

“Why OTT Bypass Could Kill Voice Revenues”

Introduction

Ubiquitous communications technologies have provided impetus for widespread adoption of mobile Internet access. The mobile Internet has given rise to a plethora of over-the-top (OTT) applications. It is difficult to ignore the dramatic impact of OTT players on mobile operator (MNO) revenues. Effectively, the OTTs transit operator facilities via the edge of the network without compensating for apportioned infrastructure development costs nor other industry related taxes, fees or regulation oversight, such as the recent Title II decisions by US federal courts. Recent advancements have made many seasoned telecom veterans ponder this cause and effect on their operations and revenues.

OTT applications have greatly increased data usage and revenues from the exponential spike in traffic and the operators are clearly benefitting. Pricing of data plans obviously has a huge impact on the monetization of data usage. Both unlimited data plans offered early on and zero-rated data plans offered more recently can temper revenue growth, on a planned yet potentially faulty premise.

MNOs have seen revenues decline with regard to both voice and SMS traffic. Regarding voice traffic, lower pricing has increased traffic by multiples, which helped somewhat to mediate the slide in revenue declination to a certain extent; however, revenues per unit over time declined greatly. Revenue declines for SMS traffic have been highly precipitous. Competitive market pressures on mobile termination rates as well as standard industry maturation of service pricing have assisted the decline in revenue. The commoditization of mobile services has developed revenue streams that tend to decrease by the unit as market liberalization and other market dynamics have driven down these costs.

Threats to industry come and go and many are dealt with as normal business activities, for all business must manage challenges on a constant basis. The evolution of the business model has gone so far, where now there is another but very significant threat from the OTT sector, which is called OTT Bypass fraud, which has tremendous effects and implications on the revenues and networks of operators, governments and users. This is transcendental in scale and if not abated in some measure, the MNO's business model is under cataclysmic challenge. Prior to OTT Bypass, the OTT's created a disruptive force on the access side of the network; however now under peril is the terminating side of the network. Voice revenues are under a new risk and could be rendered totally extinct.

Fragmentation of Communications

The competition brought by OTT market players has resulted from disruptive technology. The mobile telecom market has had to adapt and adjust to a new playing field, which some believe is not level, while others consider the result to be a greater good for consumers. There arises a huge challenge for regulators: Should OTT applications be characterized as telecom services (voice or data) or telecom infrastructure? And ought they be subject to further regulation and taxation?

Moreover, market liberalization has not only resulted from the issuance of additional MNO licenses by governments in world markets, for de facto market liberalization has occurred from the actions of OTT players and states' benevolent attitudes toward them, with regard to regulatory classification and taxation. Regulators are caught in the crosshairs of what is truly the next MFJ type of scenario, where they try to maintain competitive balance and total access to information, yet preserve investor value, private and government revenue generation, and adherence to general law.

The added competition from OTT application providers, (current apps like Skype, Viber, WhatsApp, and a cast of hundreds, as well as industry-wide efforts such as WebRTC and others) allows users to communicate more efficiently and more cost effectively. This OTT activity created initial benefits for MNOs by driving increased data usage, which, if effectively priced, improved revenues although with certain inherent risk. Some users received flat-rate unlimited data packages. The standard 80 – 20 rule tended to apply, where 20% of users created 80% of data traffic, and this was usually over unlimited data plans. Larger revenues and market share potentially mitigated financial risk, at least when these pricing plans were launched.

“Operators will remain the dominant force in mobile voice but will be significantly weakened as OTT VoIP services continue to grow.” – OTT communication services worldwide: forecasts 2013–2018

Operators in many countries have struggled, while data traffic spiked enormously from mounting messaging, gaming, video, and voice traffic over the same data networks, and, principally, OTT providers were not assisting with regard to investment in infrastructure, which is so critical toward successful deployment of broadband programs.

Many operators that were slower to adapt suffered. Regulation in some markets demanded operators to stay with pricing that did not properly monetize data usage, and a resultant decrease in revenue efficiencies occurred.

