Cartesian®

How Consumers Access Streaming Video

The Risks of Credential Sharing – SURVEY REPORT

Introduction

Protecting TV and video content distribution against piracy is a major preoccupation for companies within the media and entertainment sector. Over-the-top (OTT) video streaming makes content security more complex as the internet spawns new forms of piracy and ways for consumers to "freely" access content.

An area of increasing concern is credential sharing – when a viewer uses someone else's account ID and password to access a streaming video service. Sharing passwords isn't anything new, nor is it a surprise. OTT video service providers used the practice successfully as a marketing strategy to win viewers.

However, with increasing competition, slowing subscriber growth rates and rising concerns about personal data security, not caring about sharing is to the detriment of legitimate content distribution.

To highlight this issue, Cartesian recently conducted a survey to see how today's consumers are currently accessing streaming video content and their attitudes towards sharing account credentials.

Referencing survey results and drawing from our work in analytics and content security, this report:

- Reveals consumer viewing habits and attitudes towards video services access
- Explains credential sharing in the context of piracy and content protection
- Defines unwanted credential sharing and its three main types
- Examines the risk to content owners and service providers, and
- Outlines an approach to track, stop, and prevent unwanted sharing activity, while minimizing negative impact on customer experience.

Our Survey

In November 2018, we conducted an online survey. 1,183 American consumers participated: 40% of respondents were between the ages 18-34, 42% between 35-64, and over 65s made up 16%. Under 18s were less than 2% of responses.

Our participants represent a broad scope of households where 40% live with a partner, 28% live alone, 22% with children, 15% with parents or guardians, 9% with friends or roommates, and 5% noted other living arrangements.

Key Findings

27% 27% access video services using account details from someone outside their household.

28% 28% share their account credentials with someone outside their household.

68% Of those who use shared credentials, 68% obtain them from a close friend or non-household family member.

15% 15% of those who use shared credentials obtain them from an acquaintance or someone they don't know personally.

27% Of those who use shared credentials, "It is an easy and convenient way to access content" was the main reason for 27% of them.

42% 42% of people who use shared credentials to access content would consider paying if they no longer had access for free.

Content protection made more complicated by streaming video

Content Piracy

Most of us spend a considerable amount of time watching TV and streaming video. With "TV Everywhere", we don't just watch from the set in our living rooms but on laptops, tablets, and mobile devices, and in any room in our homes, our modes of transport, and public spaces.

As much as service providers seek to fulfill our demand to watch what we want, when we want, and how we want, we don't always *want to pay.* "Free-for-view" is enticing and often too easy. If we didn't have access to desired content on our current services, according to our survey one in five (18%) would choose to gain access through free online streams (piracy).

Stopping content piracy has long been fought for by content owners and service providers. Content owners, video service providers, regulators, and law enforcement all work to dissuade and stop piracy, and although they find success, the fight is never-ending.

The growth of over-the-top (OTT) video streaming makes content protection more challenging and complex. The traditional battleground for the fight between operators and pirates was the set top box, and the smartcards allowing access to premium content. This battleground is now being bypassed by the ease with which content can be shared on the internet.

Companies use a wide range of technology and detection techniques, such as watermarking and geo-blocking, to track and stop unwanted and illegal access to valuable content in this ongoing piracy game of "cat-and-mouse".

Credential Sharing

Adding to the fight between paid and pirate viewing is shared viewing via shared user IDs and passwords (i.e. credentials) to subscriptions for streaming video services.

Up until recently, credential sharing was an overlooked grey area in content protection, mainly for marketing reasons – as a survey respondent commented, sharing is okay "so someone can try before they buy". Allowing sharing was a strategic route for OTT streaming video services to win future subscribers, and indeed it has been successful.

As the industry is maturing with more OTT competition and slowing subscriber growth rates, credential sharing is no longer a safe strategy.

