DARKNET, ANONYMITY & LAW

PAVAN DUGGAL

DARKNET, ANONYMITY & LAW

BY

PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA

2015 Edition

PREFACE

My work on cyber legal regimes in the superficial web started encouraging me to think of new challenges that Internet is facing. It is in this regard that I found the Darknet to be the next big challenge for legal frameworks. Darknet is wild-wild-west, a cybercriminals' paradise, a place where cybercrimes are available as a way of life. The Darknet today allows large quantum of criminal and illegal activities to be done primarily because of the anonymity veil that the Darknet provides. This is intrinsically so because of the technology that The Onion Router (TOR) uses. The technology used is so powerful that it invariably hides the identity of the user behind various layers of anonymity so that the person virtually becomes faceless and unknown on the Darknet.

While scholars believe that the Darknet is a very disturbing place to visit, the fact also remains that more and more people are now going on to the Darknet. Whether it is because of increased interception, monitoring, decryption and blocking of individuals and their activities online or whether it is the Snowden revelations, the fact remains that more and more people are now concerned that their activities are being monitored by governments and political establishments and hence they are increasingly turning onto the Darknet for legitimate purposes of exercising their freedom of speech and expression and venting political dissent.

However, while the good news of the Darknet cannot be missed, the fact remains that the very fertile opportunity that technology has provided on the Darknet have been misused and abused by the cybercriminals on the Darknet for the purposes of engaging into repeated cybercriminal activities and modes of criminal conduct. It is in this regard, anonymity on the Darknet provides a distinct shot in the arms for all cyber criminals. Seen from the law-enforcement perspective, anonymity on the Darknet provides immense amount of challenges for the law-enforcement agencies. This is so because, law-enforcement agencies invariably, at the time of writing, do not have adequate tools or wherewithal to go ahead and pierce the anonymity veil on the Darknet as also to seize, produce and also prove in accordance with the legal frameworks before courts of law, the relevant incriminating electronic evidence which can actually provide the basis for cybercrime convictions on the Darknet.

In this context, anonymity on the Darknet is an immensely powerful paradigm which brings forward extremely complicated legal and policy challenges. What are these challenges? How can these challenges of anonymity on the Darknet be addressed by legal frameworks? What kind of legal principles need to be kept in mind by jurisprudence on the Darknet as it proceeds forward in the direction of addressing the legal frameworks pertaining to anonymity? These and variety of other questions are sought to be discussed and elaborated in the present eBook. At the time of writing, there is very little work being done on the legal jurisprudence on the Darknet. I distinctly believe that Darknet is a network of the future. Hence legal frameworks have to quickly tighten their belts and concentrate on coming up with appropriate robust and elastic legislative frameworks, principles and parameters which can help fight the misuse of anonymity on the Darknet for criminal or illegal purposes.

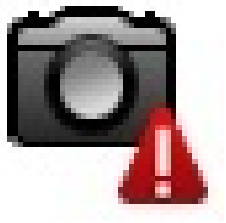
I have written this eBook in a layman's language identifying and explaining the legal and policy challenges that anonymity on the Darknet is currently posing before cyber legal frameworks across the world.

This is an intrinsically important area of Cyberlaw jurisprudence which will be effectively evolving with the passage of time.
This eBook will be of benefit for all stakeholders who are either interested in the Darknet or are doing activities in the Darknet so that they can be more educated about the legal and policy challenges thrown up by anonymity on the Darknet before legal frameworks.

Pavan Duggal

pavan@pavanduggal.com
pavanduggal@yahoo.com
http://www.linkedin.com/in/pavanduggal
http://www.twitter.com/pavanduggal
http://www.pavanduggal.com

ABOUT THE AUTHOR



Pavan Duggal, is the Founder & Chairman of International Commission on Cyber Security Law.

Pavan Duggal who is the president of CyberlawsDarknet, has been working in the pioneering area of Cyber Law, Cyber Security Law & Mobile Law. While a practicing Advocate, Supreme Court of India, Pavan Duggal has made an immense impact with an international reputation as an expert and authority on cyber law, Cyber Security Law and e-commerce law.

Pavan Duggal Has Been Acknowledged As One Of The Top 4 Cyber Lawyers Around The World.