Impact of Smartphone and OTT Services

The use of ubiquitous technologies greatly altered the basic means of either sending a message or making a voice call. The free costs, the convenience of access, as well as the unique novelty of application converted many users from traditional SMS. The prime catalyst is smartphone usage and ownership: eMarketer states there will be 1.5 billion smartphones worldwide by the end of 2015. Seventy per cent (70%) of the world's population will own smartphones by 2020 (Ericsson 2014). Costs for entry-level smartphones continue to decline, and global vendors are focusing on developing markets with burgeoning populations yearning for mobile services. Lower-cost smartphones sold in developing countries can greatly alter market forces in the industry. The second catalyst for change was the ability for users to send free over data networks rather than paying operators per SMS. Voice usage follows similarly, although slightly less radically.

“More than half of smartphone owners worldwide are already active users of OTT messaging apps.” – Future Comms and Media, 2014

The advent of the smartphone has essentially created an entire cottage industry with regard to how people speak to and message each other as well as message each other. This new ecosystem is highly dependent upon the Internet, bandwidth requirements, and operating systems for smartphones, such as Google's Android, Apple's iOS, and Microsoft's Windows platform.

“By 2017, the US will account for 12% of total global smartphone-based OTT users. The UK will have 51.4 million smart phone users by the end of 2013, of which 24.7 million will be using OTT communication services.” – Mobilesquared, 2014

OTT Messaging Services

OTT messaging services, in particular, have proved popular, and adoption levels soared in many countries throughout 2012 and 2013. Analysys Mason (2014) estimated 55% of smartphone owners worldwide were active users of IP messaging services at the end of 2013. These services are driving more elevated numbers of user commitment compared with SMS. In June 2013, WhatsApp recorded an as-of-yet unsurpassed record of 10 billion messages sent out in a day, which is more than 30 messages per user per day. Analysys Mason further estimated the aggregate volume of messages sent from mobile phones through IP services surpassed the volume of SMS messages in 2013, at more than 10.3 trillion compared to 6.5 trillion worldwide. These patterns are expected to continue, driven by expanding acceptance levels. The volume of OTT messages are expected to reach 37.8 trillion messages sent in 2018.

Ensuring Voice and Messaging Revenues

MNO's have experienced large declines in voice and SMS traffic revenues over the past five years, and are yet again confronted by new attacks on their revenues. Services like WhatsApp, and iMessage, along with many others, have transitioned revenues from the use of standard voice and SMS to OTT applications over data networks provided by those same operators.

“Smartphone penetration of VoIP applications in Saudi Arabia and UAE is probably the highest in the world. In Turkey, smartphone penetration stands at 16 million, 24% of the market, meaning the market is still dominated by feature phones.” - Mobilesquared, 2014

Revenues earned from SMS traffic essentially morphed into revenues from increased data traffic for operators, however, not at the same scale, and operators were slow to adapt. The requirement has never been greater for operators to be competent in such a turbulent business environment, and a highly detailed understanding of the various types of fraud is essential.

“There are now over 500 million iOS devices globally, with iPads accounting for almost 85 million devices. From those devices iMessage users now send over 200 million messages a day.” - Mobilesquared, 2014

