Pragya Chaudhari

CYBR 641 Section 01

Professor Adam Lippe

March 01, 2020

Table of Contents

Introduction

The Internet has become the most important commodity for people to operate on a daily basis. “The Internet is a global network of billions of computers and other electronic devices. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and do much more.” (Internet Basics: What is the Internet?) Access to the Internet means an easy path to a vast array of information from news to social media. In today’s fast-paced world, the Internet has become the most important platform for people to connect with each other easily and access the information they need. To ensure, people are connected to the Internet, Internet Service Providers (ISP) play an indispensable role. “An Internet service provider (ISP) is a company that provides access to the Internet. Access ISPs connect customers to the Internet using copper, wireless or fiber connections. Hosting ISPs provide email, web-hosting, or online storage services. Other services include virtual server, cloud services, or physical server operation. Transit ISPs interconnect other ISPs.” (Connecting to the Internet, 2014) Essentially, an ISP is the gateway to access the Internet and is responsible for routing Internet traffic, determining domain names, and managing the network infrastructure. Unfortunately, such ease of access to the digital world makes Internet users vulnerable to cybercriminals who can access the Internet just as easily. They can easily conduct malicious activities to harm unsuspecting users by using malware. In the article, *Facebook Says 14 Million Accounts Had Broad Array Of Personal Data Stolen,* NPR reported that 30 million Facebook accounts were compromised because of a security breach in September 2018. Malware is malicious software which includes viruses, adware, spyware, worms and trojans with the intent to compromise the privacy of the user as well as their computer’s security. With the kind of unfiltered access to the Internet available to users, it is easy for them to fall prey to such malicious attacks, especially given the fact that there are currently no requirements for ISPs to prevent, block or filter malicious content and traffic running through their network.

However, one of the most significant positive impacts that the Internet has had on the modern world is the creation and rapid progression of an unprecedented stream of extraordinary innovation. With the help of its inherent free-flowing and all-pervasive nature, the Internet has opened to its users a plethora of resources of knowledge, commerce, communication, and technology worldwide. To ensure the continuance of such exceptional innovation, it is necessary for the Internet to flourish without restrictions. On the other hand, it is also necessary to have some

governance in the form of legislation and/or liabilities in order to prevent the misuse of the Internet by cybercriminals or even ISPs who sometimes may exploit their ISP privileges. For example, a large ISP which also happens to be the owner of a popular movie streaming service might provide a "fast lane" to its own content's traffic, when compared to other such streaming services' traffic. This debate has continued for years as the US Congress has made different rulings over time. In 2015, the Federal Communications Commission (FCC) established a law to endorse the "Open Internet" and protect it. "Specifically, the Open Internet Order adopts bright-line rules that prohibit blocking, throttling, and paid prioritization; a rule preventing broadband providers from unreasonably interfering or disadvantaging consumers or edge providers from reaching one another on the Internet; and provides for enhanced transparency into network management practices, network performance, and commercial terms of broadband Internet access service." (Protecting and Promoting the Open Internet, 2015) But only a couple of years later in December 2017, FCC overturned this law that imposed Net Neutrality and also repealed the legislation that viewed the Internet as a utility, just like electricity or water. Because of this indecisive flurry of decisions, ISPs have been operating somewhat without direction in the past decade. This makes proper and streamlined legislation even more important in terms of the rules that govern ISPs.

The objective of this analysis and research is to evaluate the current state of affairs about what ISPs can and cannot do, the laws and rules that govern them, and why they have not been held to the same standards as other service providers when it comes to providing a clean Internet which is devoid of any malicious content. This research paper will also propose how the current situation can be changed through legislation and legal liabilities and how ISPs can be held more accountable for providing such unfiltered access to the Internet, thus making their subscribers vulnerable to attacks targeted at their personal information and privacy. The proposals have been suggested keeping in mind the ethical reasoning and the costs for conducting them.

Current state of affairs for ISPs and what they can and cannot do

The Communications Act of 1934 was a "law that regulates interstate and foreign communication by wire or radio." (Maras, 67) This was originally implemented due to concerns from customers towards telecommunication companies claiming that these companies misused customers' personal information records. This Act was later amended by the Telecommunications

Act of 1996 so that the Internet could be included as part of the broadcasting domain. This Act categorized broadcasting-based providers into “information services” and “telecommunication services”. Title I of the Act regulates information services whereas Title II regulates telecommunication services. Telecommunication services belonging to Title II of the Act are subject to heavier legislative regulation because they fall under the common-carrier rules as laid out by the 1934 Communications Act whereas information services do not. Ever since this regulation-based division, the debate between identifying the Internet as a telecommunication service or an information service has been ongoing until today. In 1996 when the Internet became a more common part of American households, it was categorized as a Title II telecommunication service. In 2005, the FCC revised its stance and reclassified the Internet as a Title I information service. Later on, in 2015, with the Open Internet Order, FCC reverted the classification of the Internet to Title II telecommunication service. However, from the year 2017 to present day, the Internet is classified as a Title I information service. Notwithstanding the political clashes behind this back and forth categorization, the impact it has had on the kind of regulations that can exist and be implemented for the ISPs is substantial. In other words, rules and regulations for ISPs are evolving at a rapid pace even today. For example, the EARN IT Act which aims to amend Section 230 of the Communications Decency Act is currently under debate in the US Congress. This is relevant to ISPs because Section 230 provides ISPs a safe harbor from liability in certain cases of carrying objectionable content.