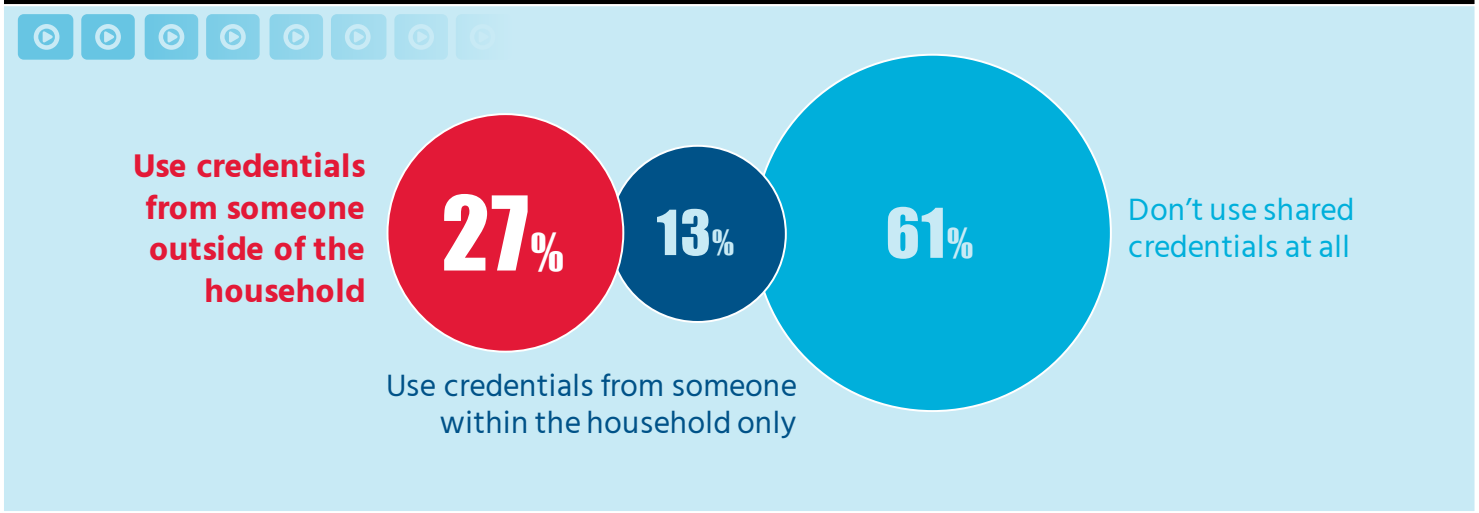
For example, it was reported in November 2018 that despite Netflix having 147.5 million US consumers using its platform in 2018, the company only reported 58.4 million subscribers in the third quarter[i]. The huge difference in number is thought to be because many Netflix users don't own a subscription and instead use a friend or family member's account.

In our survey, 27% of respondents admit to using account credentials from someone outside their household to access video services and 28% admit to letting someone outside their household use their account credentials to access their video subscriptions.

Previous tolerance may actually have led to damaging relaxed consumer attitudes.

As one respondent commented, it's okay to share streaming accounts because they're "not blocked from it", and another noted that the content is "streamed, not downloaded and kept".

Use of others' credentials: Percentage of respondents who...



If you did not currently have access to the appropriate service for a title you were interested in, what alternatives would you consider?

("Select all that apply")

52%	32%	31%	19%	18%	18%
Pay for the service myself	View it at a friend's	Not view it	View it in a public place if available	Try and borrow someone else's password	Use free online streams (piracy)

The risk of the extended network

Not all credential sharing is considered unacceptable. For example, 36% of respondents in our survey only share account credentials with someone in their household.

Consumers and streaming service providers generally agree that it makes sense for people who live together to share services. Service providers' terms of service typically allow members of the same household to use and share a single account.

The concern is primarily with sharing activity beyond the household. As one survey respondent commented "It's okay to share, but not with anyone who doesn't live with you. That's like stealing."

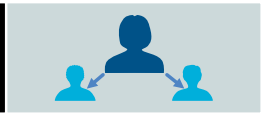
Often, sharing extends to non-household relatives, close friends and even to people that subscribers don't know very well, and sometimes without the account holder's knowledge or permission.

We define credential sharing as sharing an account's access details with someone outside of the household for which the subscription was purchased.