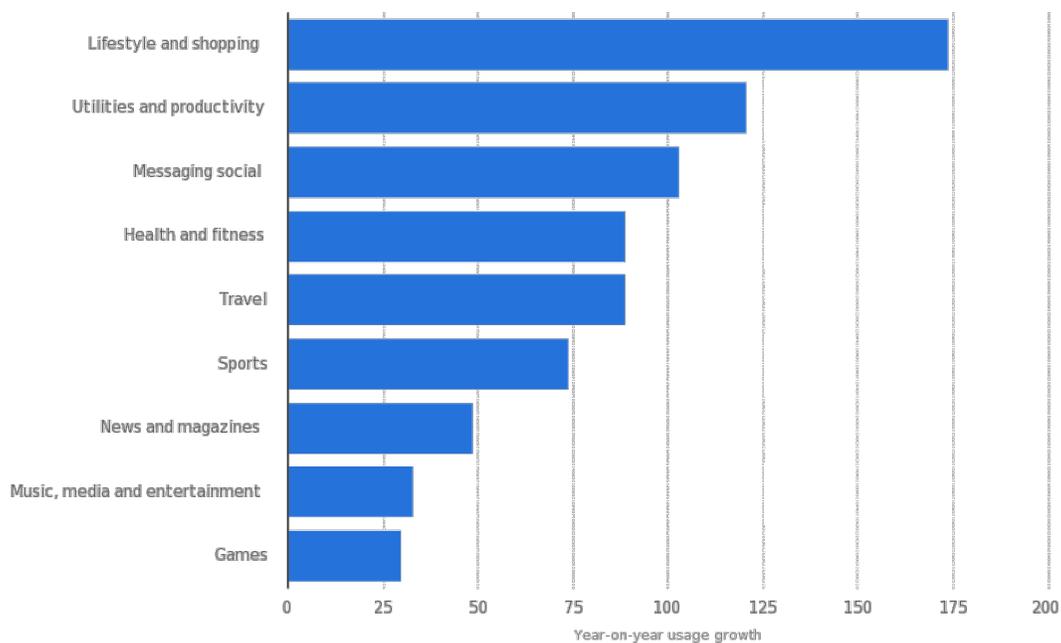


Figure 1: Year-on-year growth: time spent per mobile app category in 2014

- Flurry, Statista 2015

OTT Bypass Fraud

OTT bypass fraud is a relatively new means of telecom fraud, posing serious trouble for telecom operators, as there exist a number of services where, by design, OTT providers intrude in various ways within operators' networks. This new type of fraud has recently become quite a phenomenon. The opportunity for OTT bypass fraud is huge in markets where OTT communication services such as WhatsApp, Viber, and others are in use. These services work across multiple platforms and offer both voice and messaging services, which are provided free of charge to users. OTT bypass attacks are different from simply the use of applications by OTT providers on top of data networks, taking new originating voice and SMS traffic. This new threat effectively redirects terminating traffic from legitimate mobile calls onto exactly the same applications that cause originating call revenues to decline. The situation is grave: Calls to mobile numbers are redirected in the middle of the calls, generally at the interconnect phase of call connection, onto wholesale or pirate networks, which terminate the calls to OTT applications that are assigned by and associated with the mobile numbers of the users. Untreated bypass fraud is commonly associated with OTT services because the accounts are linked to the mobile phone numbers of the users. WhatsApp and Viber are ubiquitous now and, therefore, the volume and scale of calls increases every month. However, there are entrepreneurs now building hundreds of such smart phone applications that are only exacerbating the situation. This type of fraud is extremely harmful in the long term, since it is paradigm changing. It has the capacity to drastically change the business model for all operators.

