IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 22, Issue 10, Ver. IV. (October. 2017) PP 39-45
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

VPNs and Pedophilia: An Issue or a Solution?

Marcia R Pinheiro
drmarciapinheiro@gmail.com

Abstract: In this paper, we worry about investigating the use of Virtual Private Networks for the commission of crimes involving pedophilia. Recent political decisions in China seem to point at the world leaders connecting it to organized crime. The overall impression of professionals from Information Technology is that Virtual Private Networks are excellent tools for any sort of establishment or individual that depend on non-physical communications. The Australian government seems to have no concerns whatsoever with pedophilia and the use of VPNs. We here want to determine the effects on non-criminalization of the use of VPNs in what comes to pedophilia. On the way to that, we provide a good introduction to the topic and a good collection of intelligence tokens.

Keywords: VPN, safety, cyber, crime, Internet

Date of Submission: 28-09-2017 Date of acceptance: 10-10-2017

I. INTRODUCTION

From physical social networks[1] to Peer-to-Peer and Virtual Private Networks, nothing is more in fashion than what in the past would be called gang formation and be associated through the law with crime. We focus on virtual networks. They hold strong connection with IP numbers:

> *Every single time a device; smartphone, computer, tablet and even a smart refrigerator connects to the internet, an IP address is assigned to it*[2].

The ISP (Internet Service Provider)[2] does that.

Well, an IP address is a unique number that is assigned to a device connected to the Internet or network. This number can be used to identify a particular device to the point of determining its physical location.

> *You can think of it like a fingerprint: No two devices have the same IP Address.*
> *When you access the internet, your IP address is broadcast for all to see it.*
> *Every website you visit, and every network you use will know your IP address and they can use it for a number of different purposes, some completely fine, and others you should be very worries about*[2].

IP (Internet Protocol[3]) addresses are the equivalent to the Brazilian ID card number[4] or the Australian Driver's License number[5] on the Internet. In real life, if someone knows your licence or ID number, that is not enough for them to impersonate you. Notwithstanding, in the Virtual World, your IP number is enough for those purposes. Furthermore, people can target you (cybercrime[6]),and that can make your online activity materially, not only virtually, impossible: Some people cannot use their keyboards[7] or computers[8]after anattack. Because of that, exhibiting a virtual public identity number that points at another continent when we are online may mean self-protection; it does not have to mean crime.

> IP Spoofing[9]
> *IP spoofing*involves changing the packet headers of a message to indicate that it came from an IP address other than the true source. In essence, the sending computer impersonates another machine, fooling the recipient into accepting its messages. The spoofed address is normally a trusted port, which allows a hacker to get a message through a firewall or router that would otherwise be filtered out. When configured properly, modern firewalls protect against IP spoofing.

[1] Cruz-Cunha, p. 394

> Spoofing is used whenever it is beneficial for one machine to impersonate another. It is often used in combination with one of the other types of attacks. For example, a spoofed address is used to hide the true IP address of the attacker in Ping of Death, Teardrop, and other attacks. Remote Procedure Call (RPC) services, the X Window system, the UNIX **r** services (rlogin, rsh, and so on) and any service that uses IP address authentication are all susceptible to IP spoofing.

VPNs help us remain anonymous[2], and access sites that we cannot normally access[2], maybe sites that are relevant for our work (academics, research and/or others). They also provide a tunnel of protection against investigative authorities[2], so that some defend that they make crime and non-deterrence more possible[10].

> *online pedophile* will be used here to refer to this heterogeneous group of individuals whose interactions are focused essentially on child pornography in cyberspace and whose behaviour is punishable under certain sections of …, which prohibits the making, distribution and accessing of child pornography, and section …, which since 2002 prohibits the luring of children[11].
> …
> The three *A's* of the virtual world, *accessibility*, *affordability* and *anonymity*, facilitate more than ever before illegal exchanges of child pornography between users, whether for the purpose of distributing and making such pornography or of luring children for sexual purposes[11].

> Paedophileswillgravitatetowards technologiesthatmaximiseanonymity.Indeed,itcanbe expected that somepaedophileshavealreadychosentoconducttheirbusinesswithinvirtual private networks (VPNs).Monitoring VPNs will provedifficultbecausetransactionswillbe encryptedandInternettrailswill be elusive[12].

If VPNs maximise anonymity and possessing them compares to possessing no other popular item, perhaps we should forbid their existence or use, given the information we get from the extract above.

Russia andChina seem to be heading that way[13].