WDD [World Domain Day] Recognises Pavan Duggal As One Of The Top 10 Cyber Lawyers Around The World.

His empanelment as a consultant to UNCTAD And UNESCAP On Cyber Law And Cyber Crime Respectively, Membership Of The AFACT Legal Working Group Of The UN / CEFAT, Consulting As An Expert With The Council Of Europe On Cyber Crime, Inclusion In The Board Of Experts Of European Commission's Dr. E-Commerce And His Work As An Expert Authority On A Cyber Law Primer For E-ASEAN Task Force And As A Reviewer For Asian Development Bank Speaks Volumes Of His Worldwide Acceptance As An Authority. Pavan is The President Of Cyberlaw Asia, Asia's Pioneering Organization Committed To The Passing Of Dynamic Cyber Laws In The Asian Continent. Pavan Is Also A Member Of The WIPO Arbitration And Mediation Center Panel Of Neutrals.

As an internationally renowned Cyber law and Cyber security subject expert, at

the world stage during the High-Level Policy Statement delivered by him at the World Summit on Information Society (WSIS) organized by the International Telecommunications Union (ITU), UNESCO, UNCTAD & UNDP in Geneva, Switzerland from 25th May – 29th May, 2015 Pavan Duggal has recommended the need for coming up with an #International #Convention on #Cyberlaw & #Cyber Security.

As a thought leader, Pavan has suggested that India requires a new that is wholly dedicated to cyber security.

Pavan Has Been The Member Of The Public Interest Registry's. Org Advisory Council. He Is A Member Of ICT Policy And Governance Working Group Of The UNICT Taskforce. He Is The Legal And Policy Consultant To Internet Mark 2 Project, Which Is Examining The Next Level Of Internet. He Has Been Invited To Be An Associated Fellow Of The Centre For Asia Pacific Technology Law And Policy (CAPTEL) At Singapore. Pavan Is A Member Of Panel Of Arbitrators Of The Regional Centre For Arbitration, Kuala Lumpur And Asian Domain Names Dispute Resolution Centre At Hong Kong.

Pavan Duggal Is A Panel Member Of Permanent Monitoring Panel For Information Security-World Federation Of Scientists

He Has Been Associated With The Ministry Of Communication And Information Technology, Government Of India On Cyber Law And Electronic Governance Legal Issues. He Is A Member Of Advisory Committee On E-Governance In Karnataka Constituted By The Government Of Karnataka. Pavan Is A Member Of Information Forensic Working Group On E-Information Systems, Security And Audit Association.

Pavan Is A Member Of Multi – Stakeholder Steering Group Of The Asia Pacific Region Internet Governance Forum (APrIGF)

Pavan Heads His Niche Law Firm Pavan Duggal Associates, Which Has Practice Areas, Amongst Others, In Cyber Law, Business Process Outsourcing Law, Intellectual Property Rights And Information Technology Law, Information Security Law, Defence, Biotech And Corporate Law.

While He Has Been A Member Of The Nominating Committee, Membership Advisory Committee And Membership Implementation Task Force

OfICANN, Pavan Is Also The President Of CyberlawsDarknet, Which Is Internet's First Ever-Unique Cyber Law Consultancy.

In Addition To That, He Is Also The Founder Of The Cyber Law Association And Is Also The Founder-President, Cyberlaw India.

Some Outstanding Pioneering Work In The Field Of BPO Legal Issues Has Resulted In His Being A Member Of The BPO Steering Committee Of ASSOCHAM. Today, He Advises A Number Of BPO Concerns On Different Legal Issues Relating To Outsourcing. Pavan Was The Chairman Of The Cyber Law Committee Of ASSOCHAM And Works Closely With CII And FICCI.

Pavan is a Regular on The Lecture Circuit. He Has Spoken At Over 1200 Conferences, Seminars and Workshops In The Last Seven Years, And Has Lectured Extensively In Select Law Colleges. As a writer, he has made his mark with sixty seven books on various aspects of the law in the last six years. He has contributed a continuing weekly column on diverse aspects of the law, titled 'Brief Cases' to the Economic Times, for the last seven years.

More about Pavan Duggal is available at http://www.linkedin.com/in/pavanduggal.