However, there still have been a sizable number of legislations passed and laws created that govern ISPs and dictate actions that ISPs can take, actions that ISPs are prohibited from, and conditions wherein ISPs can and cannot be held liable. Among the laws that lay prohibitions on ISPs, the Electronic Communications Privacy Act of 1986 (ECPA) is the most notable. ECPA “governs the privacy and collection, access, disclosure, and interception of content and traffic data related to electronic communications.” (Maras, 57) Title I of ECPA consists of the Wiretap Act which regulates interception of content by entities like ISPs in real-time. “Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.” (Electronic Communications Act of 1986, 2019) Title I also prohibits the use of illegally obtained communications as evidence. Title II of ECPA consists of the Stored Communication Act which regulates access to stored content and

non-content records held by ISPs. It protects the privacy of the user and their personal information which is stored with the ISPs.

Another law that played an important role was the Communications Act of 1934 as mentioned previously. The act combined with the Telecommunications Act of 1996 protects privacy and directs that all Internet traffic is treated equally by ISPs. Telecommunications Act of 1996 "requires telecommunications companies to obtain the consent of the customer before using customer proprietary network information." (Maras, 67) Following the footprints of the Communications Act, the Open Internet Order of 2015 also mandated "no blocking, no throttling and no paid prioritization of Internet traffic" (Protecting and Promoting the Open Internet, 2015) by ISPs, which also happen to be the founding principles of the very popular concept of Network Neutrality. Even though in 2017, the Open Internet Order was reversed by the FCC, certain states have since attempted to pass legislations meant for ISPs and aimed at protecting their subscribers' privacy and at reinstatement of the principles of Net Neutrality. In California, the first ever state-level law was passed that restored Net Neutrality and made ISPs liable once again to violation of its principles. "Like the 2015 Order, SB 822 ensures that Californians, not the companies they pay to get online, get to be in control of what sites, apps and services they use. SB 822 bans ISPs from blocking, throttling, and charging websites fees for access to the ISP's subscribers or for fast lanes, which will protect California's economic growth, innovation economy and democratic engagement." (Gov. Jerry Brown signs SB 822, Restoring Net Neutrality to California, 2018). In Maine, Gov. Janet Mills, signed the Net Neutrality bill into law in 2019 with the aim of open Internet for people of Maine. Given these laws directed towards protecting user privacy and net neutrality, it is evident that providing a clean Internet free of all malware to its subscribers is an uphill task for ISPs, since it most definitely requires intercepting Internet traffic to and from subscribers.

There are laws that protect privacy rights of Internet subscribers and restrain ISPs from snooping into the subscribers' Internet traffic and from filtering content. On the contrary, there are also laws that define certain things that ISPs can do or are legally bound to do. An important law that defines the responsibilities of ISPs is the Digital Millennium Copyright Act established in 1998. The act "made it illegal to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that… is primarily

designed or produced for the purpose of circumventing a technological measure that effectively controls access to [protected work].” (Maras, 124) Title II of this act, also known as Online Copyright Infringement Liability Limitation Act - OCILLA, makes it mandatory for ISPs to restrict access to content that qualifies as infringement of the act and remove such content from their servers if they are notified of this infringement from the original content creator. Conducting electronic surveillance of its subscribers is another domain where ISPs are sometimes legally bound to help the government. One such legislation is the Foreign Intelligence Surveillance Act (FISA) which was created in 1978. This act lowered the bar for government intelligence agencies to be able to obtain physical and electronic surveillance warrants. Examples of electronic surveillance include wiretapping, bugging, videotaping, geolocation tracking, a few of which demand cooperation from ISPs. In January 2018, FISA's section 702 which deals with electronic surveillance of non-US citizens located outside the United States, was renewed by President Trump for the next six years.

