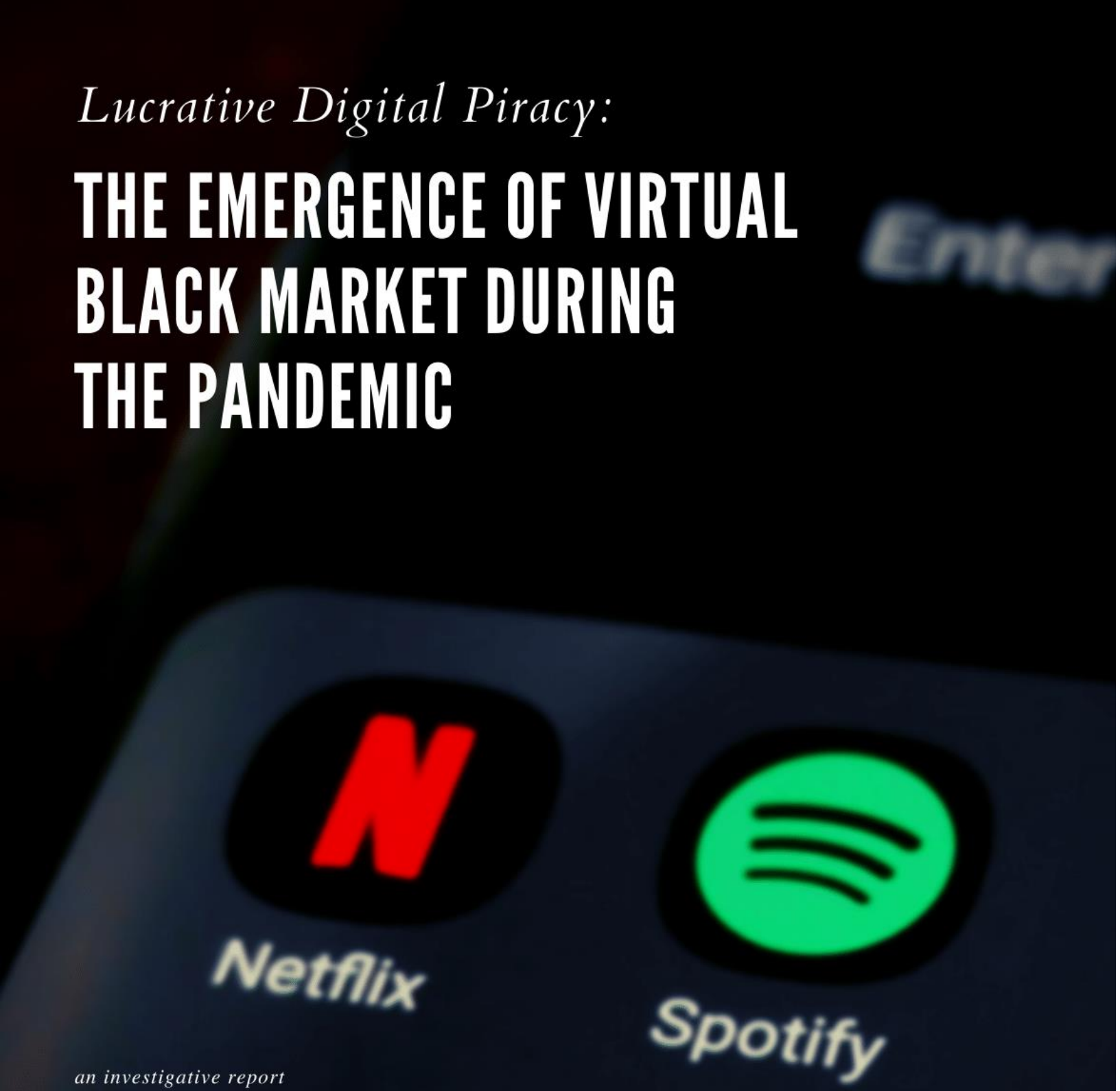
Lucrative Digital Piracy:

THE EMERGENCE OF VIRTUAL BLACK MARKET DURING THE PANDEMIC



an investigative report

De Leon, Franco Luis
Estrada, Hyacinth
Hall, Angelica
Manalang, Kyle Gerard
Marin, Charnamy
Palabrica, Jeremiah
Vivar, Sherilyn

Polytechnic University of the Philippines
College of Communication
Department of Journalism
3-1D

ABSTRACT

This article explores the rampant digital piracy during the COVID-19 pandemic where there has been a significant rise of illicit online marketplace activities in social media sites, where illegally acquired Spotify premium subscribed accounts and Netflix accounts are being sold for a cheaper price.

The COVID-19 pandemic is becoming a double-edged sword, so to speak, since watching films in cinemas has been banned due to lockdown. Therefore, it has increased the demand for online streaming platforms among consumers to prevent the violation of quarantine protocols while continuing this leisure activity of watching movies; and its demand being an untapped market for people who were looking for ways to generate income due to the recent economic recession brought by halted economic activities during the extended period of lockdown in the Philippines.

The processes on how these illicit streaming services premium accounts are acquired will be discussed here, along with the dangers to the consumers, and the current scene of battling this illegal activity, as it is considered as a form of piracy in the Philippines.

TABLE OF CONTENTS

Introduction

Piracy is not just a phenomenon, but a stubborn stain in the creative industry. Although the industry has been fighting back, its methods are not always sufficient due to various misconceptions.

Worst, some companies have already embraced this issue, forcing them to adapt and normalize it. For instance, unofficial and unconsented audio and visual content, like new music videos, can spread worldwide in just a blink of an eye with the emergence of another form of lucrative copyright infringement - the digital/online piracy.

As the Internet access became a commonplace, piracy obtained an enormous power to challenge intellectual property rights, where illegal downloads and streaming reached high peaks of media viewership. However, most people blurt out "fair use" as an excuse for them to access and reproduce copyrighted works online.

When people keep on turning a blind eye, a small but nagging issue can transform into something massive later on. That is how a supposed-to-be “sideline” of pirating creative works online transcended towards an adverse industry - virtual black market.

While most people and lawful authorities carp that black market only serves to patronize and tolerate illegal and unethical practices of profiteering from other people’s fortune, black market is evidently an easy way out during crucial times, especially when someone’s life is at stake.

Will Kenton stated in an Investopedia online article that black market is an economic activity that takes place outside government-sanctioned channels, avoiding government price controls or taxes. Black markets can also take its toll on the economy due to unrecorded and tax-free processes.

Amid the COVID-19 pandemic, a black market can be a person’s only choice to procure goods and necessities. The pandemic indeed brought direful effects to people, where they had to seize any jobs that will help them earn a living.

E-commerce or online selling became the to-go business and income source of people due to community lockdown and restrictions. Meanwhile, some people are running out of things to do while staying at home, preventing themselves from succumbing into boredom.

Thus, upon all online businesses, streaming sites like Netflix, Spotify, Viu, and Youtube are the most in-demand ways not only to entertain oneself, but also an opportunity to have lucrative monetary sources. With the giant streaming applications emerging nowadays, online sellers of cheap premium accounts have also dominated social media, particularly Twitter and Facebook, providing easy access for its users just by using specific tags and keywords.

Up to this date, these platforms offering paid subscriptions have already influenced the streaming activities of their audience with its highly relatable and entertaining content. However, these applications' prevalence provides another opportunity for exploitative ways to earn money, which is through selling cheaper subscriptions online.

With the prevalence of these illicit activities, most people inevitably perceive this as "normal" as there is only a minimal regulation on this issue. Although it is inconspicuous to many, authorities who must impose protocols regarding these illegal methods could not par with the prevalence of illegal streaming sites and emergence of digital piracy techniques.