In Development, we present pros and cons of using VPNs, but also varied and technical aspects of the product. We discuss pedophilia when the phenomenon appears associated with virtual networks: We focus on the impact of legalising VPNs. We hope to present an analysis that allows for all types of readers to make the freest choices as possible. In Conclusion, we present an unbiased sum of arguments in order to give an overall idea of the impact of legalizing VPNs on the deterrence of groups that practice pedophilia.

II. DEVELOPMENT

Russia banned VPNs (2017) because people could access forbidden sites through them. See[13]:

> *VPNs use encryption to disguise the source of Internet traffic, allowing users to view websites that are banned in their home countries. Many popular VPN services cost around $10 a month.Russian Internet regulator Roskomnadzor maintains a blacklist of thousands of websites.*

VPNs letuserslie about their physical location: We can pretend to bein America, and access sites that are forbidden in Russia from Russia.

An Internet discussion[14]:

> Netflix are just sulking because people are using VPN's to connect to Netflix when not in the US. VPN's, like all tech, are not inherently good or bad. It's all in how people use them.
> …
> VPNs are not bad, they're simply a tool. You don't yell at hammer manufacturers because they can be used for nefarious purposes, so why do the same with VPNs?
> If HBO and Netflix have issues with people using VPNs to access their content, then maybe they shouldn't limit content based on geographical region. Just like any DRM, people will find a way around it pretty easily.
> …
> I use VPNs extensively both for professional as well as personal purposes. Not to pirate content, mainly because I really don't have time or interest, but to connect to secure services and in some

> cases because I still do security research on the side. I'm reasonably sure my ISP's privacy practices are a bad joke. Last thing I need is to wind up on a secret watch list while hunting down who's trying to rip one of my clients off.
> …
> Hack the planet. Information does not want to be free, people do. People use tools. Tools like VPN. People use tools like VPN to become free, and the wild fire of information continues.

In the extracts above, we see some hacktivism[15](last paragraph), some arguments to the side of the providers whose contents are being inappropriately used (without paying), and some arguments to the side of those who are deprived from those contents, including one that sounds like hacktivism[16].

> *The list of Australian government departments that theoretically can access metadata collected by the ISPs and telecommunication companies is extensive and wide ranging. This means that a larger part of Australians' lives become accessible to these agencies, and the information collected could potentially be used against them.*
> *The most effective way of protecting privacy of communications on the Internet is to use a virtual private network (VPN), which will quite simply prevent all details of communications (and yes, also browsing history) from being visible to an ISP[17].*

VPNs are then about protection of rights. The necessity would come from the fact that the government is requesting ISPs to provide personal users' data[18,19,20].

More, same source[17]:

> *VPNs are becoming an essential part of being on the Internet. Apart from the privacy aspect, there is the added security they provide, especially when using unknown wireless networks such as in cafes, airports, or even at work. They also provide the ability to avoid geolocked content on services like Netflix, which up until the advent of metadata retention was the main reason for most people using a VPN, especially in Australia.*
> *Given the commitments to privacy and security made by companies like Apple and Google, it would not be at all surprising if they started to provide their own VPN services to customers that were seamlessly built into their devices.*

Culture makes an enormous difference: Inspiration, ideas, and solutions[21]. If Australians do not watch The Matrix[22] in time, a major catastrophe may occur: Imagine a comet is about to strike earth. Australian people's cultural experience is very different from the American people's: They could see Keanu moving and realise, just like Newton and his apple[23], that we could be using laser in triangulation to avoid obstacles, saysatellites. Americans could never see that, and therefore the catastrophe would be avoided only if Australians watched The Matrix in time.

To the side of crime, there is more likelihood that the person commit a crime, such as accessing pedophilia websites, if they trust they will remain anonymous. The Australian government, however, does not seem to have any problems with VPNs and the activity[24]. Besides, we now have tools to investigate things: Honeypots[25]and others.

Several other resources make anonymous surfing something material. For instance[26]:Tor (browser and network), and Incognito mode (Google Chrome, Internet Explorer, Mozilla Firefox, and Safari).Opera has a free VPN built-in[27] and that is why anonymous surfing is guaranteed.One can also use proxies[27].

Consequently, if we forbid VPNs because they allow for anonymous surfing, we must also forbid incognito mode, proxies, Tor, and others.

Since perpetrators may also rely on anonymous communication tools and keep browsing activities as non-super secretive, we also have to stop Mailvelope, SecureGmail, and alike[27].