CONTENTS

- **Electronic Evidence And Anonymity On The Darknet**
- **Cybersecurity, Anonymity And Darknet**
- **Increasing Scope Of Darknet**
- **Conclusion**

DARKNET, ANONYMITY & LAW

Introduction

Internet is one of the biggest game changers in the history of mankind. Nothing has impacted mankind, so much since the advent of fire as the Internet. No wonder, today Internet is a transformative and innovative catalyst which is increasingly being adopted in various walks of human life. *Today, almost one-third of the world's 6.8 billion people use the Internet regularly*[1].

Internet gets used not only for legitimate purposes but also for criminal and terrorist activities. Cyber criminals use the Internet for perpetuating all kinds of frauds and illegal activities. From the perspective of terrorists, Internet opens up a vista of new opportunities. One of the primary uses of the Internet by terrorists is for the dissemination of propaganda. Propaganda generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers.[2]

Consequently, with the advent of increased cyber criminal and terrorist activities on the Internet, more and more countries have increasingly started targeting criminal activities online. State surveillance mechanisms have increased and aim to become more comprehensive, with each passing month. In a scenario like this, it is but natural to expect that criminals would look at a safe haven. Consequently, netizens and criminals have been searching for a new parallel network where they can be free from any kind of surveillance, and this is the beginning of the emergence of Darknet or Darkweb.

Consequently, we are beginning to see the evolution and increased adoption of the Darknet. A small proportion use sophisticated anonymity systems that offer stronger protection for an overview of these systems. The most popular anonymity system is called 'Tor'. In 2014, Tor had an estimated 2.5 million daily users.[3]

Definition

Darknet has been defined by various scholars and entities in a variety of ways. The term 'Darknet' is used to refer to websites whose operators can conceal their identity with sophisticated anonymity systems[4].

Wikipedia defines Darknet as 'An overlay network that can only be accessed with specific software, configurations, or authorization, often using non-standard communications protocols and ports.'[5]

Further A Darknet is a routed allocation of IP address space that is not discoverable by any usual means. The term is used to refer to both a single private network and the collective portion of Internet address space that has been configured in that manner. Technically, a Darknet is a variation on a virtual private network (VPN) with additional measures in place to ensure that the network and IP addresses of members are not discoverable.[6]

A Darknet is a Internet or private network, where information and content are shared by Darknet participants anonymously. Darknets are popular with users who share copy protected files as the service will let users send and receive files anonymously — that is, users cannot be traced, tracked or personally identified. Usually, Darknets are not easily accessible via regular Web browsers.[7]

The freedictionary.com defines Darknet as a network or internet service that allows users to transfer data anonymously.[8]

Darknet is a computer network that only a small number of people have the right to use and that is mainly used for sharing computer files, often illegally.[9]

Darknet is also defined as any network that operates clandestinely and hides the identity of its users, such as Silk Road, Freenet, Tor and anonymous Web surfing.[10]

Darknet Statistics

Darknet is believed to be a growing wide spread phenomenon. However, statistical figures pertaining to Darknet are increasingly difficult to find. Darknet tends to get used for variety of illegal and criminal purposes including for the trading of drugs and other contraband items as also weaponry. Drug consumers prefer to move online because dark net markets guarantee cheaper and better quality products and less exposure to violence, says the Global Drug Survey 2015, published on 7 June, 2015. The most extensive drug survey in history, it is based on the information obtained from more than 100,000 drug consumers from 50 different countries during November and December 2014.[11]

Darknet also came to prominence because of huge potential of its hidden market places. Until September 2013, the most prominent hidden market place on the Tor Network was Silk Road. It allowed users to sell and buy illegal drugs and other commodities in a format similar to that of eBay. From its launch in February 2011 until July 2013, the site processed over $1.2 billion worth of sales between 4,000 vendors and 150,000 customers.[12]

According to an August study by researchers at Carnegie Mellon University, criminals earn an estimated $100 million a year by selling drugs and other contraband on hidden websites using the virtual currency bitcoin, the digital cash that doesn't require a credit card or bank to process the transactions.[13]

One of the most significant aspects about the dark net is its anonymity thanks to the TOR or The Onion Router.