In our survey, two out of three (68%) sharers admit to obtaining account credentials from a close friend or non-household family member.

Cartesian sees three main types of sharing outside the household:

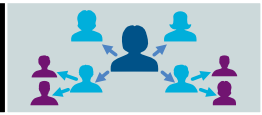
1 Family & Friends



This is sharing account details with family, partners, close friends, and includes students (e.g. children living away from the main household).

Typically, sharing is for a specific piece of content, but access is often maintained beyond the original intention.

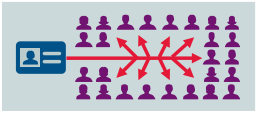
2 Extended Network



Extended network sharing is often the result of third-degree sharing: you share with one person (e.g. family or close friend) who shares with another. It also refers to sharing with colleagues and acquaintances.

Third-degree sharing can result in many users – some without a link to the account holder – having account access. Also, the account holder may not have consented or is even aware that someone is using their account.

3 Buying/Selling Credentials



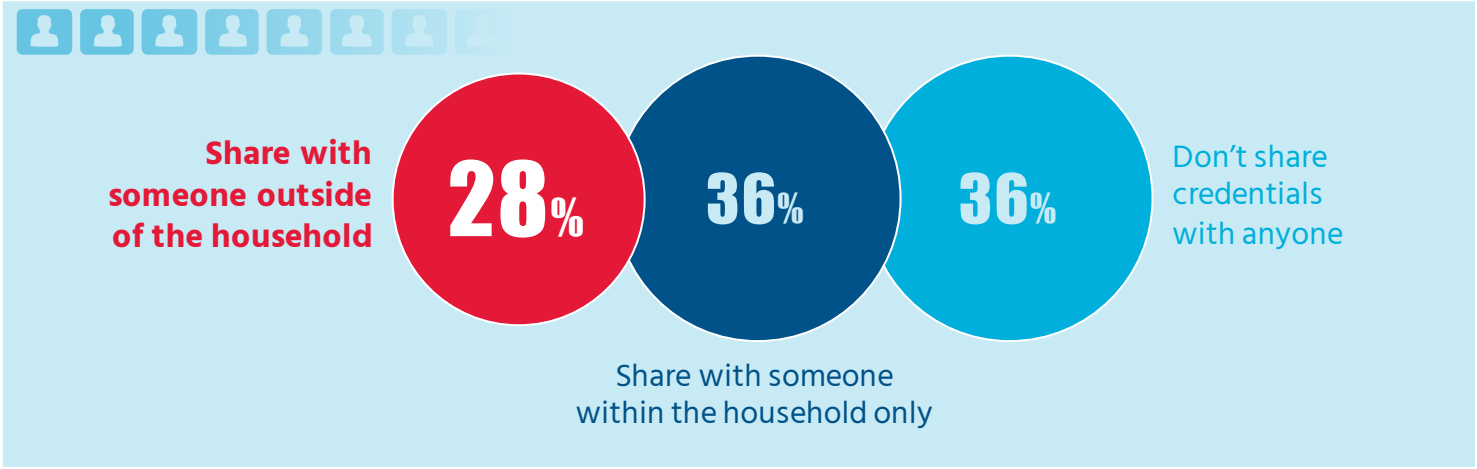
Account subscription details are being purchased and sold through various websites and other means. Although this activity is not common and more often found where a service provider's platform restrictions are fairly relaxed (e.g. no device limitation), it can have a significantly disproportionate impact on usage.

Any of these types of sharing activity can also be the result of credential theft (sharing without the permission of the subscription account holder) whether done intentionally or not.

In our survey, although only 8% of sharers say they share with acquaintances, half of them (48%) admitted to allowing a partner they don't live with use their account subscriptions. In addition, 43% say they would share with a non-household family member and 48% with close friends, if asked.

Although company policies have tightened up on account sharing, as our survey suggests, a significant number of viewers borrow or allow other people to access their subscription.

Sharing with others: Percentage of respondents who...



Who do you currently share with outside of the household?