PART 1: The Emergence of Digital Piracy

As how the US Constitutional Rights Foundation coined, the "age of digital piracy" dated way back in the 1980s through the form of data and images compression using MP3 (MPEG-1 Audio Layer 3 or ISO/IEC 11172-3) computer files for easier downloading and copying processes to a computer and CD burner.

More than a decade later, an "explosion" of illegally downloaded music instigated when a college student developed the "Napster" peer-to-peer file sharing method, providing an efficient way to find and download MP3 files via the Internet.

Unfortunately, the rise of broadband high-speed internet connection escalated the advent of online piracy, extending to piracy of movies via file sharing methods. Group members of "warez" are the proponents during this time, where they post movies illegally on the Internet to gain fame and glory from online peers.

Online piracy did not stop on music and movies as it also extended to CDs, DVDs, video games, and computer programs and applications, may it be through:

- Obtaining movie copies before the release date on the theaters through an inside job (buying them from employees in the industry as well as film reviewers),
- using a camcorder to record the screen, and
- selling copies to bootleg factories where it will be CD-burned by the thousands to sell.

With the pandemic crisis, cinemas and other physical entertainment establishments hit the rock-bottom as they were mandated to shut down for months (and counting), making attendances plop to zero. The combination of the public's need for entertainment through audiovisual content and the shifting of the industry through online means have led to the proliferation of piracy in the digital realm.

In a span of four months (March to June 2020), the Intellectual Property Office of the Philippines (IPOPHL) has received 67 complaints and reports on intellectual property rights violations. Despite the pandemic, IPOPHL's Intellectual Property Rights (IPR) Enforcement Office had 28 complaints filed regarding piracy (illegal reproduction of copyrighted content and illegal streaming), noting that even e-books have been pirated as well.

In September 2020, YouGov for Asia Video Industry Association (AVIA) conducted an online survey, where nearly half (49%) of the Filipinos admitted using illegal streaming or torrent sites and 47% of consumers who accessed piracy sites cancelled their subscriptions to both local and international content services, showing how potential growth of subscription-based content service providers in the country were negatively affected.

The levels of online piracy in the Philippines are among the highest ones in Southeast Asia compared to neighboring countries. However, the same survey stated that 53% of the 1,098

Filipino respondents agreed that a "government order or law for ISPs to block piracy websites" would be the most effective measure against the rampant illegal streaming and online piracy.

In Southeast Asian countries, the key variable to mitigate online piracy levels is through a proactive piracy site-blocking initiative by the government. Thus, it is not only the streaming sites' responsibility but also the governments' job to slam down these bravado illegal streamers and pirates online, just like what happened in Malaysia, where more than half (55%) of online consumers noticed that a notorious piracy service has been blocked by the Malaysian government, resulting in decrease to inability of access and usage to those piracy services.

AVIA and Coalition Against Piracy has been promoting for the passage of the Philippine Online Infringement Act authored by Senate President Vicente Sotto III proposes a regulatory site blocking mechanism, empowering authorities to mandate and ensure that internet service providers (ISPs) take "reasonable steps to disable access to sites whenever these sites are reported to be infringing copyright or facilitating copyright infringement."

Although the government has taken measures to fight against online piracy, it is evident how stagnant the authorities are in combating this issue. Despite how content producers urged the government to block illegal streaming sites, the Philippine Senate Bill No. 497 entitled "Online Infringement Act" is still yet to be approved.

With the increasing rate of online piracy in the country, Globe President and CEO Ernest Cu expressed that "the ill effects of online piracy cannot be underestimated," advocating the company's #PlayItRight program that educates people about the impacts of digital piracy, as well as making the right choices when it comes to online consumption.

Vivencio Ballano's *Tracing Media Piracy: Current and Future Trends (2016)* implied how the country's increasing Internet penetration contributed to the media piracy shifts from the temporal space of sidewalk stalls to the cyberspace of the Internet, paired with the convenience, accessibility, and affordability of direct illegal downloading, peer-to-peer sharing, and other evasive techniques through hardware and software technologies.

With the deep-rooted piracy problems in the Philippines, it is no wonder how people easily took advantage of the vulnerability of online streaming platforms, like Youtube, Spotify, Netflix, Viu, etc. Worse, along with quarantine restrictions, many Filipinos have turned to the Internet in search of entertainment and ways for passing the time while cooped up inside their homes.

If people want an easier way to "Netflix and Chill" and jam with their favorite songs on Spotify while only paying almost half the price, they are naturally resorting to options ranging from cheaper to free subscriptions compared to authorized means, which is through the black market.

To some people, it is bothering to witness people patronizing illicitly acquired subscriptions. It may sound an excuse, but the low-price ranges and minimal purchasing power of the majority in the Filipino society complements the need of Filipinos for extra income during

the pandemic, as well as the increasing demand of online streaming platforms in the creative industry.

Evidently, there are various stimulants as to why it is hard for lawful authorities to regulate the increasing black market for cheaper subscriptions, which are:

- The ingrained culture of normalized piracy in the Filipino mindset,
- The apparent divide between the privileged (those who can afford the subscription cost of entertainment streaming sites) and the less privileged people from the lower class (who cannot afford entertainment streaming sites),
- Fair use rights being an excuse for digital piracy, and
- Piracy misconceptions (only a copyright infringement and not theft)

The Rise of Digital Piracy During the Pandemic

Media piracy has been plaguing the Philippine society for decades now. Apparently, along with its rise in the global context, the Filipino society adopted it through modem-backed software piracy and video cassette recorder (VCR) technology in 1980s, evolving as the rise of pirated optical media contents has been rampant in the early 2000s. Media piracy had transcended time and adapted perfectly to its technological and social environment.

The normalization of media piracy had blurred the line between what is in demand and what's illegal. Sociology professor Vivencio Ballano stated in his book *Sociological Perspectives on Media Piracy (2016)* that counterfeiting and piracy were "not fixed forms of rule-breaking phenomenon". Rather, it used to be a personal activity that seeks to entertain and pleasure.

The commercialization of online piracy started during the dawn of digital technology, when internet users began sharing copyrighted materials in Peer-to-peer (P2P) networks and file sharing sites. This gave birth to what was known today as "illegal streaming" or the unauthorized distribution of digital media contents (mostly, videos and films) to generate web traffic and advertising revenue.

Along with the boom of illegal streaming is the rise of virtual black markets that capitalize on the commercial use of illegally acquired Subscription Videos on Demand (SVOD) subscriptions. This modus operandi has seen a significant growth during the pandemic, where most activities are carried out through digital means. As reported in the previous parts, media piracy has evidently robbed the creative industry of their bread and butter.

One factor that greatly contributes on the prevailing culture of piracy in the Philippines' local creative industry is the massive economic decline that hit the country due to COVID-19 restrictions, which also handicapped our retail and tourism sector, notwithstanding the natural disasters that wrecked the agricultural sector.

These economic catastrophes closed business establishments and left millions unemployed. Due to the lack of primary livelihood, some people were forced to resort to illegal means in order to financially support themselves and their families.

Most sellers and providers of illegally distributed online media contents capitalize on the desire of most people to have cheap entertainment.

In a survey conducted by YouGov study in September 2020, the Philippines was ranked as the third country in Asia with the highest percentage of video on demand piracy. According to the results, 49 percent of Filipinos engage in the use of piracy streaming sites.

Factors such as financial practicality and easier access to illegal streaming sites contribute greatly on the high percentage of piracy use in our society. However, these are not the only elements that fuel this industry. Based on the results of the investigation, there are deeper motivations as to why both sellers (providers) and buyers (customers) continue to take part in the illegal activities that empower the virtual black market.

Given this fact, we can insinuate that the COVID-19 crisis has become a double-edged sword, affecting content creation, exhibition, and online piracy; adding up to the struggle of finding ways to resume productions through alternative screening platforms without violating quarantine protocols.