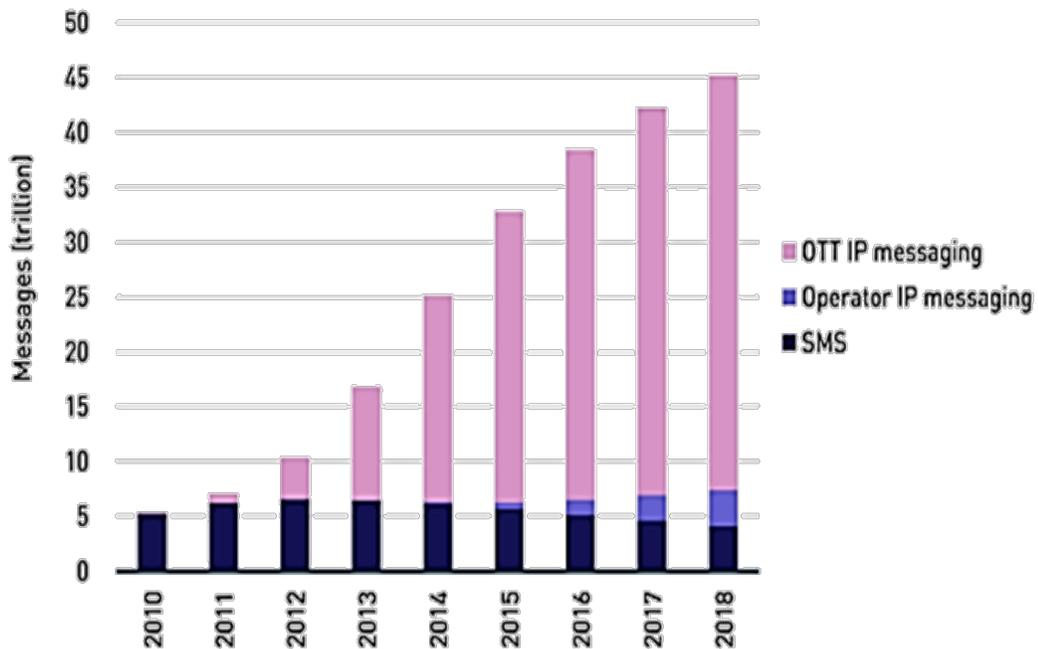


Figure 2: Messages sent via mobile handsets by service type, worldwide, 2010–2018

- Analysis Mason, 2014

How OTT Bypass Fraud Works

Typically, OTT bypass fraud occurs on mobile-to-mobile calls. The interception of calls from originating mobile networks and putting them onto wholesale international telecommunications networks is where most of the so-called hijacking occurs. Some OTT providers/partners have created discrete - or not so discrete - wholesale network environments, where they are able to redirect calls from the originating (legitimate) mobile network that normally terminate to an MSISDN addressed device via the operator network of the same MSISDN, but rather intercept the call within the matrix of the interchange of networks within the wholesale environment, where service providers enlist the redirection of the call onto a data connection that terminates to the OTT application resident on a called parties MSISDN identified smart phone.

Wholesale operators work hard to decrease costs for call termination. If a call can be terminated onto a data network rather than through a traditional mobile voice network, the actual cost of terminating the call is greatly reduced, if not free of charge. This is the explicit OTT/partner motivation for the redirection of the calls. Either the OTT provider that owns the host cellular network is able to earn additional revenues or possibly, originating network service providers are able to lower the terminating costs of a call. However, the mobile operator owning the (MSISDN) mobile number receives little or no compensation, only that of the marginal data traffic plan they have for the owner of the MSISDN, rather than terminating voice revenue.

The hijacked or intercepted call, which once identified as a terminating number that belongs either to an OTT that has provided a database, allows the service provider (sometimes owned by an OTT or is a partner), to identify if the called mobile number belongs to an application used by the called party that is owned by the OTT. If the MSISDN matches, the call can be rerouted to the OTT data network, which would terminate to the application on the smart phone. Aggregation of MSISDNs, which are also owners of smart phones that have resident communications apps from various OTTs, is also going to be prevalent, once the economies of scale get large enough, where these MSISDNs can be bought and sold on the wholesale market.

Additionally, some less than scrupulous mobile networks, could work with multiple OTTs, and as such, build a far larger number of re-routable mobile numbers that would greatly reduce their termination costs. But this comes at the loss of the mobile network operator that operates the network hosting, the called number (MSISDN) as well as the user themselves, who are denied the free termination of a mobile call onto their phone (in most countries, called party does NOT pay for the call). The called party, who is not aware of the routing method of the call, will have to pay for the call via data usage for their data usage plan, unless the OTT provider delivers them a zero-rating program.

This is highly disruptive and disturbs the revenue chain for typical termination of that call. Operators have agreements for termination from other operators. However, in the new environment, wholesale service providers can provide a list of mobile numbers, which belong to application users, as a terminating field for sale, to other originating traffic senders, where the cost for termination is much less than the terminating cost to the actual mobile number network.