("Select all that apply")

Acquaintance	8%
Close friend	27%
Non-household family member	42%
Partner (non-household)	48%
Someone not known personally	3%

Industry Impact: Missed opportunities and increased costs

Companies should consider the business risks associated with credential sharing and theft:

Excess Operating Expenses

A disproportionate share of streaming video usage is associated with sharers. These non-paying users strain infrastructure and can substantially increase operating costs as well as negatively impacting customer experience. For example, sharers can result in viewership spikes for live events and shows, which may cause delays and even outages. One non-sharer in our survey thought that it isn't okay to share streaming accounts because "it drives up the cost for paying users".

Complex Rights Negotiations

Credential sharing impacts the perception of value for content, affecting content licensing negotiations. Put simply, for service providers, value is based on what they can monetize; for rights owners, value is based on how much their content is consumed. Unchecked credential sharing and theft adds increased complexity into critical value negotiations.

Content Agreement Violations

A typical content agreement includes clauses related to anti-piracy, geo-filtering, watermarking standards, and other security measures. Increasingly, policies to limit credential sharing are of greater interest within these agreements and are being explicitly referenced. Inadequate controls put content providers at risk of violating these agreements.

Customer Data Security Gaps

One of our survey respondents wouldn't share their credentials "because it's unsafe". Yet, many consumers are unaware that they risk exposing their private data when sharing passwords. Sharing account details can give access to other data such as payment details and other personal information. One password may also be the gateway to access their other personal accounts.

Anyone with account credentials can access sensitive customer and billing information, e.g. name, address, credit card details etc. Government regulation is changing, e.g. strong penalties in place with the EU's GDPR, putting the onus on businesses to safeguard against data breaches. Allowing credential sharing activity to occur – particularly in cases where it is not always with the consent of the account holder, such as in third-degree sharing – could leave video services at risk of data security violations.

Lost Revenue Opportunity

Many individuals who use shared credentials are willing to pay to access the content they want. In our survey, 42% of those who use shared credentials from someone outside of their household would consider paying for the content they are accessing.

With the proper incentives and disincentives (e.g. access restrictions), it is possible to convert a significant portion of sharers. 1 in 4 sharers (27%) say the main reason they do so is because it's easy and convenient. One sharer commented, "I pay for services when they're more convenient than finding another avenue".

Also, in our survey, two out of ten (21%) say the main reason is because the content they want is not available on current services, "It gets ridiculous to pay for them [streaming services] all yourself when you want to watch one show".

By ignoring credential sharing and the reasons why, companies miss the opportunity to convert these consumers into paying customers.

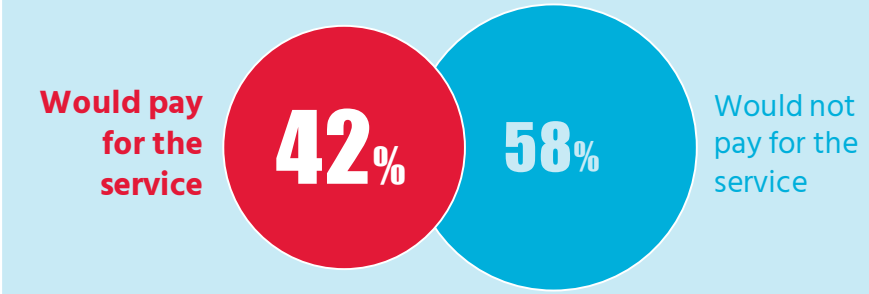
Credential sharing and theft has five negative impacts on providers

LOST REVENUE	EXCESS OPERATING EXPENSES	COMPLEX RIGHTS NEGOTIATIONS	CONTENT AGREEMENT VIOLATIONS	CUSTOMER DATA SECURITY GAPS

Top reason for using someone else's account to access content

52%	27%	21%
"I already pay enough"	"It's easy and convenient"	"Content I want is not available on my service"

Paying for services: Percentage of users of out-of-household credentials who...



The trade-off between security and consumer expectations

It may seem that the easy answer to prevent credential sharing is heavily restricting access. Indeed, many service providers have recently tightened up on account sharing with policies such as restricting the number of devices, geography, content, and concurrent streaming.