A pirated DVD store in Quiapo, Manila. Retrieved from: Pirated DVD stores | Cebu Social (wordpress.com)

PART 2: Discoveries of a Wide and Systemic Illegal Distribution of Premium Streaming Apps

The Hacking Industry and Tools of the Trade

The researchers encountered two hackers whose identity shall remain confidential. The hackers will henceforth be referred to as Nine and Healer.

According to the Offensive Security Society, an organization which primarily aim to bring cybersecurity to the public, there are three primary types of hackers which exist: the White Hat hackers, the Black Hat hackers, and the Grey Hat hackers.

White Hat hackers are known as ethical hackers, or those who act for the interest of society. These hackers act out of goodwill and find exploits within a particular system through rigorous testing and report the findings to the system administrators to be fixed. They are also employed by companies, such as Spotify who employs the cybersecurity company HackerOne; and Netflix, which implemented the Bugcrowd initiative, which seek protection against Black Hat hackers. Both employ White Hat hackers to find bugs and exploits in exchange for monetary incentives.

Grey Hat hackers are similar to White Hat hackers, where their actions are for the benefit of society, in contrast with the While Hat hackers, they sometimes refer to illegal or questionable methods to achieve their goals.

Black Hat hackers, on the other hand, are hackers with purely malicious intentions. They use their knowledge for personal gain, engaging in malicious activities such as server attacks: stealing millions of login credentials from a vulnerable server mainframe, which, in turn, are used to generate a list of thousands of accounts on other platforms in a process called “credential stuffing”.

Credential Stuffing

Healer described credential stuffing as “waiting for someone else to dump a bunch of usernames and passwords and just leaching off of that.” It involves compiling and testing the stolen login credentials, often a combination of emails and passwords, which are called “combo lists”. These *combo lists* are tested on various sites, and, when they match, it is referred to as a “hit”, or a successfully stolen account.

Database breaches have resulted in hundreds and thousands of premium subscription accounts being affected, wherein these accounts are “recycled”, or have their email and password reset and sold as a fresh account with a pre-paid subscription.

Brute Force Attacks

Another effective method used by black hat hackers include brute force attacks, which utilizes an intensive password guessing algorithm to process thousands of frequently used passwords until it result in hits. This is often used in combination with proxies, which dynamically changes the Internet Protocol (IP) address of the device used in brute forcing in order to avoid detection.

"Most sites block you from logging in over and overusing the same IP. So, we use proxies to dynamically change the IP every few attempts.", said Nine.

Phishing

Another commonly-used method is phishing, "Phishing emails are tried and [tested]. Requires almost zero effort as well.", Healer stated. Phishing is the process setting up fraudulent imitations of an account login page of a particular service which trick legitimate users of the service into typing their login information. The information is then sent to the hackers running the fraudulent website, and the acquired information would be used in generating new combo lists to obtain more accounts.

Phishing emails are sent by hackers to unsuspecting victims, which are mistaken for legitimate emails by the companies they disguise themselves as, which then link to the fraudulent websites.

Verizon's 2020 Data Breach Investigations Report revealed that phishing is the most common reason behind data breaches, with phishing comprising over 20% of data breach incidents. The report also states that phishing is a type of social malware that relies on social engineering techniques which, in this case, is through deception.

It also showed that login credentials are the most commonly stolen information with over 60% of all phishing attacks targeting login credentials. The data revealed that phishing emails is still a very reliable method for hackers, with a 3.4% chance that the email recipient would be victimized. With thousands of these automated emails being sent daily, that 3.4% figure becomes a significant quantity of victims.

A study conducted by the security firm LastPass, entitled *The Psychology of Passwords: Neglect is Helping Hackers Win*, revealed that among 2,000 respondents, 59 percent have admitted to using the same password across all their accounts. Respondents of the study only change their passwords only when they are required to do so, or when they have been already affected or victimized by a hack. Combo lists are effective due to this negligence, as one combination of an email and password could give a hacker access to dozens of accounts across different platforms.

Most account hackers could be considered as "Script Kiddies", a subcategory of Black Hat hackers. They are called as such since they use downloadable hacking tools such as the brute force tools, and basic methods such as launching a proxy site. "Typical DNM people do phishing campaigns. Nothing really technical or cool about any of it, literal skid level stuff. Most of them are too stupid to secure their phishing sites as well.", said Healer.

Dark Net Market: An Illegal Commercial Hub

The top of the food chain of the illegal streaming account market are the suppliers. Suppliers get their hands the dirtiest, and their work runs the entire underground network. The suppliers are the hackers that personally obtain stolen accounts. They operate within Dark Net Markets (DNM), where they sell the stolen accounts.

The DarkMarket was one of many DNMs which offers services such as buying and selling of stolen data and the manufacturing of illegal drugs. It was shut down in a multinational raid conducted by Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom and the United States (DEA, FBI, and IRS). Similar sites lie within the confines of the *dark web*: a closed-off, encrypted depository of rogue sites which act as hubs of multinational criminal activity. The security and anonymity within the dark web are a necessity, due to the controversial nature of these sites.

DNMs often go defunct, or non-operational, due to takedowns by international law enforcement agencies such as the International Criminal Police Organization (INTERPOL).

Nine sells the stolen premium subscription accounts on the DNM Hell, a forum that focuses on the buying and selling of stolen accounts. Another popular DNM utilized by hackers is Dread, a reddit-like forum that allows hackers to interact and collaborate.

Healer estimates the price at $0.50 to $1.00, while Nine places the price at $0.40 per hacked account, depending on the 'quality' of the account. Longer pre-paid subscription plans are sold at slightly higher prices. "A lot of them [account hackers] resell the same accounts to new buyers once they run out as well.", Healer claimed. The same account could be sold multiple times to different people,

Two-Factor Authentication and the Future of Account Hacking

Nine mentioned that the introduction of two factor authentication (2FA) has been detrimental to modern hacking. "The thing with these sites is 2 step verification is either optional and off by default for "ease of use" or just plain nonexistent. It's the biggest hurdle to hacking now because you can't mess with the network providers' verification codes sent out to the users."

2FA is a security measure which requires a non-internet-based input to prevent hacking attempts. Twilio, a company which offers their own brand of 2FA under the brand Authy, lists three categories of second inputs. Many of which are currently implemented by thousands of companies, from online banking to social media.

The first of these categories is 'Something you know', which is defined as a Personal Identification Number (PIN), a "secret question", or a keystroke pattern. PINs have been in use in banking even before the advent of the digital age, secret questions are used as account recovery methods in social media platforms such as Facebook, and keystroke patterns are commonly present in encrypted smartphone applications, such as cryptocurrency wallets.

The second category is "Something you have" which would be a physical object that would be used to login into the account. The most common object this refers to would be a

smartphone. 2FA utilizes the cellular network of the smartphone's service provider to send a single-use code, called a push notification, to use for logging in.

This, according to Nine, is an increasingly common roadblock in modern account hacking. By requiring an account to be authorized for login via text message, even though a hacker inputs the correct username and password, it is effectively immune to attempts to compromise the account, by having a hard physical gate that prevents access, the text message code.

The third category, "Something you are", is by far the most secure input. These security inputs are unique biometric patterns such as a fingerprint, voice prompt, or iris scan. These methods are employed in safeguarding bank vaults, museums, and, most commonly, smartphone lock screens.

The presence of 2FA drastically raises the difficulty of hacking attempts, but as Nine has mentioned, it has one fatal flaw: on many platforms, it is optional and off by default. User prompts to activate the feature are frequently ignored, and it is perceived as an inconvenient hassle. A study conducted by the security firm Duo Labs entitled *State of the Auth - Experiences and Perceptions of Multi-Factor Authentication* revealed that only 53% of internet users enable two factor authentications, leaving the remaining 47% vulnerable to hacking using only combo lists.