Despite the premise of this study being the fact that ISPs are not held accountable for not preventing various cyber threats, Denial-of-Service (DoS) attacks and Distributed Denial-of-Service (DDoS) attacks are threats which ISPs do take very seriously. DoS and DDoS attacks weigh a higher value in their minds due to the financial harm they can cause to an ISP, if not stopped. Moreover, DoS and DDoS attacks are also penalized under the Computer Fraud and Abuse Act’s U.S. Code 1030(a)(5)(A). An example of this is when Anthony Scott Clark was found guilty as he launched a DDoS attack against the company eBay. Such attacks cause direct financial harm to ISPs as they overload the servers and the machines crash. On the other hand, ISPs do not show a similar interest in filtering malware from Internet traffic because it does not embody a similar financial loss as DDoS attacks do. “When ISPs’ direct financial interests are at risk, however, they have proven to be more than willing to filter, block, or redirect traffic. And the information about threats flows freely.” (Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs, 2011) Lastly, the Clarifying Lawful Overseas Use of Data (CLOUD) Act was introduced as a part of the Consolidated Appropriations Act in 2018. It made two consequential changes to ECPA. The first change was that ISPs are now explicitly required to respond to law enforcement’s requests to deliver customer information that meet ECPA guidelines regardless of the location where the information is stored. “Second, the act allows foreign governments that qualify under new rules to directly submit requests for information held by U.S.-

based service providers." (Congress Reshapes Legal Requirements for International Access to Communications Information with the CLOUD Act, 2018)

Rules that govern the ISPs

There are several rules that govern and dictate the ISPs. As previously mentioned, one of them is the ECPA which includes Title I and Title II. Title I describes the Wiretap Act whereas Title II describes the Stored Communications Act. ECPA ensures privacy of the subscribers and denies access to their private electronic communications. Online Copyright Infringement Liability Limitation Act, which is part of the Digital Millennium Copyright Act of 1998, protects ISPs from liability provided they take appropriate action once they find out about infringing content being carried by them. The Telecommunications Act of 1996 which amended the Communications Act of 1934 ensured that telecommunications companies did not misuse their subscribers' personal information. Companies would have to get consent from their subscriber before using their personal information. Specifically, under Title 47 of U.S.C. § 222, ISPs have to keep their subscribers' customer proprietary network information confidential.

Another law that governs the ISPs is the Section 230 of The Communications Decency Act of 1996. The Communications Decency Act of 1996 "was designed to protect children from exposure to indecent material. A violation of this Act occurs when an individual knowingly transmits indecent material to a person younger than 18 years old." (Maras, 72) This section states that an ISP cannot be held responsible for indecent content created or circulated by another content provider. Lastly, the Stop Enabling Sex Traffickers Act and the Fight Online Sex Trafficking Act (SESTA/FOSTA) enhance the Communications Decency Act of 1996 which had a loophole wherein ISPs were immune to liability even if they did not take down websites that promoted sex trafficking. SESTA/FOSTA Acts address this shortcoming and make ISPs accountable for hosting sex trafficking websites.

Why ISPs are not held to the same standards as other service providers

If one were to look at their monthly expenditure, they would come across utility bills such as water, electricity, gas, cable television and so on. Also present would be the monthly Internet bill. This begs the question whether or not the Internet is also a utility, just like electricity and

water. And the answer is that the Internet is in fact not very different from such utilities. Today, just like water, the Internet is available to the general public at a monthly charge. Just like water, a subscriber pays for Internet access in proportion to their consumption. And just like water is distributed by the municipal water service provider, the Internet is distributed by the city's Internet Service Provider. Moreover, Title II of the Communications Act of 1934, interchangeably uses the terms "common carrier" and "utility". Then, why is it that on one hand, water subscribers receive pure and potable water in their homes, whereas on the other hand, Internet subscribers receive Internet traffic that can potentially be carrying malicious content including viruses, worms, spyware, bots and other malware? In other words, why are ISPs not held to the same standards as other utility service providers?

Speaking from a utility point of view, this is a very relevant question. However, if one were to dig a little deeper into the subject, there are multiple reasons for this. Firstly, while municipal water companies have laws directed towards them that are very straightforward, ISPs on the other hand struggle to understand the do's and don'ts of their privacy law. Many courts and scholars have mentioned how the Electronic Communications Privacy Act (ECPA) lacks clarity and is confusing in terms of legality. Because of this confusion, with no clear liability nor immunity, and because of a fear of "over-surveillance", many ISPs refrain from new and invasive forms of Internet traffic filtering, just so that they can avoid legal culpability and potential lawsuits. Given the presence of a rather confusing privacy law, and the absence of a directed legislation compelling ISPs to provide clean Internet, the risk of legal liabilities is too drastic for ISPs to act out of a purely good Samaritan intention. Whereas a municipal water company will never have to face any legal consequences whatsoever for providing "too clean" water. Therefore, ISPs perform no data surveillance with respect to filtering out malware and ultimately deliver unfiltered content to their subscribers.