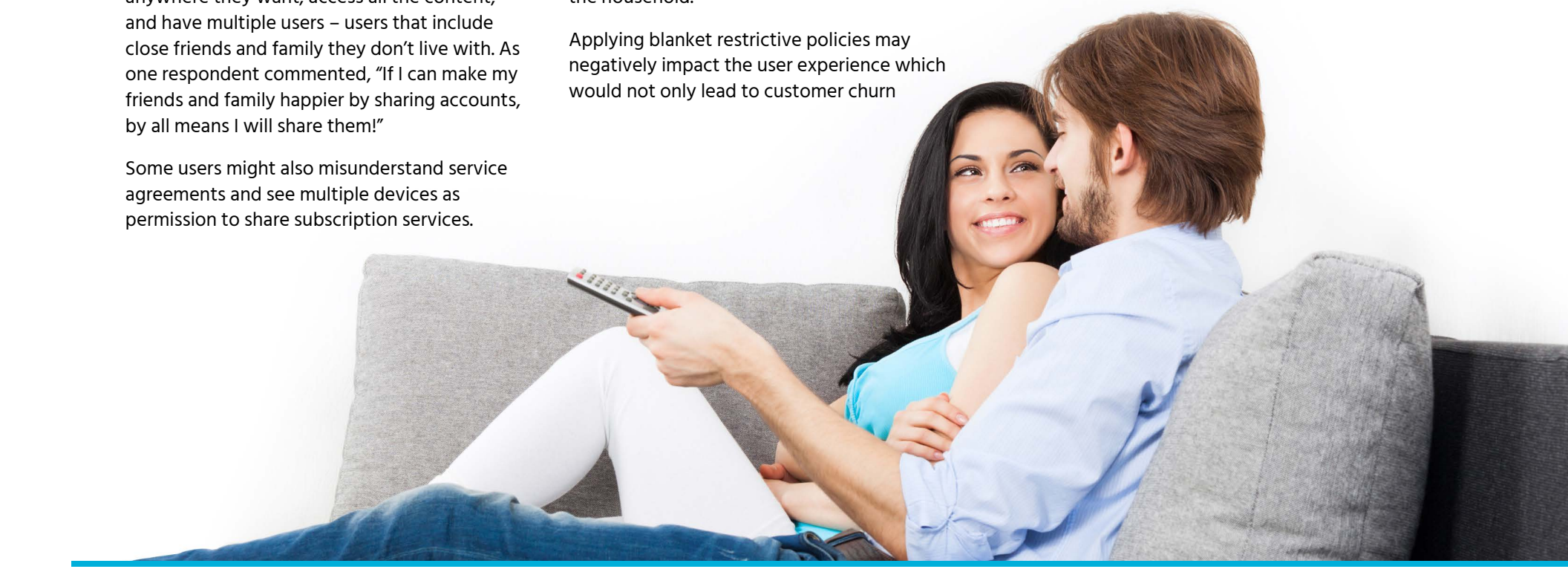
However, consumer expectations, fueled by the concept of "TV Everywhere", are that they should be able to use any device, watch anywhere they want, access all the content, and have multiple users – users that include close friends and family they don't live with. As one respondent commented, "If I can make my friends and family happier by sharing accounts, by all means I will share them!"

Some users might also misunderstand service agreements and see multiple devices as permission to share subscription services. "I pay for two screens, so therefore I feel it's ok to share my extra screen with a close family member".

However, it's important to note that most account sharing occurs only within households (as allowed), and a significant number of subscribers do not share, nor do they intend to. In our survey, 72% of subscribers do not share account subscriptions at all or only share within the household.

Applying blanket restrictive policies may negatively impact the user experience which would not only lead to customer churn but viewers to turn to piracy. For example, restricting location and content could see a rise in geo-filtering via VPNs.

Instead, service providers and content owners need solutions that seek to protect account access and the user experience. Is there a way to achieve both?



Who would you share with outside of your household, if asked? ("Select all that apply")	
Acquaintance	3%
Close friend	48%
Non-household family member	43%
Partner (non-household)	65%
Someone not known personally	2%

The trade-off?