Pirated Apps

Vivencio O. Ballano's *Tracing Media Piracy: Current and Future Trends* (2016) explains that the emergence of modern technologies, particularly the internet and software applications, have brought modernized shifts in piracy methods.

"As the country increases in Internet penetration, the locus of media piracy shifts from the temporal space of the sidewalk stalls selling pirated DVDs or illegal CD–DVD shops to the cyberspace of the Internet. The use of discs becomes less popular as media piracy becomes more convenient, easier, and cheaper with direct illegal downloading, peer-to-peer sharing, and other evasive techniques using the latest sophisticated hardware and software technologies." (Ballano, 2016)

Today, a form of modern digital piracy comes in the form of MOD APKs. In the investigation, it was discovered that this is one of the methods used to illegally access premium Netflix and Spotify accounts. Using MOD APKs, which are the cracked/altered or pirated version of the apps, various users can now use the premium versions of streaming entertainment apps unlimitedly for a cheaper price.

This was revealed through an interview with an online seller who preferred to stay anonymous. Ren, not their real name, disclosed that they do not directly sell premium subscriptions of Netflix, Spotify, and Crunchyroll. Rather, those are part of the freebies that comes with their products upon purchase.

"We are not selling subscriptions but as a freebie for buying our [product] bundles, we provide downloadable mods for Netflix, Spotify, and Crunchyroll. These mods allow our customers to use the apps for free, while gaining access to premium features," Ren stated.

When asked how they were able to get those premium subscriptions at a cheaper price, they answered that it came from the reseller's package which they bought from a main supplier.

"Upon purchasing the reseller's package from the main supplier, we were given access to a Google drive folder [containing] unlimited shareable mods."

Ren also claimed that they have no knowledge of where their suppliers get those mods, though they believe that those are being obtained from another main supplier. When asked why they sell these subscriptions [in this case, as freebies along with their bundles], despite the possibility of it being illegal, they replied, "We are just selling this for extra income. We do not actually use the money to buy our needs. It is only used to buy other stuff that we don't bother asking our parents to buy for. Also, it seems as though the customers are really interested in buying these, so we just provide what they need."

Anon is another seller who requested anonymity. Anon sells Netflix and Spotify premiums that are good for one month, three months, and one-year subscriptions. In an online interview, they disclosed that their products are "hacked and APK[s]", to justify the reason for the cheaper prices. They started this business of selling hacked and APK versions of these entertainment apps without any capital involved.

However, Anon denied knowing where their suppliers obtained these mod APKs. Only that they started doing this to help their friend financially. "I am just helping my friend because it contributes with his school financial expenses," Anon said.

The process for purchasing their premium accounts usually involves giving the account to the buyer first to test whether it works. Then, they receive the payments through GCash or cellular load. Anon also stated that they never got in trouble for selling those cheaper subscriptions despite the possible illegalities.

AMEX and Gift Card Methods

Meanwhile, an online seller shared another method of obtaining cheaper premium subscriptions. Cess, a seller of Netflix, Spotify, Viu, Crunchy Roll, Youtube premium and VPN accounts said that her products are paid through gift cards, which their supplier provides, making them cheaper than their original prices. This way of acquiring premium accounts is technically legal due to the legitimacy of the account subscriptions being sold – they are not APKs or mods.

Cess cited in the interview how other suppliers got their cheaper premium subscriptions. One of those is the American Express or AMEX method, where payment is done through GCash American Express virtual pay. The process for a Netflix premium plan involves an individual user with the virtual pay account to first choose a mobile plan that costs 149 pesos. Upon payment, the user must put their details on the virtual card they got from GCash, then change their plan to a premium account in the account settings.

After this process, the user is instructed to do a subscription renewal by cancelling the current (and newly chosen) premium subscription before the billing date (after 30 days free trial). This will prevent the app from billing them, but the premium subscription will remain until the end of the trial. This method is effective for individual users who are interested in using the free

trial of Netflix premium subscriptions because it does not require having the full price in their virtual e-payments.

Based on Cess's interview statement, suppliers are possibly using this method through stolen credit cards or Bank Identification Numbers (bins).

"Yes, they use different kind of method some methods that are much cheaper often has more problem. For example, AMEX method, they use cc [credit card] or bins [bank identification numbers] from the internet then start using a fake credit card to create an account, while the one that I usually sell uses GC method or gift card method. Meaning, it is pricier than the other methods, but then 80-90% of the buyers' payment is being paid to create an account," Cess answered, on the question of whether or not they knew where the cheaper premium subscriptions came from.

The Mysterious Origins

One of the common things that premium subscription accounts resellers Sushi, Vel, and Ad shared, is that they themselves are unaware of where and how their premium account products were obtained by their respective suppliers.

Vel is a reseller of various premium accounts including Netflix and Spotify. She started to sell these as a source of income during the pandemic. As a seller, her job entails her to edit the emails and passwords of the unauthorized premium accounts that she buys from her supplier. Though she called those accounts unauthorized, she does not know for sure whether they are hacked or legitimately purchased. Vel buys those accounts for a price of one thousand pesos and makes use of them by changing their existing login credentials when a buyer purchases one.

"I am the one who are creating accounts and will give it to the customers. In exchange, they will send money through online bank/wallets," Vel stated in a chat interview.

Similarly, Sushi does not know how their supplier creates their premium subscription accounts. The accounts that Sushi sells are of full warranty, meaning that in the event of disabling and other technical issues, it will be fixed or replaced. Other than that, they expressed no more information on how those accounts were obtained and where they came from.

Ad, who is a neophyte seller, resells the premium accounts that his co-worker creates. He is likewise unaware of the process involved behind it. Ad did not need any sort of capital to enter this business, since his duty is merely to find customers who will be interested to avail cheaper Netflix and Spotify subscriptions.

Buyer Perspectives

A buyer under the name of "Jen" have availed a cheaper Netflix premium subscription from her friend. She described it as similar to using a legitimate Netflix premium plan except, with her friend's services, she is able to save more cash by paying less than the original price. Despite the possibility of using illegal premium accounts, Jen continuously avail this kind of service for the reason that it is budget-friendly and convenient.

"… Why would it be cheaper if [it's] directly from Netflix? Obviously [it's] from an illegal source. I choose buying from my friend since [it's] almost 4 times cheaper. Before pandemic and before knowing that there are sellers who sell this account, we pay 550 pesos monthly for 6 months, that more than 3000 pesos. But when I saw my friend's post 12 months subscription can only be bought for 2k. Basically I save for more than 4k for a year compared to subscribing directly in Netflix," Jen said in a chat interview.

Jen answered that she does not know how the premium accounts were acquired as well as their origins. Only that she receives her account after communicating with her friend through chat.

"I'll just chat my friend whenever I will avail and send my payment through bank transfer. Then she'll send me the account… she will just give me my account, no other infos as to where she made it."

Expert Opinions

Data Privacy Breach

Through interviews with eight computer-field experts (IT and Computer Science), the cyber dangers behind the use of cheaper premium subscriptions of streaming applications gets unveiled.

Robert Maru De Vera, a software developer from Marley Spoon (a Berlin-based company), claimed that cheaper premium subscriptions are being sold online by hackers not mainly for the purpose of earning, but to mine personal information from people to be sold and used in scamming activities such as identity theft and extortion.

In a Facebook chat interview, he stated, "As for the subject of Netflix credentials being sold in the black market, they aren't being sold there to provide a cheaper Netflix subscription to other individuals. After all, piracy is always ever present and if someone were to try to buy cheap Netflix, they might as well just pirate the shows they want to watch at no cost to themselves.