Another reason which has made the governance of ISPs difficult is the fact that ISP law and in general Internet law is still rapidly evolving and goes through radical changes every few years. This means that ISPs have not had a standard set of statutes governing them for an extended period of time, which informs them about their responsibilities and lays out conditions under which ISPs can and cannot be held liable. As elaborated earlier, the repetitive change in categorization (telecommunication service vs. information service) of the Internet has left ISPs unsure of what

their concrete status is - whether they are a Title I provider or a Title II provider, whether the Federal Communications Commission governs them or the Federal Trade Commission. Even Section 230 of the Communications Decency Act, which is also known as the "Twenty-Six Words that Created the Internet" comes under staunch criticism as of today and is constantly evolving as lawsuits pass by. On the contrary, most utility service providers have remained under the purview of the same set of laws for a long period of time and have achieved an equilibrium between the law and their own accountability. Hence, it might be a bit fairer if ISPs are expected to be held at the same standards as other utility providers when they also get to have a constant set of legislations governing them for a substantial period of time.

Moreover, the domain of cybersecurity is relatively new itself and is undergoing a similarly evolving set of legislations and creation of governing bodies. It was less than twenty-five years ago that the Internet became a commodity known to common households. Soon after, with the advent of the first of many computer viruses and malicious attacks, the domain of cybersecurity came into being. Since then, the US government has been working on legislations that apply to cybersecurity in general. It was as recent as 2017 that the National Security Council was created. Through this authority, President Trump created the National Security Presidential Memorandum (NSPM-4). This is the Memorandum that directs the system for conducting the National Security Process. Until this memorandum, the decision-making committees and the distribution of power varied compared to previous administration. The Office of Cybersecurity and Communications which was previously known as the Office of Cybersecurity and Telecommunications was created by the Congress in 2006. It is housed within DHS's National Protection and Programs Directorate (NPPD) and is responsible for enhancing the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

ISPs can also not be held to the same standards as other utility service providers due to the complex technical aspects of filtering malware from live flowing Internet traffic. Besides the immense compute power that is going to be required, it will be an uphill task for ISPs to identify malicious content flowing through their network in a day and age when encryption protocols such as HTTPS and SSL have become a norm. In 2018, the software company Mozilla came up with the concept of DNS over HTTPS (DoH), wherein a subscriber's DNS queries, instead of being in plain text, are encrypted using HTTPS protocol. In an article called *ISPs call Mozilla 'Internet*

Villain' for promoting DNS privacy, ISPs in the United Kingdom heavily criticized Mozilla's innovation because it makes it nearly impossible for them to keep up with their obligation to the UK government of maintaining one year's worth of subscribers' browsing data, in case the government needs it as evidence later on. "The point of DoH (and the related DNS over TLS, or DoT) is to encrypt DNS requests, which makes it impossible, or at least very difficult, for entities such as ISPs or governments to monitor which websites people are visiting. And because the DNS requests are sent inside encrypted HTTPS requests, they're also indistinguishable from other web traffic, so they can't be blocked without blocking all web traffic." (ISPs call Mozilla 'Internet Villain' for promoting DNS privacy, 2019) This situation can also apply to the United States in terms of the technical difficulties that ISPs might face when attempting to filter malware from the Internet traffic.

Approach to changing the current situation and how ISPs could be held accountable and the ethical reasonings and cost of this implementation

Throughout this analysis, it has become apparent that ISPs are not held to the same standard as other utility providers and do not have a driving force to provide filtered content to their subscribers. To change this status quo, and ensure that ISPs are held more accountable for not providing a clean Internet free of harmful viruses, malware, hackers and other bad actors, a new federal statutory tort law is proposed, which places an indirect, joint and several liability on ISPs as a countrywide group. Under this law, ISPs shall -

- Take preemptive measures that actively detect and block malware of all kinds including but not limited to viruses, worms, spyware, trojans, ransomware, and adware
- Take reactive measures to immediately block malware of all kinds once such a threat has been reported by a subscriber or another relevant party
- Adopt strict identity verification measures when enrolling a new subscriber for the purpose of enhanced traceability if required
- Immediately inform their subscribers and neighboring ISPs of a circulating malware threat, once identified
- Conduct periodic cursory screenings on electronic content being generated by subscribers for the sole purpose of identifying malware