Salient Features of the Darknet

Darknet has got various salient features including the following:

i. Darknet, a network that can be accessed with specific software, configurations, or authorization using non-standard communications protocols and ports.

ii. Darknet by its own standards is an overlay network. An overlay network is a computer network that is built on top of another network.

iii. Darknet is the part of the World Wide Web.

iv. 'Darknet' is part of the Deep Web.[14]
v. Anonymity is an essential element of the darknet.
vi. Its contents are not accessible through normal search engines.
vii. It can be accessed through friend-to-friend networks.

viii. It can also be accessed through anonymity networks such as Tor via an anonymized series of connections.

ix. It is the anonymous Internet. Within the Darknet both Web surfers and website publishers are entirely anonymous.

x. It allows internet users to access the web and to create websites called Tor Hidden Services without revealing their identity.

xi. Darknet is used to monitor network traffic on unallocated IP space.

Darknet are sites that are using the **Tor (The Onion Router) network**. The basis of Tor network is to include so many nodes that the origin cannot trace where the data is going or where it is coming from. Normal browsers cannot open the Darknet websites whose top level domains are **.onion** because they are not normal domain names, but a string of random characters followed with **.onion.** .[15]

Definition of Anonymity

More and more people throng to the Darknet because of the anonymity that it provides.

Before proceeding forward, it is important to appreciate how the concept of anonymity is defined by different entities.

Anonymity, adjective "anonymous", is derived from the Greek word "*anonymia*" meaning "without a name" or "namelessness". In colloquial use, "anonymous" is used to describe situations where the acting person's name is unknown. It can be said as not using your own name, simply. Some writers have argued that namelessness, though technically correct, does

not capture what is more centrally at stake in contexts of anonymity. The important idea here is that a person be non-identifiable, unreachable, or untrackable.[16]

Anonymity means the quality or state of being unknown to most people; the quality or state of being anonymous[17]

The noun anonymity comes from a Greek word meaning "without a name." or the state of being anonymous.[18]

The definition of anonymity is the quality of being unknown.[19]

Concept of Anonymity

One needs to keep in mind that the concept of anonymity is a relative concept, more so in the perspective of the Internet. It is not an absolute concept, you cannot be 100% anonymous unless you decide not to be on the network at all. Now, keep in mind that nothing short of unplugging your computer will make you 100% anonymous. You can have fifty proxies and a handful of VPNs, but never consider yourself to be completely masked. Look at anonymity as a tradeoff between function and speed. The idea is to have enough masking, while maintaining a level of usefulness. While it is not impossible to track your actions, ideally you want to make it logistically too complex to be attempted in a realistic way.[20]

Normally speaking, the concept of anonymity brings forward distinct images in one's mind. A number of people would tend to see anonymity as being bad while others would want to see anonymity as an integral part of their basic human rights. There are no two doubts that anonymity can be used in a positive sense as well. As such, the anonymity provided by Tor has positive and legitimate uses.

Even the FBI, when writing up their report on the Silk Road arrests, acknowledged that it can be used for good, writing that “Tor has known legitimate uses”. Parker Higgins, an activist at the Electronic Frontier Foundation, wrote in the wake of the Silk Road raids that: “It's essential that the use of encryption, anonymization techniques, and other privacy practices is not deemed a suspicious activity. Rather, it must be recognized as an essential

element for practicing freedom of speech in a digital environment."Similarly, the Tor Project, which makes the browser, argues that it actually keeps normal people from becoming victims of crime.[21]

For the purposes of achieving anonymity, TOR plays an important role.

Tor relays a user's data through the Tor Network, which hides the user's Internet Protocol (IP) address and other identifiers from the websites they visit and disguises the user's online activities. This means that anyone monitoring internet communication will find it difficult to trace these activities back to a specific user. One of the main reasons for Tor's popularity is that users do not need to have a sophisticated knowledge of computers. The software enabling access to the Tor Network can be downloaded from the internet for free and is easy to install on a computer. It can also be used on mobile phones.