The reason these accounts are being sold in the black market is most likely as part of a larger scheme to mine personal information from swathes of individuals and use these to perform identity theft and similar scamming activities. Some hackers specialize in collection of these log in credentials, so they collect these *en masse* then sell them in bulk to individuals or entities who would be capable of using these login credentials to say get more information about a certain individual then through social engineering, eventually apply for loans using that person's information or maybe plain extortion."

Asked to confirm De Vera's professional claims, former test engineer and current Quality Assurance (QA) Manager for Glints Singapore Aimee Kristel Santos agreed that these purposes of mining personal information with the use of cheaper subscriptions are indeed possible to happen.

"Yes, I believe so too. If real users engage in this activity, they get access to email, bank information, stuff like that which ultimately contains your identity, logins to social sites, access

to address, your circle of friends, where it could endanger not only that person but also family and friends."

However, a contrasting response came from Christian Angel, a consultant who handles cyber security matters in Manila Bulletin. According to him, it would be impossible for hackers to mine personal information if they themselves are the ones creating premium accounts illegally.

In a google form interview, Christian Angel said, "I think this is wrong. Logically thinking the hackers are the one who's creating the premium accounts with random information using illegal methods. With this [it's] really impossible for them to mine personal information."

Nevertheless, he also shared in the interview that the cheaper Netflix and Spotify subscriptions being sold online are not safe to use. He said that those accounts were obtained with the use of illegal means.

Another expert is Carl Steven Velasco, a Junior QA from Offshorly, who affirmed the possibility of De Vera's statement. In a google-form interview asking his opinion on cheaper subscriptions being used to mine personal information, he answered, "Yes, since when subscribing to those services, user must provide some personal details which can be used by the hackers."

Regarding availing these cheaper premiums from online sellers, Software Engineer Louie Gonzales expressed his perspective on its safety or lack thereof.

"I think the security of availing cheaper subscriptions depends on how aware they are of the billing information used by sellers. If cheaper subscriptions can be availed without having knowledge about this, it cannot be said that it is safe to purchase cheaper subscriptions because they may already be using the customer's information. Or worse, they are already using fraud," said Gonzales.

Eau Benetton Lim, also a Software Engineer, shared the pros and cons of purchasing these cheaper subscriptions. The pros, he said, is that they are cheap and affordable, while the cons would be that there is no assurance and no security involved in these services. This was seconded by Project Manager Lhander Miranda's answer to the same question. He said that as an IT professional, he would not recommend buying cheaper subscriptions online when it comes to safety and security.

Gonzales and Miranda agreed with De Vera's earlier notion that cheaper premium subscriptions are being sold for the purpose of mining personal information. In Gonzales' answer, he pointed out the importance of educating users on data privacy. "This can actually be true because hacking and fraud in the use of technology is not new. I think even if there is no official context about this, users should be educated on data security so that all transactions we do using any technologies are safe," he said.

Miranda on the other hand emphasized that "information is powerful" in his answer from the google form interview.

"As an IT professional, information is very powerful, and to answer the question, yes there is a big possibility that some people may use user's data to create an information that may lead to serious problems."

MOD APKs

As mentioned earlier, one of methods done by suppliers to obtain unlimited and cheaper premium subscriptions is by creating a cracked or pirated versions of entertainment streaming applications. Those apps are called MOD APKs, APK, or simply mods.

Santos likened these mods to cheats that gives unlimited gems, money, or health, which destroys the *game*. Adding gravity to De Vera's statements, she explained how mods work and how it can potentially endanger one's online privacy.

"Depending on the intent of the Black Hat Hacker, scripts can be incorporated in the mods to steal your login credentials, bank details etcetera and these can be sold to other people for money purposes. These "modified apps" can't be uploaded or downloaded by the users thru Google App or App Stores because it is already altered and app stores usually have verifications in place, so usually, hackers who want to earn in this way share a link for users to access and they download the app there."

In the previous interviews with various cheaper premium account sellers, some of them disclosed that their products are mods or cracked version of the apps. The other sellers, however, were unaware of where and how their premium accounts were acquired.

Christian Angel discouraged the use of APKs or mods in accessing premium subscription. He mentioned a process called "Rooting", which can enable malware to enter and control devices.

"[It's] not really recommended to use these cracked [APKs], Most of these apps requires the Phone to be Rooted (Rooting is the process of allowing users of the Android mobile operating system to attain privileged control) if your phone is rooted these apps will abuse it to escalate controls on your phone such as installing malware.

A malware can even download other mobile apps without your consent. By installing the cracked Spotify or Netflix APK into your phone, you will be putting your data at a huge risk. From a glance, some APKs may look genuine, however, they may be designed to steal critical data from your device. They can be used to tap passwords of some online payment accounts such as PayPal, Paymaya or GCASH. In general, it affects the [behaviour] of your mobile phone. [Let's] keep in mind that nothing in this world is free. You may only enjoy an instant gratification because you are not paying at that moment. However, you will still pay for that item later on," Christian Angel explained.

Meanwhile, Velasco confirmed that APK mods effectively works similarly as the original applications, with Lim agreeing that those indeed are pirated versions of the official apps. "The possible danger would be there might be a virus that can harm your device or get your personal details saved in your device," Velasco added.

An existing study in 2018 published by the Institute of Electrical and Electronics Engineers supports these responses expressed by the interviewed experts. In K. Grammatikakis, A. Ioannou, S. Shiaeles and N. Kolokotronis' *WiP: Are Cracked Applications Really Free? An Empirical Analysis on Android Devices* (2018), the study compared 25 applications, between the official ones and the cracked third-party versions, on the premise that the widespread use of smart devices such as smartphones and tablets is an opportunity for malware to spread.

Based on the experimental results of a behavioral analysis conducted between the official and the third-party cracked applications, the researchers then classified the cracked applications as "malicious or benign". According to them, the cracked applications regularly used more resources and *"request access to more (dangerous) permissions than their official counterparts."* (K. Grammatikakis, A. Ioannou, S. Shiaeles and N. Kolokotronis, 2018)

Despite these virtual dangers surrounding the use of APKs or cracked applications in order to access premium entertainment sites for free or for a lower price, there are still ways however, for online users to protect themselves from malicious malwares and third-party hackers.

Santos said that internet users should only get their applications from official App Stores. This is to ensure that the apps they are installing are legitimate and safe to use.

"Only avail on official App Stores because these app stores usually have verifications already in place for the apps so you can be sure that they are safe to download. Also, when signing up, legitimate apps usually have Terms of Use before asking to subscribe to plans. Aside from this, legitimate apps have security features to verify your email, your phone number and codes sent out to ask for payment from your banks. So, you'll know they are legitimate merchants," she advised.

Santos added, "It'll be ultimately your responsibility to protect your own identity so just to summarize, don't believe in what you see, try to dig deeper and always question first, because there are a lot of fake apps or news nowadays."

Christian Angel and Miranda, on the other hand, provided more technical advices on online safety. Angel recommended social media users to always use two-factor authentication since it is free.

And for those who already availed on APK mods of cheaper premium subscription accounts, he advised, "If your Device is not rooted, uninstall these cracked [APKs] and monitor your device for strange behavior. If your device is rooted, backup your important data and do a factory reset on your phone. If you purchased discounted premium accounts, I strongly suggest that you should stop using them."

As for Miranda, his advice is to trace the APK user's email. "Stop using the application, then try to trace if your email and other information is in other platform. Email is the easy way to trace your information."

The Bigger and Darker Industry

Based on the investigations, it is certain that an industry is booming out of the illegal distribution of hacked premium subscription accounts, as well as the online streaming of pirated films and music. Whether or not this industry is bigger than what is virtually visible, however, is still indeterminable.

The trails of this investigative report showed that this emerging industry of digital piracy uses illegal methods, specifically hacking and pirating, for various profitable and darker purposes.