"A statute is a law passed by a legislature; and statutory law is the body of law resulting from statutes. A statute—or the statutory law—may also be referred to as legislation." (Statutory vs. Common Law) A tort is an act that is opposite of proper policy. It is considered a wrongful act and the compensation usually involves the victim receiving money in damages. For example, if a server serves extremely hot coffee to their customer without warning and the customer injures themselves, the victim can then receive money as compensation for this negligent act. Similarly, ISPs too need to be held financially responsible if their subscribers receive unfiltered Internet content which happens to contain malware that eventually leads to personal and financial harm to the subscribers. Using the proposed statute, the liability for ISPs shall be indirect meaning if the original perpetrator of the crime cannot be found or is "judgment-proof", ISPs would be responsible for the financial fees and compensation. A liable party is said to be judgment-proof when they are unable to pay the adjudged liability amount. Finally, ISPs shall be held jointly and severally liable, implying that each of the involved ISPs is independently liable for the entire compensation amount ordered under this tort law. For example, if malicious Internet traffic travels through the proprietary networks of ISPs A, B and C, and finally infects the computers of XYZ corporation's local office, and a liability judgment of $10,000 is ordered under the proposed legislation, then XYZ corporation is allowed to demand the full compensation amount of $10,000 from ISP C, and ISP C shall be liable to pay the entire compensation amount. ISP C can later demand contributions from ISPs A and B. Similar federal law addressing ISPs can be found on other domains. Laws such as SESTA/FOSTA and OCILLA hold ISPs responsible for blocking Internet domains linked to these laws. In an article called *SESTA/FOSTA imposes accountability on internet service providers, remains misinterpreted by many,* it is mentioned that ISPs do not have immunity if they do not take proper measures to take down sex trafficking websites. Similarly, for OCILLA, under Title II, ISPs are responsible for ensuring any piracy websites or content is not promoted.

The aim of this proposal is that ISPs start taking controlling measures to stop malicious acts and malware before any damage is done to the subscribers. ISPs may choose to create a mechanism using which subscribers can report malware that violated their systems while using the Internet. This would also help in keeping track of patterns of malicious traffic and its origins. And in cases where a circulating malware threat is identified by an ISP, they must educate their subscribers on the necessary steps towards avoidance as well as resolution. On the other hand, the

reasoning behind a stricter identity verification protocol that may include a background check of subscribers at enrollment is so that it is easier to trace the perpetrator when a cybercrime is committed. It is also proposed that ISPs are liable for any malware that is propagated, intentionally or unintentionally, by a subscriber. This would keep ISPs in the chain of responsibility and make them responsible for the subscribers' actions. ISPs will also be legally bound to disclose identifying information about the perpetrator if he or she happens to be one of their subscribers. The proposed periodic cursory screening of subscribers is solely meant for the purpose of identifying any suspicious traffic patterns which may lead to a potential security threat. ISPs can do this by conducting screenings of their subscribers' DNS queries. It needs to be noted that such screenings shall only be as invasive as absolutely necessary and shall in no manner violate any existing privacy laws related to electronic communication media. It is for the same reason that there will need to be an amendment in the Electronics Communication Privacy Act (ECPA) enlisting appropriate accommodations for ISPs so that they are able to implement the proposed legislation.

Looking at this proposal from an ISP's point of view can be daunting. A federal statute like this comes with several financial factors to consider for any such ISP. The infrastructure cost to build such a system coupled with the indirect liability clause carries the potential to severely harm an ISP corporation and may even drive a smaller "mom-n'-pop" ISP operation to bankruptcy. Moreover, ISPs might run into legal turmoil with privacy laws as well. To counter and avoid such drastic financial crises for ISPs due to potential lawsuits, it is proposed that a government-backed liability insurance program is introduced for ISPs. Insurance companies can target a liability insurance scheme specifically towards ISPs and offer competitive pricing. This will help ISPs feel more motivated towards adhering to the proposed legislation because it will give them a financial cushion if they were to run into legal issues such as ECPA violation or tort liability judgments. Overall, it will result in a cleaner and safer Internet.

It is also proposed that a tax cut benefit be granted to ISPs based on the number of subscribers an ISP has. This proposal can be added to the Permanent Internet Tax Freedom Act which is a legislation aimed at permanently banning state and local taxing of Internet access. "A tax cut is justified when the marginal dollars raised are of more worth to society when held in private hands than when flowing through the government." (When is a Tax Cut Justified?, 1999)

In an article called *How bad are cyberattacks for the economy? This professor helped the White House assess the damage,* a senior economist revealed that the United States spent between $57 billion and $109 billion towards tackling malicious cyber activity in 2016. This figure is about 0.58 per cent of the country's gross domestic product. With large corporations, government agencies, banks and other financial firms, the stock market, department stores, healthcare institutes and nowadays even automobiles and medical monitors running on the Internet, a sophisticated cyber-attack, be it a virus or a self-replicating worm, can bring down all major infrastructure of the country, which might take days to recover from. The financial impact this can have on the economy is unimaginable. Given this knowledge, it makes sense to deploy a tax cut benefit directed towards ISPs, so that they can invest in building a robust and infallible infrastructure which is specifically designed to preemptively detect and stop such security threats and mitigate its ill impact. A resultant tax deficit for the government today can lead to the avoidance of billions of dollars of losses and expenditure in the future by not having to deal with an uncontrolled number of cyber threats. Moreover, a tax cut like this would help keeping smaller ISP operations afloat in the middle of their efforts trying to comply with the proposed legislation. Tax incentives like these have already been offered to e-commerce companies like Amazon by the government. In such cases, the tax cut encourages company growth by allowing the company to reinvest its profits into expanding operations which in turn creates more employment opportunities.