We canblock all that, but the easiest way to target someone online is the IP address[28,29,30]. People prefer preventing to suffering crime,having to identify perpetrators,and try their luck with the authorities[31]. The number of perpetrators must be smaller than the number of victims in democratic countries[32,33,34], since the voice

of the people is the voice of God (figurative[35])in those, and therefore the laws are an agreement,not an imposition.

It is much more likely that a non-marginal need to disguise their IP to pass anote to someone overseas than a marginal need to disguise their IP to attack: There is way more retaliation for attempting to exercise human rightsthan for attempting to commit crime through a computer. Just consider the number of people who are officially told to be in slavery: 45.8 million[36]. This figure must outnumber by much the total of the people complaining about IT crimes. One of these slaves might find out thatthose who enslaved them will soon attackAmerica. A computer might be available to them. If someone finds out that they told the Americans, they get killed. If they never find out, America might be prepared for the strike, and even save them out of gratitude. Nobody will ever know they were the informant.

Kids could try to ask other countries to help them if we talk about pedophilia. The IP disguiser could protect them: Perhaps the Afghanistan police officers[37] will intercept the message and kill them otherwise.

There is still encryption:

> *For example, if an offender uses encryption software with a 20-bit encryption, the size of the keyspace is around one million. Using a current computer processing onemillion operations per second, the encryption could be broken in less than one second. However,ifoffenders use a 40-bit encryption, it could take up to two weeks to break the encryption. In 2002, theWall Street Journal was for example able to successfully decrypt files found on an Al Qaedacomputerthatwere encrypted with 40-bit encryption. Using a 56-bit encryption, a single computer would take up to2 285 years to break the encryption. If offenders use a 128-bit encryption, a billion computer systemsoperating solely on the encryption could take thousands of billions years to break it. The latestversionof the popular encryption software PGP permits 1 024-bit encryption[38].*

In a VPN environment, the end that sends communication encrypts and the end that receives decrypts, so that they create a tunnel to communicate and that is when enforcement could have to do much more than the usual.

> *Tools are also available to encrypt communications – for example, e-mails and phone calls – that can be sent using VoIP. Using encrypted VoIP technology, offenders can protect voice conversations from interception[38].*

In this case, if enforcement wanted to finish with VPNs because of the work decryptiongives, they would have to also finish with encrypted VoIP technology.

> *Techniques can also be combined. Using software tools, offenders can encrypt messages and exchangethem in pictures or images – this technology is called steganography. For investigative authorities,itisdifficult to distinguish the harmless exchange of holiday pictures and the exchange ofpictureswithencrypted hidden messages[38].*

As a conclusion, upon deciding to finish with VPNs because of the encryption systems, enforcement would also have to finish with the software that is currently used for encryption.

> *The availability and use of encryption technologies by criminals is a challenge for law-enforcementagencies. Various legal approaches to address the problem are currently under discussion,including:potential obligations for software developers to install a back-door for law-enforcement agencies;limitations on key strength; and obligations to disclose keys, in the case of criminal investigations. Butencryption technology is not only used by offenders – there are various ways such technology isusedforlegal purposes. Without adequate access to encryption technology, it may be difficult to protect sensitiveinformation. Given the growing number of attacks, self-protection is an important elementofcybersecurity[38].*

Consequently, there might be important applications of encryption technology. Enforcement seems to havealternatives to finishing with the VPNs. For those who like independence of the authorities, the back-door entry point is certainly the most attractive option. Limitations on key strength does not seem to be a reasonable suggestion because they probably go as far as needed most of the time (in Australia, authorities disciplineus:

Only proportional force to the force applied against us[39]). Obligation to disclose keys upon request (investigations) is a good option for those who like dependent authorities: Perhaps in this way we have more control over them. Human lives may depend on that information being disclosed: Having to request things and counting on the collaboration of others may mean death or lifetime injury[40]. The most democratic would probably think that as long as the public can get information from the authority in an expedite manner, information that may save the lives and/or bodies of those that they care about,then it is OK[41]. Marcia R Pinheiro[42] requested that authorities disclosed the ownership of the vehicle NOI916, a vehicle whose driver and passenger stalked and harassed her throughout the length of Charnwood Road in the end of 2001. She was denied the information by every Australian authority for law and order each, and every, time (Equity VUT, 2001; VICPOL through subpoena, 2004; NSW police, 2005; and so on). Yet, the authorities clearly had the information requested plus extra. By the principles of democracy (privacy, freedom, equal opportunity, etc.),they should be obliged to disclose that in an immediate manner (pictures were presented alongside with reports that included Equity VUT branch employees holding all needed information). For not having the information, many years and personal resources were lost: Crime committed by the same agents. We must always see both sides: That the authorities access what they need in a timely manner, and that we access what we need in a timely manner. Citizens can only trust a relationship, and, in this case, we talk about the relationship between The State and the citizen in democracy, if things work both ways[42]. If they don't, it seems that the tendency is self-protection, and therefore supporting obstruction of investigation and protection against invasion of privacy to maximum. Let's call this resistance to authority. Citizens are probably prepared to be as clean as the authority, but never cleaner than them.