Content providers appear to be faced with a trade-off between platform security and building an experience that meets increasing consumer expectations.

Using data science for targeted action

Making general platform restrictions is not the answer to uncontrolled credential sharing if companies want to meet and exceed growing consumer expectations. Like the solutions to pirate activity, taking targeted action is.

Unlike many forms of piracy, service providers can track and evaluate sharing behavior using the information they already have.

The kind of analysis needed goes beyond simple account-level metrics such as looking at the number of active devices or activity to identify sharing accounts. Like general platform policies, a simple approach will fail to capture the nuance involved in many cases.

For example, take a household of a family with two working adults and two young children. Their viewing footprint could look like:

- Watch at home on a TV screen
- Use two tablets for traveling (e.g. for kids on a long journey)
- Use individual laptops to view content, both in and out of the home
- Occasionally cast to a TV at someone else's house
- Occasionally watch content on mobile devices

All this usage is legitimate. But a simple analysis of this data would register a high number of devices and so activity may be classified incorrectly as illegitimate.

To capture nuance, companies need data science that leverages the vast amount of information captured by their video services and that combines machine learning with behavioral analysis.

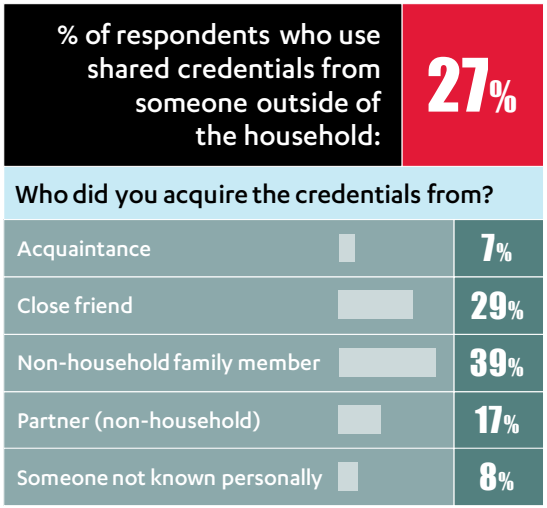
Potential fraud indicators include out-of-home devices, geographically dispersed activity, out-of-home streaming volume and repeat device types.

In our survey, of those who share account details with others, one out of three (28%) share with someone outside the household – not legitimate use for most subscription contracts. When analyzing viewing information, additional signals could indicate sharing with a non-household viewer. In our family example, we can use these potential red flags:

- Watching from a TV screen at another location becomes regular
- Viewing live programs concurrently in multiple locations
- Repeated content streams

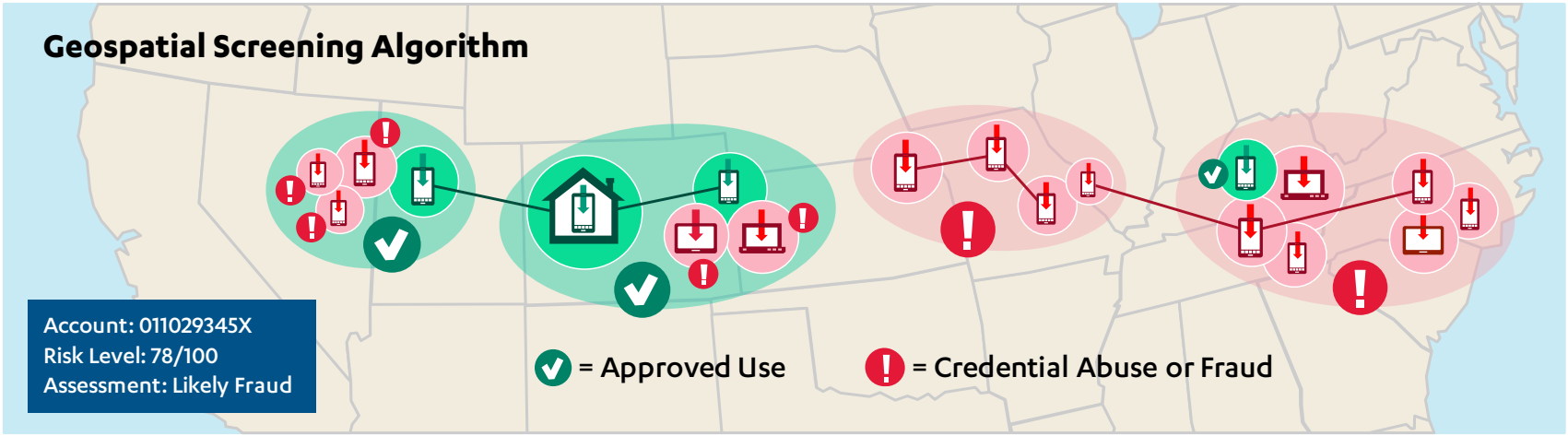
Using combinations of multiple signals, service providers can better track and evaluate usage patterns and discrepancies to create a holistic view of sharing on an account. From here, they can select accounts and match them to the appropriate action.