These rising online black market of pirated streaming sites and hacked subscription accounts, undoubtedly attacks and victimizes the creative industries. A Manila Standard news article in October 2020 based on a report from Media Partners Asia, revealed that the industry of video producers, distributors and aggregators were set to lose $120 million.

This is because despite the growing presence of legal subscription video on demand (SVOD) in the Philippines, piracy remains prevalent among Filipinos. In fact, according to a YouGov September 2020 survey, the Philippines ranked as third in the percentages of consumers who admitted to accessing streaming sites.

As for the illegal distribution of hacked premium subscription accounts, the potential targets here are not just consumers and banks, but also larger companies, even including governments. Through cracked applications and other hacking methods, malicious malware can proliferate in devices for the purpose of harvesting bulks of personal and confidential information, to be used for fraudulent purposes, as many of the interviewed experts confirmed. They can be used for identity theft, extortion, bank loans scam, selling of personal data to other companies, and many other activities violating one's online data privacy.

This new wave of a virtual illegal industry is something that is yet to be addressed strongly by existing Philippine laws; and one that is yet to be improved upon by the government in terms of updating related laws, creating new specific laws altogether, and a more effective implementation of it.

The interface of The DarkMarket, where bulk credential transactions are found to hack legitimate online streaming sites accounts. Retrieved from: Inside the 'DarkMarket' Prototype, a Silk Road the FBI Can Never Seize | WIRED

PART 3: The Economic Impacts of Digital Piracy

In October 2016, the PNP Anti-Cybercrime Group arrested Rainier Tamayo, the personality behind the site 'www.rainiertamayo.com' for illegally streaming pirated movies and TV shows on his website.

Then PNP-ACG Public Information Office chief Jay Guillermo told the media that Tamayo was earning at least P120,000 a month from advertisement revenues on his website, which had recorded around 5,000 audiences during its operations.

"A day after it [movies] was shown, andun na sa website. 'Pag nakita mo free online, bakit ka pa pupunta sa cinema?" Guillermo stated, pointing that Tamayo's illegal activities were directly robbing directors and personnel working in the film industry of their livelihood.

Film Development Council chairperson Liza Diño-Seguerra also talked about the negative impact of piracy in her Sunday Times Magazine article released in January 2021. According to her, piracy have not only affected the profits generated from films, but also caused a huge devastation on the self-esteem of local film developers.

From March to June 2020, during the initial stages of COVID-19 lockdown in our country, the Intellectual Property Office of the Philippines (IPO-PHL) have received 67 reports of intellectual property violations. These violations include the illegal reproduction and streaming of copyrighted materials such as films, TV shows, and even electronic books.

As emphasized by Diño-Esguerra, the pandemic had not only affected the health sector in the Philippines, but also served as a "double-edged sword" for film content production. It might have made film contents easily accessible online through streaming and pay-per-views, but it also gave way to the rise of online video piracy.

In October 2020, Media Partners Asia reported that in the Philippines, video piracy had been depriving media services that uses legal Subscription Video on Demand (SVOD) of $120 million dollars in annual revenue.

These legal SVODs include streaming sites like Netflix, Viu, HBO Go, and Disney+.

In the same survey, 47 percent of Filipinos had admitted to canceling their subscriptions to streaming services due to piracy. Most users think that using illegally acquired streaming accounts or watching and downloading media contents from illegal sites is much more accessible and practical.

Another practice that contributes to the revenue loss of streaming site Netflix is the 'password sharing'. Password sharing refers to the act of "sponging off" other people's streaming accounts by sharing its login credentials to multiple users, who can stream Netflix contents simultaneously using different devices. This method is commonly utilized in by families or group of friends to legally avail cheaper Netflix accounts, although some Black Hat hackers are also exploiting this feature to leach off of other people's account without the owner's consent.

Cordcutting.com (2019) revealed in their study that this practice had been costing Netflix a staggering amount of $192 million every month. They also stated in the same study that "Netflix is the service which users sponge off other people for the longest", with an average duration of 26 months.

This was not the first time that Netflix was exploited by cyber criminals and pirates. In April 2017, an anonymous hacker group known for their alias 'The Dark Overlord' stole the fifth season of the Netflix series *Orange Is The New Black* and demanded a "modest" ransom for it. In their ransom note, the group also claimed that they had stolen "dozens of titles" from other major studios like ABC, CBS, and Disney and that if the ransoms are not paid, they would be releasing these series to the public.

Larson Studios, the post-production company behind the Netflix series, had quietly paid the hackers $50,000 in crypto currency, as it had been revealed that the hackers were able to acquire these contents by hacking an old computer at Larson Studios that was still running on Windows 7.

Larson's Studios chief engineer David Dondorf explained that the hacker group were primarily looking for old computers to hack and that Larson Studios were not their primary target.

"They were basically just trolling around to see if they could find a computer that they could open. It wasn't aimed at us." Dondorf stated in an exclusive interview with media company *Variety* in June 2017.

The local creative industry had also been subject to the negative economic impacts of online piracy.

During the online screening of the 46th Metro Manila Film Festival (MMFF) held from December 2020 to January 2021, Best Picture awardee "Fan Girl" have recorded around 10 to 20 pirated links every hour. This led the Optical Media Board (OMB) to file a lawsuit against 15 civilians for illegally streaming the said movie on their social media accounts.

Consequently, the festival was only able to accumulate P19 million through ticket sales or merely 1.9 percent of more than P995 million revenue of the 2019 MMFF.

This incident urged Creative Industry and Performing Arts special committee chair and Pangasinan Representative Christopher De Venecia and 30 other house members to file a resolution that will investigate the online piracy that took place during the film festival.

The lucrative business of digital piracy that continuously fuel the operation of virtual black market was proven to have more negative impacts than benefits in our economy. Open Syllabus director Joe Karaganis enumerated in his book *Media Piracy in Emerging Economies (2011)* the harmful effects of piracy.

According to him, piracy can

- 'generate unemployment' as it robs people from creative industry of their livelihood,

- 'encourage tax evasion' as pirates are not legally bound by the law to pay tax,
- infringe intellectual property,
- provoke unfair competition in economy,
- generate inflation and,
- stimulate organized crimes.

In a hindsight, digital piracy is not just all-beneficial to its users. It also poses dangers of data breach which gathers information to be used for malicious intent. Nothing can really be acquired easily in this world, even digital piracy and streaming are paid for by consequences.

Legitimate Subscription Video on Demand companies who offer streaming services. Retrieved from: [Successful SVOD Companies Set to Rule the Era of Online TV (cleeng.com)]

PART 4: The Loopholes in the Local Law that Enable the Emergence of Virtual Black Market

There have been numerous laws established to address the growing piracy problem in our country. For an instance, Republic Act 8293 or the *Intellectual Property Code of the Philippines* strengthened the intellectual rights of copyrighted media by prohibiting unauthorized people from manufacturing, using, and commercializing patented and copyrighted products.

R. A. 10175 or the *Cybercrime Prevention Act of 2012* also criminalizes the illegal acquisition of any digital copyrighted material. This law also states that any crime under the Revised Penal Code is classified as cybercrime if done through the internet or a computer, which further strengthen the economic rights of digital media producers.

However, why is it that even after the enforcement of these laws, more and more people are still engaging in digital piracy? Even founding a business industry that caters to the commercial selling of illegally distributed media contents and hacked streaming sites accounts?

The answer primarily lies in the law itself.

In a 2019 interview with Inquirer.net, OMB chief and lawyer Anselmo Adriano stated that they cannot criminalize people who watch or share illegally distributed or pirated movies online, due to the gaps in the law addressing the piracy of optical media contents.