III. CONCLUSION

Virtual Private Networks (VPNs) increase the likelihood of pedophilic crimes because they provide anonymity, but they also increase the chances of getting saved for those who are in slavery, and the number of people who would want to practice pedophilic crimes is very low when compared to those who are in slavery (about 46 million).

At least two very well-known countries have forbidden the use of VPNs: Russia and China. The reasons for them to do so are censored websites, terrorism, and circulation of unwanted information.

If we finish with VPNs, so say we pass a law in Australia forbidding them, but our government seems to be well informed and not think that VPNs are a problem, we will have to finish with several other things if the reason is anonymous surfing: Incognito option in browsers, Tor (network and browser), Mailvelope, SecureGmail, and the alike.

If a person targets us, and getting our IP is easy for them, they can attack us in several ways, even physically, so that VPNs help protect the figure of the good citizen, not only the marginal, and there are way more possible victims of cybercrime than people willing to commit that sort of crime, so that the number of possible benefits of having itis again larger than the number of possible losses.

People might use VPNs to pretend to be overseas, so that they may pay lower fees for a certainpiece of software or even have access when their Country forbids it. Some organizations, such as Netflix, seem to be upset with that sort of thing; perhaps very upset. Companies complaining about this are usually private, and the governments have not yet showed any major concern with that, so that this issue is minor.

The information contained in a movie can change the destiny of human kind: An Australian watching The Matrix might have an idea thatAmericans doing the same thing will never have because of cultural differences. That idea might actually save human kind from a major disgrace. Australians may never watch The Matrix in time if they don't have VPNs.

Enforcement seems to go through a lot of struggle to break the walls between the message and them when there is encryption: All seems to depend on the size of the key and it can take them from two weeks to about two thousand and three hundred years to get to the contents. That is certainly not reasonable. This token of information makes us seriously think of forbidding VPNs. Notwithstanding, the International Technological University, which seems to be the origin of our data on this matter, has alternatives: One of them is obliging software developers to install a back-door for enforcement. Another is limitations on key strength. Yet another is obliging them to disclose keys in the case of criminal investigations. If enforcement has to put in requests with third-parties, people may die or suffer lifetime injury during the waiting time and because of it. Limitations on key strength does not seem to be a wise move because society probably acts under the principle of proportional reaction. Leaving a back-door open for enforcement looks like the most interesting approach, but one must bear in mind that this is a good idea only when the authority responds to the needs of the individuals who are honest in an expedite manner: The population should not be happy with this choice otherwise.

REFERENCES

[1] [1]Cruz-Cunha, M. M. (2011).*Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions: Organizational, Managerial, and Technological Dimensions*. IGI Global. Retrieved from https://books.google.com.au/books?id=dOmeBQAAQBAJ&dq=physical+social+network&source=gbs_navlinks_s

[2] [2]Strouvali, S. (2015). How to Change Your IP to any Other Country You Want. Retrieved September 4, 2017, from https://securitygladiators.com/change-ip-to-other-country/

[3] [3]Russ Smith of Consumer.Net. (1997). IP Address: Your Internet Identity. Retrieved September 7, 2017, from https://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm

[4] [4]Biblioteca Virtual do Governo do Estado de Sao Paulo. (2017). Carteira de Identidade (RG). Retrieved September 7, 2017, from http://www.bibliotecavirtual.sp.gov.br/temas/documentos-pessoais/rg.php

[5] [5]Roads and Maritime Services. (2017). Proving Your Identity. Retrieved September 7, 2017, from http://www.rms.nsw.gov.au/roads/licence/identity/index.html

[6] [6]Syngress. (2002).*Scene of the Cybercrime: Computer Forensics Handbook*. Syngress. Retrieved from https://books.google.com.au/books?id=BLjomivi1asC&dq=another+ip+was+used+cyber+crime&source=gbs_navlinks_s