Ever since 2017, when the Internet was reclassified as an information service under Title I of the Communications Act of 1934, ISPs are no longer regulated by the FCC and are instead regulated by the Federal Trade Commission (FTC). Because of this ISPs are legally allowed to have access to subscribers' personal information including name, address, IP address, other information such as subscribers' geographic location, health data, financial information, Internet browsing history and so on. There also are ongoing investigations about ISPs selling subscriber data to the industry, monitoring subscriber Internet searches to direct them to specific results, inserting advertisements based on what a subscriber is browsing, and injecting undetectable cookies that track data on the web. Companies such as AT&T, Sprint, and T-Mobile can use software to track every URL that their subscriber visits. Given the kind of surveillance on subscriber data already being carried out by ISPs for monetary benefits, it is hard to argue that a legislative approach towards preventing malware attacks by intercepting subscriber traffic is ethically out of bounds. Moreover, a sense of justice needs to prevail. For years now, if a subscriber

happens to download malware into their computer, the consequential financial damage is something the subscriber has to deal with. There is no sense of liability and justice, even though ISPs are multi-million dollar corporations with a bird's eye view of large subsets of the network which is known as the Internet, and if anyone could present a detailed picture of Internet traffic patterns including ongoing malicious activities, it would be the ISPs. Besides, finding the actual minds behind a malicious cyber act among three billion Internet users is extremely difficult and even if they do get caught, they are often unable to pay the financial damage and are considered "judgment-proof." Needless to say, a legislative approach which makes ISPs responsible for provision of a clean Internet free from all malware is also desirable from the point of view of the common masses. As far as the privacy concerns with such an approach are concerned, as already stated, the new statute that has been proposed will be in accordance with the amended ECPA, and thus will aim to meet the standards set by the preexisting privacy act. Considering all these factors, a legislative approach, despite the slightly intrusive first impressions, is the best way to ensure accountability of ISPs for a clean Internet, speaking from an ethics point of view as well.

As briefly touched upon earlier, the implementation of the proposed legislation will come at a heavy cost to the ISPs. ISPs will need a very elaborate infrastructure to be able to accomplish something like intercepting petabytes of Internet traffic, scanning for, identifying, and filtering malicious data and re-inserting traffic back into their network, all in a matter of milliseconds. A Goliath effort like this will need an overwhelming amount of compute and storage power as well as large investments in research and development so as to come up with sophisticated and effective real-time filtering techniques. It would require acquiring a large amount of high performing servers, very high electricity costs for operating as well as cooling all equipment, and also persistent maintenance costs.

Amortized Cost	Component	Sub-Components
~45%	Servers	CPU, memory, storage systems
~25%	Infrastructure	Power distribution and cooling
~15%	Power draw	Electrical utility costs
~15%	Network	Links, transit, equipment

Greenburg, A., Hamilton, J., Maltz, D. and Patel, P., 2020. The Cost of a Cloud: Research Problems in Data Center Networks. [online] Microsoft.com. Available at: <https://www.microsoft.com/en-us/research/wp-content/uploads/2009/01/p68-v39n1o-greenberg.pdf>.

As per a research conducted by Microsoft in 2009, *The Cost of a Cloud: Research Problems in Data Center Networks*, the amortized cost of 50,000 servers alone is about 52.5 million dollars per year, infrastructure cost for such a facility is about 18.4 million dollars per year, and the power draw and network costs are roughly 9.3 million dollars each per year. Even if larger ISPs already have functional data centers that can be expanded and enhanced to cater to the additional requirement of filtering traffic in real time, the costs are still going to be in the order of millions of dollars per year. Another cost that needs to be considered is the liability insurance that ISPs are going to need. As per the article, *How Much Will Insurance Cost For My Small Business*, the per year liability insurance premium for a relatively smaller ISP can be anywhere between 500 to 1,000 dollars per year. It is best left to imagination how high this expenditure would be for a much larger ISP corporation spanning different states. ISPs will have to incorporate these costs into their financial plans and budgets. Ultimately, the subscribers and the government are going to have to bear the brunt for most part of these extra costs in the form of their monthly bills and tax deficits respectively, as a price that they pay today for a far better and cleaner Internet in the future.

