compromise.

*Not all fields are available for IPv6

CONSIDERATIONS

In order to be actionable, IP geolocation data must be fresh, precise, and accurate. Here are a few things to consider:

- **How often is the data updated?** Neustar updates our IP geolocation database on a weekly basis. This allows us to keep up with streaming media companies that are adding vast numbers of new subscribers every month.
- **What level of granularity is needed?** Some content providers need to know only the country in which the IP is located. Others require city, ZIP code, or Nielsen DMA detail.
- **Are your data analysts up to speed on the latest regulatory mandates and licensing requirements?** You don't want to block users from a newly added location or allow access from an area where licensing rights have just expired.

2

MANAGE ANONYMOUS USERS

To complicate things even more, some users consume content through a VPN or proxy server. This masks their originating/assigned IP address and allows these users to log in anonymously. In many cases, proxy use is perfectly legal. Examples include a company's VPN or a public service for anonymous browsing, such as Tor. However, when someone uses a proxy server to mask their location for the purpose of evading geographic boundaries, their action may violate terms of service or content viewing restrictions. In some cases, the action may be prohibited.

Location masking complicates the determination of password sharing. **If you can't assess the location from which your users are logging in, it makes it difficult to identify fraudulent logins** from alternative locations.

Neustar developed our IP decisioning data with both known and anonymous users in mind. The granular IP and internet connectivity data of IP GeoPoint lets media providers create rules to both "geo-authenticate" users and "geo-fence" their content if necessary. This blocks unauthorized users from connecting from outside of an approved area.

CONSIDERATIONS

Should you let proxy users connect to your service? There are pros and cons. If you allow an unauthorized anonymous proxy user, you risk failing a compliance audit. But if you block all proxy user logins, your customer retention numbers could drop.

Neustar suggests content providers:

- **Scan network connections for the presence of a mobile gateway.** Then route visitors originating from a mobile data connection through one of their carrier's nodes, well outside the viewing radius. Request an additional location check for mobile gateway traffic to confirm if the user should be blocked from content.
- **Filter users who frequently access content via a public proxy or VPN.** If you know, based on their history and connection profile, this subscriber typically connects from a proxy or VPN, there is no need to flag them for review.
- **Flag anonymous proxy users.** Use the type and level of anonymous proxy browsing associated with a specific IP address to flag suspicious behavior.
- **Use secondary authentication techniques (SMS, KBA)** for users logging in from VPNs and proxies. This ensures you truly connect with authorized end users.

3

TRACK “TYPICAL” BEHAVIOR

IP addresses and proxy server usage all factor into user profiles, contributing to digital histories of typical activity for a given subscriber. User histories are always in flux. However, **by establishing a geo-footprint or baseline for “normal,” these profiles help you flag anomalies** that could be indicative of password sharing—for instance, when a user based in San Diego suddenly logs in from Singapore.

CONSIDERATIONS

User profiles can be a powerful tool for weeding out bad actors while avoiding unnecessary blocks on legitimate users. You can use these profiles to:

- **Keep historic records of where users log in**.
  If a login deviates outside of “normal” patterns, you may want to flag it for additional review.

- **Capture and store a user’s consistently visited locations.**
  If your subscriber logs in from both Los Angeles and New York City on a regular basis, you can consider this “normal” behavior and avoid unnecessary challenge questions.

- **Flag and filter users who are frequent travelers.**
  For example, if your subscriber logs in frequently from several locations in the United States, as well as from Canada and Europe, this can be flagged as their “normal” behavior. Only when the subscriber deviates from this behavior, would it be necessary to flag the account for a secondary review.

4

MONITOR THE LANDSCAPE

A velocity check is another way to spot atypical activity. Fraud prevention platforms often use these checks to flag changes in a user's location that happen in an unrealistically short amount of time. Take, for example, the San Diego subscriber in our previous example, who logs in from California in the morning and Singapore at lunch. Because it's impossible to fly across the Pacific Ocean in only a few hours, this user would likely be flagged for further review.

CONSIDERATIONS

Neustar IP Reputation assigns a risk score to an IP address. On a scale from 1 to 100, **how likely is the IP address to be associated with suspicious behavior?** The higher the number, the more likely the IP has been associated with malicious activities, like credential stuffing or an account takeover to mimic and defraud your actual subscribers. For another layer of risk insight, IP Reputation also assigns an IP address a Real User Score, which is a ranking from 1 to 5 on how likely the IP address is to be associated with non-human traffic, such as a bot. The higher the score, the greater the likelihood of illicit activity.

You can use these insights to narrow in on unauthorized users who have exhibited risky past and current behavior, as well as countries, cities, and networks where unauthorized access has been detected or is prone to happen.

5

ENGAGE BEFORE YOU BLOCK

It’s easier and far less expensive to retain a current subscriber than to acquire a new one. For this reason, **OTT content providers need to be cautious about “blanket blocks” of all suspicious password-sharing activity.**

Legitimate subscribers don’t want to see “access denied” when logging in for a long-anticipated game, show, or movie. And they certainly don’t want to feel like their OTT or streaming media content provider is scolding them or accusing them of prohibited activity.

CONSIDERATIONS

Rather than assume bad behavior at the outset, gain further insight through “soft enforcement.” For instance, we recommend:

- Dialogue that assumes legitimate behavior (“We saw you logged in from a different location.”)
- Message of concern (“We want to make sure your account wasn’t hijacked.”)
- Request for verification (“Please confirm your user ID and password.”)
- Deadline for further action (“For your security, we are placing a block on your account for the next 48 hours due to suspicious login activity. If you feel this is incorrect, please contact our customer care team to verify your identity and to help us ensure that your account has not been compromised.”)
- Considering challenge questions or additional queries for identity verification when a user logs in from a new location. These can be simple questions to verify the subscriber’s identity. For example: “We noticed that you are logging in from a new location. To confirm your identity, please select the correct answers to the questions below.”

FIGHT PASSWORD SHARING THE SMART WAY WITH IP INTELLIGENCE DATA

Although the login for a premier sports package may spread across an office or a Netflix password may migrate from a roommate to a classmate to a boyfriend's cousin, content providers still have more control than they might think in the fight against password sharing.

With the right decisioning data and tools, you can strengthen your ability to identify suspicious activity and set effective access criteria and rules. But you'll also need humans—specialists who've been there and seen it all—to verify IP locations and attributes and to make sense of internet traffic patterns and more. These specialists will be able to collect and decipher risks, identify the red flags deserving of a customer prompt, and know when to follow up with further action.

For gaming, movie and TV subscriptions, premier sports access, and beyond, Neustar can help your company find the best way to prevent unauthorized password sharing.

LEARN MORE

To learn more about how Neustar IP Intelligence decisioning data can help you accurately deliver your OTT content, click here, or call us at 1-855-898-0036 in the US and at +44 1784 448444 in the UK.

About Neustar.

Neustar, Inc. is a leading global information services provider driving the connected world forward with responsible identity resolution. As a company built on a foundation of Privacy by Design, Neustar is depended upon by the world's largest corporations to help grow, guard and guide their businesses with the most complete understanding of how to connect people, places and things. Neustar's unique, accurate and real-time identity system, continuously corroborated through billions of transactions, empowers critical decisions across our clients' enterprise needs.

More information is available at

www.home.neustar