Section 19 (a) (1) of R. A. 9239 or the *Optical Media Act of 2003* specifically states that only those who engage in the production, replication, importation, and exportation of pirated optical media contents can be penalized by the law. Moreover, this law is only applicable to media contents that are produced in CDs, DVDs, and Blu-ray discs, which means that illegal distribution of hacked streaming accounts cannot be penalized by this law.

Another law that can be used to combat this crime is the R. A. 8484 or the *Access Devices Regulation Act of 1998*, amended in 2019 as R. A. 11449, which seeks to protect credit card users against online fraudulent. In its amended version, the law declares the hacking of banking systems as a form of "economic sabotage". However, this law only tackles cases that involve credit card fraudulent. This law doesn't have the teeth to punish hackers who generate login credentials through combo lists and other illegal means.

The gap in this law could be filled by R. A. 8792 or the *Electronic Commerce Act of 2000* which seeks to fine anyone found guilty of unauthorized access or interference of ICT systems with the purpose of corrupting, altering, stealing, or destroying information, without the knowledge and consent of the owner; and R. A. 10173 or the *Data Privacy Act of 2013* which recognizes the need for privacy protection of information encoded in the digital space.

Lastly, R. A. 10088 or the *Anti-Camcording Act of 2010* prohibits and penalizes the "unauthorize use, possession and control of audiovisual recording devices for the unauthorized recording of cinematographic films and other audio-visual works, including their soundtracks in an exhibition facility."

However, just like the other laws enumerated above, these provisions failed to recognize the emerging black market of cheaper subscription accounts and pirated online media contents that were acquired through illegal means, not only limited to the techniques mentioned in the second part of this series.

Intellectual Property consultant Ann Edilon weighed in on this topic by stating that the virtual black market of cheaper subscription accounts can only be abolished if the government continues to implement new laws and amendments to the existing laws "for the purpose of adding more teeth to online enforcement". She also emphasized the importance of awareness to fight these crimes.

"Cheaper subscription accounts acquired via hacking, cracking codes, and combo lists are more centrally a cybercrime concern and perhaps only peripherally an IP concern. However, this is tied to our findings of increasing criminal activity online which also affects intellectual property [...] We believe in further strengthening the whole of society approach by continuous cooperation of both the public and private sector in removing barriers in enforcement and strengthening public knowledge on these criminal activities online." said Attorney Edilon.

Glints Singapore QA manager and former test engineer Aimee Kristel Santos also agreed with this, saying that "there are very low to none" authoritarian powers issued by the government to control these illegal activities.

"For example, the Data Privacy Act, if I recall correctly, they only penalize people who do illegal activities on this matter. They lack the implementation and follow through unlike other countries who are very strict on this matter that they actually ban or issue imprisonment consistently. [In our country], it's most likely up to the private companies to sue and to track illegal sites [who copy movies from their platforms.]" Santos stated.

On the other hand, law expert Antonio "Tony" La Viña had a differing opinion on the issue. He pointed out that even though the illegal hacking of streaming sites are "theoretically" punishable by the law, cracking it down by penalizing individual buyers and sellers, who are commonly engaging in this crime, is difficult.

"Depende 'yan ['yung punishment]. Theoretically, yes [they can be penalized by the law]. Pero kung maliliit lang naman, nobody will bother." Attorney La Viña stated.

Even though various laws can be utilized to gradually eradicate the commercialization of illegally acquired subscription accounts and online media contents, this growing industry is currently unrecognizable under the local law.

This just proves that there are still many gaps in our legal system that enable the distribution of pirated media contents and illegally acquired streaming accounts. Given this fact,

we are now face with the question: How can we reduce and slowly abolish this industry to prevent its damaging impacts, not only in the local creative industry but also in our economy?

A photo of Atty. Antonio "Tony" La Viña, who commented through a legal perspective on piracy in an interview.

PART 5: Combative and Comprehensive Solutions vs. Digital Piracy

Clampdown on Online Piracy

In the Philippines, online piracy is still one of the biggest problems faced by the creative industries. As mentioned in Part 3 of this report discussing the economic impacts of piracy, Media Partners Asia revealed how media services using legal SVOD are set to lose $120 million of their annual revenue due to the rampant video piracy in the country.

The Philippines is not alone in its existing prevalence of online piracy. Neighboring South East Asian countries such as Malaysia and Indonesia likewise had this similar problem. The difference between them and the Philippines, however, is that these countries managed to reduce the percentages of their citizens accessing online piracy services. This was showed in the survey conducted by YouGov in October 2020. In the same survey, it was reported that the Philippines ranked among the highest in online piracy with forty-nine percent of Filipinos admitted to having accessed piracy streaming websites and torrent sites.

To reiterate, Malaysia and Indonesia saw a considerable amount of reduction in online piracy streaming over the last twelve months since the survey was conducted; Indonesia in 2019 had 63% of consumers who accessed piracy websites. By 2020, their percentage visibly diminished by a massive 55%, with now only 28% of users admitting to streaming piracy websites.

Same as Malaysia, who saw a 64% reduction when it came to accessing sites with pirated contents.

Now, the question that must be asked: what is it that Malaysia and Indonesia have, and are benefitting from, that is missing in the Philippines?

This missing puzzle piece for the country to effectively combat online piracy is, simply, government action and cooperation specifically addressing this problem through updated policies.

In a news report by Cision PR Newswire, it was said that the key variable in Malaysia and Indonesia was a proactive initiative by the government to block piracy sites. The Malaysian and Indonesian government have managed to actively block websites containing piracy services and contents, which influenced viewing-habits and lead to the large reduction of online consumers accessing piracy sites.

A similar approach is being filed in the Philippine congress through the bill entitled the "Online Infringement Act" or Senate Bill 497, which seeks to propose a mechanism for regulatory site blocking, giving the Intellectual Property Office of the Philippines (IPOPHL) a

legal framework to guarantee that Internet Service Providers (ISPs) will disable sites that are reported for “infringing copyright or facilitating copyright infringement."

In the same YouGov survey report, 53% of Filipino online consumers believe that the best measure to combat online piracy is to have "a government order for internet service providers to block pirated websites."

Attorney Edilon of IPOPHL agreed with this notion by reiterating the importance of "stronger legislative/policy system" in combating this online brick and mortar and market. She also said that certain changes in our laws/policies should be observed to make it possible.

"A stronger legislative/policy system should be in place especially now in the online world where some of our laws/policies are not updated to go after these IP criminals online." she stated.

Healer, the Black Gat hacker we interviewed, believes that the fight against piracy lies on the comfort and quality that the product has to offer.

“The way it is, digital pirates are beating copyright holders fair and square at their game. The best way to combat piracy is to… provide a better product.” The hacker explained.

Since there are currently no mechanisms and legal authority for enforcement to take down piracy websites, a legislative system that will give more teeth to the current and digital violations on intellectual property rights, must be put in place to protect the creative industries who are already struggling to make a profit in the country. On the side of the legal providers, the best way to defeat this illegal industry is to step up their game in the competition. Provides what pirates have failed to offer.

Detecting Parasites

Meanwhile on the side of legal SVOD services, Netflix is considering a crackdown against the issue of password sharing to protect subscribers from ineligible and unauthorized users. They plan to do this with the use of account verification code sent thru text or email.

According to a CBS News report, this new feature is still being tested on a small, random scale, with the Netflix Spokesperson saying that it is designed to make sure that people using the accounts are “authorized to do so.”

Incomplete Protection

Going back on the subject of illegal distribution of premium subscription accounts, Attorney Tony La Viña stated that these online black market services are in violation of the country’s cybercrime law and the Intellectual Property rights.

Alas, despite the current available measures against such businesses, these laws cannot at all times, protect the creative industries because it will not realistically go against small-time

digital piracy trades; for the reason that they are expensive and that there is a lack of concern when only individuals or a small group of people are involved.