[7] [7]Kryllic. (2016).ScpToolkit Disabled Mouse and Keyboard #451. Retrieved September 7, 2017, from https://github.com/nefarius/ScpToolkit/issues/451

[8] [8]John Seabrook. (2013). Network Insecurity Are we losing the battle against cyber crime? Retrieved September 7, 2017, from https://www.newyorker.com/magazine/2013/05/20/network-insecurity

[9] [9]Syngress. (2002).*Scene of the Cybercrime: Computer Forensics Handbook*. Syngress.Page 298. Retrieved from https://books.google.com.au/books?id=BLjomivi1asC&dq=another+ip+was+used+cyber+crime&source=gbs_navlinks_s

[10] [10]Shu, C. (2017). Putin Passes Law that Will Ban VPNs in Russia. Retrieved September 7, 2017, from https://techcrunch.com/2017/07/30/putin-passes-law-that-will-ban-vpns-in-russia/

[11] [11]Corriveau, P., & Greco, C. (2017).Online Pedophilia and Cyberspace. Retrieved September 13, 2017, from https://www.inspq.qc.ca/en/sexual-assault/fact-sheets/online-pedophilia-and-cyberspace

[12] [12]Forde, P., & Patterson, A. (1998).Paedophile Internet Activity. Retrieved September 13, 2017, from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi097.pdf

[13] [13]Charles Riley. (2017). Russia Bans VPNs to Stop Users from Looking at Censored Sites. Retrieved September 8, 2017, from http://money.cnn.com/2017/07/31/technology/russia-vpn-internet-putin/index.html

[14] [14]CookieG. (2015).VPN...Good or bad? Retrieved September 8, 2017, from https://community.spiceworks.com/topic/909025-vpn-good-or-bad

[15] [15]Oxford University Press.(2017). hacktivist. Retrieved September 8, 2017, from https://en.oxforddictionaries.com/definition/hacktivist

[16] [16]Dictionary.com, L. (2017).hacktivism. Retrieved September 8, 2017, from http://www.dictionary.com/browse/hacktivism

[17] [17]David Glance. (2017). VPNs Become even more Important as ISPs Start Collecting Your Online Metadata. Retrieved September 8, 2017, from http://www.news.com.au/technology/online/security/vpns-become-even-more-important-as-isps-start-collecting-your-online-metadata/news-story/3fd498fa3a192687ce264bd3a72d5cb6

[18] [18]Simpson, Campbell 2016 'Here's Every Australian Government Agency That Wants Your Data' *Gizmodo* Available at: https://www.gizmodo.com.au/2016/01/heres-every-government-agency-that-wants-your-metadata/ Accessed 8.10.2017

[19] [19]The Conversation Media Group Ltd 2010 'VPNs Become Even More Important as ISPs Start Collecting Customer Metadata' *The Conversation* Available at: https://theconversation.com/vpns-become-even-more-important-as-isps-start-collecting-customer-metadata-76246 Accessed 8.10.2017

[20] [20]Tucker, Harry 2017 'New Data Retention Laws Begin Today, This Is What You Need To Know' *news.com.au* Available at: http://www.news.com.au/technology/online/new-data-retention-laws-begin-today-this-is-what-you-need-to-know/news-story/28ea2dc1b01d15e53f474e21b6d68501 Accessed 8.10.2017

[21] [21]Pinheiro, M. R. (2016). Your Mother Tongue Is Helping Me. *IOSR Journal of Humanities and Social Science*, *21*(9), 29–35. Retrieved from https://www.researchgate.net/publication/307608823_Your_Mother_Tongue_Is_Helping_Me

[22] [22]IMDB. (2003). The Matrix Reloaded. Retrieved October 8, 2016, from http://www.imdb.com/title/tt0234215/