All this information is legitimately gathered for a service provider to effectively deliver a video service. In the same way they use it to improve services and the user experience, they can leverage the data to deter credential sharing abuse and identify account theft.



Identifying sharing activity

Video services collect vast data that contains valuable signals to help determine which activity is legitimate or likely abuse or fraud.



- IP Address
- Network Status
- Device Identifier
- Content Title
- Geo-Location
- Known VPN IPs
- Device Type
- Viewing Duration

Conclusion

The fight to protect content distribution has a new challenge in the form of credential sharing. What is clear is that credential sharing is no longer the safe subscriber strategy for new and old players alike.

Consumers share their video streaming subscriptions a lot more freely than companies might believe – and it certainly has consequences.

Ignoring credential sharing activity puts businesses at risk for increased costs, service quality issues, litigation, security breaches, and revenue opportunity loss.

Alarmingly, subscription fatigue is rising, where many consumers do not want to pay more for content, "There are so many different ones to pay for that it gets ridiculous to pay for them all yourself when you want to watch say one show on Amazon and one show on Netflix and then the other show you like is on Hulu. Makes sense to share with people you know to save money for you both."

With more online video services launching in the US and elsewhere, will this drive competition amongst legitimate services or push consumers to piracy or to share accounts?

Yet there are sharers who are willing to pay and either lack the incentive to do so or find that borrowing credentials is an easy alternative. There is hope yet for companies to convert these viewers.

Applying blanket usage controls is a solution but not a satisfying answer. They seem out of place in the world of "TV Everywhere" with the push for ubiquitous connectivity and numerous connected devices.

Like fighting piracy, detective work is needed instead, aided by effectively using data science and machine learning. Video service providers can identify issues with the viewing information they already have and take appropriate action to reduce unwanted sharing activity.

Credential sharing is a problem that has gone on unchecked for a long time. The solution to curb account sharing abuse and fraud lies within viewing data, and it is up to video service providers to take the lead. <>

Find out more about Cartesian's Streaming Video Credential Sharing Detection & Prevention Solution

About Cartesian, Inc.

Cartesian, Inc. is a specialist provider of consulting services and managed solutions to leaders in the global communications, technology and digital media industries.

With over 25 years of experience assessing and delivering solutions for the media and entertainment sector, we offer a holistic approach to content security. Cartesian's content security services include anti-piracy services, security consulting, the Farncombe Security Audit™, and streaming video credential sharing detection and prevention services.

Cartesian's Streaming Video Credential Sharing Detection & Prevention Solution:

- Integrates with existing TV Everywhere and OTT platforms.
- Screens for all relevant credential sharing and theft patterns, leveraging proprietary and industry-leading clustering and geospatial dispersion algorithms.
- Provides lists of accounts that have been compromised and an ongoing platform-wide health check.

Cartesian's clients include TV broadcasters, video service providers, equipment vendors, and network operators. The company has offices in Boston, Kansas City, London, New York and Paris.

For more information, visit www.cartesian.com.

Cartesian®

[i] "Netflix to surpass 147 million viewers in US by end of year", The Wrap, November 2018

Protect your streaming video service and
detect and prevent credential sharing

Cartesian®