Regional Trends in OTT Communications

Analysys Mason (2014) forecasted the quantifying impact of OTT communication services in different regions worldwide. On the basis of comprehensive analysis, they exposed the heterogeneity of messaging markets in Western European usage data. Despite high smartphone penetration, OTT communication services penetration is comparatively truncated in North America. While the North American operators are somewhat advanced in the increasingly data-centric marketplace, in the developed Asia-Pacific region, social messaging apps are most widely used. For example, WeChat is the dominant messaging market in China. As compared to Asia-Pacific regions, the outlook of OTT services varies considerably in Western European countries, also the operator's response changes with market dynamics. Apparently cultures and customs affect the manner in which users uptake OTT applications in various regions across the globe and thus, the effect of OTTs on operator networks vary on a per region basis.

An operator in Kuwait recently announced it will provide zero-rating data traffic for Skype and WhatsApp. This decision could be fatal for them and the industry because this approach essentially provides an opening for all WhatsApp users on that operator's network to be sent OTT bypass calls, where the OTT provider potentially gains additional income from selling those users' numbers to wholesale operators while the operator gains absolutely nothing from those calls. Therefore, operators must not neglect OTT bypass fraud, which has been extensively associated with certain regions in the world.

What are the Impacts & Who are the victims from OTT Bypass Fraud?

When traffic is rerouted through OTT proxy networks, traverses data networks, and terminates on various applications such as Viber, WhatsApp and other network appliances, there is a litany of impacts:

- Data network traffic increases and may congest, overload, and degrade the quality of operators' data networks.
- The intended receiving network operator receives no revenue from the traffic.
- Governments do not receive revenue for calls redirected to data networks, such as usage-based taxes, fees, and USF contributions.

- Call quality suffers because call termination over the Internet is on a best effort basis and no SLAs are offered for this type of traffic.
- When call quality suffers, so does an operator's branding.
- Receivers' data packages can be consumed without their knowledge or intention
- CLI is often not passed, therefore causing safety and security issues.

Victims of OTT bypass fraud can be segmented into different groups: operators, governments, and users. Operators and their investors lose large amounts of revenue due to OTT application traffic that is redirected off their networks and onto their users' data plans. In many regions where this type of traffic is prevalent, governments own stakes in the operators and, therefore, further see their revenues reduced by this type of fraud.

Additionally, users may unwittingly incur debits to their data plans, because OTT communications services calls terminate through applications on their smartphones, If they do not have unlimited data plans, these calls will cost them. Users may also suffer poor call quality because calls are typically made through non-standards-based VoIP networks.

Conclusion

The creativity of emerging network technologies has unwrapped many opportunities for fraudsters; however, in order to combat fraudster's services, all stakeholders must stay one step ahead. OTT bypass can create a sort of tsunami of new applications, such as:

- Vendors building applications associated to mobile numbers and placing them on their handsets. These would be second- and third-tier market hungry handset manufacturers most probably, who would possibly create agreements with the major OTT network service providers to terminate calls on to the specific application numbers.
- Discussions have surfaced where entrepreneurs would create a clearinghouse of mobile numbers belonging to OTT app owners and users, and thus "selling" this list to wholesale service providers who are not indentured to the larger MNOs.
- OTTs themselves becoming virtual termination network service providers themselves
- Operators that are inadequately reliant on termination revenues would create termination field agreements with additional outside of network mobile number holders, thereby cannibalizing mobile termination traffic destined for competitor networks.

Operators have begun to realize the proliferation and implications of OTT bypass fraud. They are looking to find ways to monitor for and detect this traffic and to identify trends associated with it, and to eradicate it before it becomes too large of a problem. There are several network fraud and security firms that are working on or have nascent capabilities in recognizing this type of fraud and finding measures to deal with it. The size and scope of OTT bypass fraud are predicted

to grow non-linearly due to previous experience regarding the disruptive growth of the OTT players and the attractiveness of low costs to service providers. Therefore, OTT bypass fraud will grow unabated without extreme actions on the part of all stakeholders, including operators, regulators, OTT service providers, and fraud management firms globally. There are literally hundreds of applications, which are now sold via app stores, that can handle voice termination and in most cases, the originating end.

In summary, OTT bypass fraud is not just a threat to revenue loss, but to the entire business model of how all operators are compensated for the services they provide. The effects of OTT bypass fraud have only just begun to surface. The industry will never be the same again!!!