"Depende 'yan. Theoretically, yes. Pero kung maliliit lang naman, nobody will bother, diba? But if it becomes a big business then pwede silang habulin. I wouldn't go after small sellers here and there," Atty. La Viña stated, when asked if indirect sellers and buyers of illegal premium accounts can be punished by the mentioned laws.

Law regulation and enforcement from specific authorities only ever comes to these online black markets of illegal premium subscriptions, as well as piracy sites, if they are large enough to cause huge and noticeable damages to creative companies, or according to Attorney La Viña, when they are massive enough to become a criminal enterprise similar to a mafia.

In other words, these problems can only be addressed effectively when they become huge enough to cause alarm and complaints.

This shows the irony that entails the system supposedly set to protect intellectual properties against online piracy. Authorities cannot always act based on a flawed legislative safeguard. However, the concept of updated, future-proof solutions, suited to realistically adapt to the modernized contexts of online piracy, are not too late to be achieved.

The Philippine Congress where the bill entitled the "Online Infringement Act" or Senate Bill 497 is being filed. Retrieved from: Philippines Takes Step to Protect Children | Human Rights Watch (hrw.org)

REFERENCES

Part 1

Asia Video Industry Association. (2020, October 20). New survey SHOWS Philippines among highest in online piracy in Southeast Asia. Retrieved March 30, 2021, from https://www.prnewswire.com/news-releases/new-survey-shows-philippines-among-highest-in-online-piracy-in-southeast-asia-301154664.html

Ballano, Vivencio. (2016). Tracing Media Piracy: Current and Future Trends. 10.1007/978-981-287-922-6_7.

Ballano, Vivencio O. (2016). Sociological Perspectives on Media Piracy in the Philippines and Vietnam. Retrieved March 30, 2021 from https://link.springer.com/content/pdf/bfm%3A978-981-287-922-6%2F1.pdf

Constitutional Rights Foundation. (2008). BRIA 23 4 b digital piracy in the 21st century. Retrieved March, 2021, from https://www.crf-usa.org/bill-of-rights-in-action/bria-23-4-b-digital-piracy-in-the-21st-century

Kenton, W. (2021, March 16). Black market. Retrieved March 27, 2021, from https://www.investopedia.com/terms/b/blackmarket.asp

Newsbytes.PH. (2020, October 21). Content producers ask ph gov't to block illegal streaming websites. Retrieved March 30, 2021, from https://newsbytes.ph/2020/10/21/content-producers-ask-ph-govt-to-block-illegal-streaming-websites/

Part 2

Grammatikakis, K., Ioannou, A., Shiaeles, S., & Kolokotronis, N. (2018, October 29). Wip: Are cracked applications really free? An empirical analysis on android devices. Retrieved March 29, 2021, from https://ieeexplore.ieee.org/document/8511970

Campos, O. V. (2020, October 15). PH set to lose $120m to video piracy in 2020. Retrieved March 29, 2021, from https://manilastandard.net/mobile/article/336880

Europol - DARKMARKET: WORLD'S LARGEST ILLEGAL DARK WEB MARKETPLACE TAKEN DOWN. Retrieved on March 28, 2021 from https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

Authy - What Is Two-Factor Authentication (2FA)?. Retrieved on March 28, 2021 from https://authy.com/what-is-2fa/

Offensive Security Society – 3 Main Types of Hackers. Retrieved on March 28, 2021 from https://oss.org/featured/3-main-types-of-hackers/

Duo Labs Report - State of the Auth - Experiences and Perceptions of Multi-Factor Authentication. Retrieved on March 28, 2021 from https://duo.com/assets/ebooks/state-of-the-auth-2019.pdf

LastPass - The Psychology of Passwords: Neglect is Helping Hackers Win. Retrieved on March 28, 2021 from https://www.lastpass.com/psychology-of-passwords

Widup, S., Spitler M., Hylender, D. Bassett, G. - 2020 Verizon Data Breach Investigations Report. Retrieved on March 28, 2021 from https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

Part 3

Campos, O. V. (2020, October 15). PH set to lose $120m to video piracy in 2020. Manila Standard. Retrieved from https://manilastandard.net/mobile/article/336880

Diño-Seguerra, L. (2021, January 17). Piracy: A perennial problem in Philippine Cinema. *Film Development Council of the Philippines*. Retrieved from https://www.fdcp.ph/notes-from-the-chair/piracy-perennial-problem-philippine-cinema

Mercado, N. A. (2021, February 15). House probe on reported 'online piracy' of 2020 MMFF sought. Inquirer.net. Rerieved from https://newsinfo.inquirer.net/1396097/house-probe-on-reported-online-piracy-of-2020-mmff-films-sought

Nicholson, T. (2019, March 1). Your Sponging Off Other People's Account Is Costing Netflix $192M A Month. Esquire Mag. Retrieved from https://www.esquiremag.ph/culture/movies-and-tv/your-sponging-off-other-peoples-accounts-is-costing-netflix-dollar192m-a-month

Peralta-Malonzo, T. A. (2016, October 5). Police arrest man for illegally streaming films, TV shows. *Sunstar Philippines*. Retrieved March 27, 2021 from https://www.sunstar.com.ph/article/102020/Business/Police-arrest-man-for-illegally-streaming-films-TV-shows

Pedersen, E. (2017, April 28). 'Orange Is The New Black': Hacker Says He Stole New Season, Demands Ransom From Netflix. Deadline. Retrieved from https://deadline.com/2017/04/orange-is-the-new-black-hacker-blackmail-netflix-1202079534/

PNP - ACG (2016, October 6). IT EXPERT ARRESTED FOR ONLINE PIRACY. *PNP Anti-Cybercrime Group*. Retrieved March 27, 2021 from https://acg.pnp.gov.ph/main/press-releases/81-it-expert-arrested-for-online-piracy

Roettgers, J. (2017, June 20). How Hollywood Got Hacked: Studio at Center of Netflix Leak Breaks Silence (EXCLUSIVE). Retrieved from https://variety.com/2017/digital/features/netflix-orange-is-the-new-black-leak-dark-overlord-larson-studios-1202471400/

Part 4

Balinbin, A. L. (2019, September 26). Hacking of bank systems a form of 'economic sabotage' under new law. *Business World*. Retrieved March 27, 2021 from https://www.bworldonline.com/hacking-of-bank-systems-a-form-of-economic-sabotage-under-new-law/

Co, A. C. L. (2020, June 23). *Hacking In A Time of COVID-19*. ACCRALAW. Retrieved from https://accralaw.com/hacking-in-a-time-of-covid-19/

Lalu, G. P. (2019, October 28). OMB chief admits they can't address online piracy due to loophole in law. *Inquirer.net.* Retrieved March 27, 2021 from https://technology.inquirer.net/91778/omb-chief-admits-they-cant-address-online-piracy-due-to-loophole-in-law

Magdirila, P. (2014, March 5). With new Cybercrime Law in place, Filipinos could face jail time for piracy. *Tech in Asia*. Retrieved March 27, 2021, from https://www.techinasia.com/cybercrime-law-place-filipinos-face-jail-time-piracy

Part 5

Asia Video Industry Association (2020, October 19). New surbey shows Philippines among highest in online piracy in Southeast Asia. *Cision PR Newswire*. Retrieved from https://www.prnewswire.com/news-releases/new-survey-shows-philippines-among-highest-in-online-piracy-in-southeast-asia-301154664.html

Pangalangan, P. A. (2020, October 20). Curbing the impact of rising digital piracy. *Business World*. Retrieved from https://www.bworldonline.com/curbing-the-impact-of-rising-digital-piracy/

Cerullo, M. (2021, March 13). Netflix testing a new feature to curtail password sharing. *CBS News*. Retrieved from https://www.cbsnews.com/news/netflix-password-sharing-crackdown-feature/