Finally, given the bifurcated opinion of the Internet community over the classification of the Internet as a telecommunication service under Title II of the Information Act, or an information service under Title I of the Act, the corresponding violation of, or adherence to net neutrality principles respectively, and given the user data privacy and excessive surveillance concerns over filtering of the Internet, a very orthogonal and moderate solution is also proposed. ISPs can be encouraged to offer an option to their subscribers to select a premium service package with malware protection included. ISPs can charge higher rates for this service package and also absolve themselves of any privacy violation liabilities as part of the terms and conditions of such a premium package. On the other hand, if ISPs are unable to track and filter out malware from the Internet traffic reaching the computers of premium subscribers, they shall be held accountable for it via the usual violation of terms and conditions methods such as Federal Trade Commission's Consumer Protection resources. This way ISPs will be subject to greater accountability when it comes to

providing a clean Internet, and at the same time, subscribers having concerns about excessive surveillance and intrusion to their data privacy can prefer to opt out of this option. From a cost perspective, the implicit assumption behind this solution is that ISPs shall be able to get enough subscribers to sign up for this premium service such that they are able to break even the cost of purchase of the infrastructure required for filtering out malware and similar malicious content.

Conclusion

It has become apparent throughout this analysis that ISPs are not held accountable for not providing their subscribers a clean Internet free of malicious content. The current state of affairs makes it difficult for ISPs to monitor traffic without violating existing privacy laws and being subjected to investigations. As a result, ISPs tend to err on the side of caution in such circumstances and do not get involved in the process of filtering malware from the Internet. Moreover, it is financially difficult for ISPs to be able to afford such a rigorous infrastructure. Nevertheless, given that ISPs are the most significant resource in monitoring malicious content circulating in the Internet and have the best view of it, they are in the right position to protect their subscribers from malicious content. The world of the Internet can be protected if precautions are taken at the front door of defense - the ISPs. It is said that a hacker tries to attack a system every 39 seconds. With the Internet being used by not just subscribers at home, but also by industries such as the stock market, government agencies and offices protecting national security, banks, and energy/utility centers, it becomes even more imperative for ISPs to have a strong preventive mechanism. That is why, a couple of solutions are proposed, such as new legislation including provision of liability insurance and a tax benefit for ISPs. As detailed earlier, such legislations governing ISPs already exists in other Internet related domains such as online copyright infringement and websites promoting sex trafficking. A relatively moderate premium service-based approach has also been proposed towards achievement of the same goal. Hopefully, the need of the hour will be recognized, and similar steps will be adopted by the government and ISPs for the development of a better, cleaner, and safer Internet for the future.

Work Cited

Ammori, Marvin. "Net Neutrality's Legal Binary: An Either/Or With No 'Third Way.'" *Center for Internet and Society*, 2014, cyberlaw.stanford.edu/blog/2014/05/net-neutrality%E2%80%99s-legal-binary-eitheror-no-%E2%80%9Cthird-way%E2%80%9D.

Asp, Emily M. "Section 512 of the Digital Millennium Copyright Act: User Experience and User Frustration." *Iowa Law Review*, 2018, ilr.law.uiowa.edu/print/volume-103-issue-2/section-512-of-the-digital-millennium-copyright-act-user-experience-and-user-frustration/.

Bonner, Marianne. "How Much Does Business Insurance Cost?" *The Balance Small Business*, The Balance Small Business, 8 Jan. 2020, www.thebalancesmb.com/what-is-the-average-cost-of-small-business-insurance-4172224.

Brodkin, Jon. "Making the Internet a Utility-What's the Worst That Could Happen?" *Ars Technica*, 18 Dec. 2014, arstechnica.com/information-technology/2014/12/worst-case-scenario-why-the-cable-lobby-is-scared-of-becoming-a-utility/.

"Communications Act of 1934." Communications Act of 1934, 1934, transition.fcc.gov/Reports/1934new.pdf.

"Congress Reshapes Legal Requirements for International Access to Communications Information with the CLOUD Act." *Wilson Sonsini Goodrich & Rosati Professional Corporation Home Page - Palo Alto, Silicon Valley, San Francisco, New York, Seattle, San Diego, Washington, D.C., Shanghai, Hong Kong, Brussels - Congress Reshapes Legal Requirements for International Access to Communications Information with the CLOUD Act*, 2018, www.wsgr.com/en/insights/congress-reshapes-legal-requirements-for-international-access-to-communications-information-with-the-cloud-act.html.

Denning, Stephanie. "Why Amazon Pays No Corporate Taxes." *Forbes*, Forbes Magazine, 25 Feb. 2019, www.forbes.com/sites/stephaniedenning/2019/02/22/why-amazon-pays-no-corporate-taxes/#383037aa54d5.

Domonoske, Camila. "Facebook Says 14 Million Accounts Had Broad Array Of Personal Data Stolen." *NPR*, NPR, 13 Oct. 2018, www.npr.org/2018/10/13/657172112/facebook-says-14-million-accounts-had-broad-array-of-personal-data-stolen.