[23] [23]Connor, S. (2010). The Core of Truth behind Sir Isaac Newton's Apple. Retrieved September 13, 2017, from http://www.independent.co.uk/news/science/the-core-of-truth-behind-sir-isaac-newtons-apple-1870915.html
[24] [24]Child Protection Operations.(2016). Online Child Sex Exploitation. Retrieved September 8, 2017, from https://www.afp.gov.au/what-we-do/services/child-protection/online-child-sex-exploitation
[25] [25]Geek Stop. (2015). 14 Days Running a Secret Dark Web Pedophile Honeypot (and Why I now Think Tor Is the Devil). Retrieved September 8, 2017, from http://geekslop.com/2015/catching-pedophiles-running-secret-dark-web-tor-honeypot
[26] [26]Guardian News and Media Limited or Its Affiliated Companies. (2017). 21 Tips, Tricks and Shortcuts to Help You Stay Anonymous Online. Retrieved September 13, 2017, from https://www.theguardian.com/technology/2015/mar/06/tips-tricks-anonymous-privacy
[27] [27]Griffith, E. (2017).How to Stay Anonymous Online. Retrieved September 13, 2017, from http://au.pcmag.com/encryption-products/8903/feature/how-to-stay-anonymous-online
[28] [28]JavaHelios. (2010). What You Can Do with Someone's IP Address. Retrieved September 13, 2017, from https://www.youtube.com/watch?v=d_eXt1rGJ1I
[29] [29]Quora. (n.d.). What Can a Hacker do with an IP Address? How do Hackers Obtain such Confidential Information? Retrieved September 13, 2017, from https://www.quora.com/What-can-a-hacker-do-with-an-IP-address-How-do-hackers-obtain-such-confidential-information
[30] [30]Srinivasan. (2013). Hack a Computer Only with just a IP Address in Easy Steps. Retrieved September 13, 2017, from https://www.learn2crack.com/2013/06/hack-a-computer-only-with-just-a-ip-address-in-easy-steps.html
[31] [31]Roger A. Grimes.(2012). Why Internet Crime Goes Unpunished. Retrieved September 13, 2017, from https://www.csoonline.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html
[32] [32]Telegraph Media Group Limited. (2017). Cyber Crime: One in 10 People now Victim of Fraud or Online Offences, Figures Show. Retrieved September 13, 2017, from http://www.telegraph.co.uk/news/2016/07/21/one-in-people-now-victims-of-cyber-crime/
[33] [33]Bureau of Justice Statistics.(2017). Cybercrime. Retrieved September 13, 2017, from https://www.bjs.gov/index.cfm?ty=tp&tid=41
[34] [34]Krone, T., Smith, R. G., Cartwright, J., Hutchings, A., Tomison, A., & Napier, S. (2017). Online Child Sexual Exploitation Offenders: A Study of Australian Law Enforcement Data. Retrieved September 13, 2017, from http://crg.aic.gov.au/reports/1617/58-1213-FinalReport.pdf
[35] [35]Thurow, G. E. (1976).*Abraham Lincoln and American Political Religion*.SUNY Press. Retrieved from https://books.google.com.au/books?id=GvR2ZuFkhR0C&dq=voice+of+people+voice+of+god+democracy&source=gbs_navlinks_s
[36] [36]The Minderoo Foundation Pty Ltd. (2017). Global Findings. Retrieved September 13, 2017, from https://www.globalslaveryindex.org/findings/
[37] [37]Goldstern, J. (2015). U.S. Soldiers Told to Ignore Sexual Abuse of Boys by Afghan Allies. Retrieved September 13, 2017, from https://www.nytimes.com/2015/09/21/world/asia/us-soldiers-told-to-ignore-afghan-allies-abuse-of-boys.html?mcubz=3
[38] [38]Telecommunication Development Sector. (2014). Understanding Cybercrime: Phenomena, Challenge and Legal Response. Retrieved September 14, 2017, from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf
[39] [39]Commonwealth of Australia.(2016). Reasonableness, Proportionality and Merits Review. Retrieved September 14, 2017, from http://www.aat.gov.au/about-the-aat/engagement/speeches-and-papers/the-honourable-justice-garry-downes-am-former-pre/reasonableness-proportionality-and-merits-review
[40] [40]Perez, E., & Hume, T. (2016).Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone. Retrieved September 14, 2017, from http://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html
[41] [41]Ostrom, E., & Walker, J. (2003).*Trust and Reciprocity: Interdisciplinary Lessons for Experimental Research*. Russell Sage Foundation. Retrieved from https://books.google.com.au/books?id=cfkWAwAAQBAJ&dq=trust+police+reciprocity&source=gbs_navlinks_s
[42] [42]Pinheiro, M. R. (2017).Personal communications.
[43] [43]Tyson, J., & Crawford, S. (2017). How VPNs Work. Retrieved September 14, 2017, from http://computer.howstuffworks.com/vpn7.htm

Marcia R Pinheiro. "VPNs and Pedophilia: An Issue or a Solution?" IOSR Journal Of Humanities And Social Science (IOSR-JHSS) , vol. 22, no. 10, 2017, pp. 39–45.