Dunn, John E, et al. "ISPs Call Mozilla 'Internet Villain' for Promoting DNS Privacy." *Naked Security*, 8 July 2019, nakedsecurity.sophos.com/2019/07/08/isps-call-mozilla-internet-villain-for-promoting-dns-privacy/.

"Electronic Communications Privacy Act of 1986." *Electronic Communications Privacy Act of 1986*, 1986, it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

"Electronic Surveillance." *Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/wex/electronic_surveillance.

Evgen, et al. “A Question of Titles: Title I, Title II, and the Future for Net Neutrality.” *Web We Want*, 11 July 2017, webwewant.org/news/question-titles-title-title-ii-future-net-neutrality/.

Frazin, Rachel. “Maine Governor Signs Net Neutrality Bill.” *TheHill*, The Hill, 26 June 2019, thehill.com/homenews/state-watch/450461-maine-governor-signs-net-neutrality-bill-into-law.

Fung, Brian. “These 26 Words 'Created the Internet.' The US Government Is Coming for Them.” *CNN*, Cable News Network, 25 Feb. 2020, www.cnn.com/2020/02/25/tech/section-230-doj/index.html.

Greenberg, Albert, et al. *The Cost of a Cloud: Research Problems in Data Center Networks*. 2009, www.microsoft.com/en-us/research/wp-content/uploads/2009/01/p68-v39n1o-greenberg.pdf.

“Information Technology Services.” *Wesleyan University*, www.wesleyan.edu/its/policies/dmca.html#.

“Internet Basics: What Is The Internet?”. Gcfglobal.Org, 2020, https://edu.gcfglobal.org/en/internetbasics/what-is-the-internet/1/.

“Introduction to Business [Deprecated].” *Lumen*, courses.lumenlearning.com/wmopen-introbusiness/chapter/reading-criminal-versus-civil-law/.

ISP Liability for Copyright Infringement, cyber.harvard.edu/property99/liability/main.html.

Maras, Marie-Helen. Computer Forensics: Cybercriminals, Laws, and Evidence. Jones & Bartlett Learning, 2015.

“Malware: Viruses, Spyware, Adware & Other Malicious Software | Umass Amherst Information Technology | Umass Amherst”. Umass.Edu, 2020, https://www.umass.edu/it/security/malware-viruses-spyware-adware-other-malicious-software.

Morran, Chris. “House Votes To Allow Internet Service Providers To Sell, Share Your Personal Information.” *Consumer Reports*, 2017, www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/.

Mullins, Paul. "Networks: Connecting". Cs.Sru.Edu, 2014, http://cs.sru.edu/~mullins/cpsc100book/module08_networks/module08-05_networks.html.

Newton, Casey. “A Sneaky Attempt to End Encryption Is Worming Its Way through Congress.” *The Verge*, The Verge, 12 Mar. 2020, www.theverge.com/interface/2020/3/12/21174815/earn-it-act-encryption-killer-lindsay-graham-match-group.

Ohm, Paul. *The Rise And Fall Of Invasive ISP Surveillance*. 2009, illinoislawreview.org/wp-content/ilr-content/articles/2009/5/Ohm.pdf.

"Protecting and Promoting the Open Internet." *Federal Register*, 13 Apr. 2015, www.federalregister.gov/documents/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet.

Rhodes, Shea M., et al. "SESTA/FOSTA Imposes Accountability on Internet Service Providers, Remains Misinterpreted by Many." *TheHill*, 22 May 2018, thehill.com/blogs/congress-blog/judicial/388694-sesta-fosta-imposes-accountability-on-internet-service-providers.

Rpc.Senate.Gov, 2018, https://www.rpc.senate.gov/policy-papers/why-title-ii-is-not-the-answer-for-internet-freedom.

Schewick, Barbara. "Gov. Jerry Brown Signs SB 822, Restoring Net Neutrality to California." *Center for Internet and Society*, 30 Sept. 2018, cyberlaw.stanford.edu/blog/2018/09/gov-jerry-brown-signs-sb-822-restoring-net-neutrality-california.

Shachtman, Noah. *Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs*. 2011, www.brookings.edu/wp-content/uploads/2016/06/0725_cybersecurity_shachtman.pdf.

Steuerle, Eugene. *When Is a Tax Cut Justified?* 1999, www.urban.org/sites/default/files/publication/70956/1000173-When-is-a-Tax-Cut-Justified-.pdf.

Volz, Dustin. "Trump Signs Bill Renewing NSA's Internet Surveillance Program." *Reuters*, Thomson Reuters, 20 Jan. 2018, www.reuters.com/article/us-usa-trump-cyber-surveillance/trump-signs-bill-renewing-nsas-internet-surveillance-program-idUSKBN1F82MK.

"What Is An Internet Service Provider?". Whatismyipaddress.Com, 2020, https://whatismyipaddress.com/isp.