Tor allows users to do two distinct things:

use the open web anonymously with the Tor Browser, which looks similar to common web browsers such as Microsoft Internet Explorer or Mozilla Firefox

publish anonymous web services as Tor Hidden Services. [22]

Anonymity is an Integral Component of Darknet

Having examined the concept of anonymity, we now proceed to see as to why anonymity is an integral component of Darknet. In Darknet, a core aim is to preserve every user's anonymity. Each data stream is encrypted and routed in such a way that the source and destination of the request cannot, outside of user or program error, be determined. To prevent other forms of personal information from being leaked, it is common for Darknet application to deliberately mask or sanitize any identifiable information that is sent, such as information commonly provided by web browsers (The Tor Project, 2013b). There are also mechanisms available to applications that run on Darknets for users to maintain a consistent identity, should they wish to do so, thereby enabling users to be pseudo-anonymous. These aliases allow for social networks to be established and utilised.[23]

There are number of anonymous networks which are available on the Darknet. Tor (The onion router) is an anonymity network that also features a Darknet - its "hidden services". It is the most popular instance of a Darknet. I2P (Invisible Internet Project) is another overlay network that features a Darknet whose sites are called "Eepsites". Freenet is a popular Darknet (friend-to-friend) by default; since version 0.7 it can run as a "opennet" (peer nodes are discovered automatically).[24]

Consequently today, increasingly, the Darknet or the TOR network is used for the purposes of anonymous use of the Internet. This is invariably done for the purposes of circumventing harsh censorship regimes in different countries. The TOR or the dark network allows anonymous activism and journalism. Users use the TOR to protect their personal security and privacy and also for engaging in anonymous peer-to-peer file sharing. Further, law-enforcement agencies have also been covertly using TOR to access company websites without revealing their IP addresses to the website owner.

Seen from a global stage viewpoint, Darknet came into more prominence ever since the take down of the Silk Road online trading place. Darknet markets have multiplied since the first major takedowns in 2013, and continue to use advanced privacy and decentralisation technologies that have so far frustrated law enforcement efforts. An exclusively interdiction-based approach to Darknet markets is limited in its abilities to deter cybercrime on the Darknet, and may be politically precarious as privacy advocates will continue to criticise any circumvention of technologies that political activists and others depend on.[25]

Consequently, we find that the law-enforcement agencies are constantly trying to crack the dark markets on the Darknet.

An international law enforcement operation in early November, 2014, dubbed Operation Onymous, successfully took down more than 400 hidden sites operating on the so-called 'Darknet', in order to shut down these sites as part of a larger effort to combat the burgeoning flow of illicit goods and services through established forums and marketplaces accessible online.[26]

Assisting the anonymity ecosystem on the Darknet is the advent and increasing

popularity and adoption of various crypto currencies. Crypto currencies facilitate people to carry out economic transactions in conditions, which facilitate the protection of identities of people.

Recent dark market activity has surged with the advent of new Crypto currencies such as Bitcoin that have systematically decentralised payment processing and made it entirely anonymous. The tools and guides to connect to these sites, encrypt communications, or buy cryptocurrency are freely available on the open internet to download, and in some cases have been repurposed for illicit activity from initially unlikely development.[27]

Darknet & Cyberlaw

The bigger question remains as to what is the legal position on the entire issue of Darknet and its connected aspects of anonymity.

The first thing to note is that the world over, there is no specific law pertaining directly to the Darknet, which is applicable to the Darknet in particular. In fact, Darknet as a phenomenon itself is having perceptional issues. In large numbers of jurisdictions, we are seeing the typical response of law-enforcement agencies that they completely shake off their heads in disbelief and do not recognize the fact that Darknet already exists. Just because the law-enforcement agencies do not have the wherewithal to completely crack the Darknet and get the relevant cyber criminal activities done in the Darknet prosecuted, it does not mean that the Darknet as a phenomenon does not exist. In that connection, the question that now comes up for consideration is what exactly should be the legal frameworks to govern the Darknet and anonymity connected therewith.

There is no doubt in my mind that ultimately Darknet is nothing but a dark network which is hosted on computers, computer systems, computer networks, computer resources and communication devices. Further Darknet as a network uses data and information in the electronic form. That being so, all the salient elements which are used for the purposes of creating, hosting and sustaining the Darknet economy are computer resources as also data and information in the electronic form. As such, Darknet by a single stroke of logical reasoning, should be directly covered by all the cyber legal regimes in different parts of the world. This is so because Cyberlaw in different parts of the world have been enacted for the purposes of regulating activities done using computers, computer systems,

computer networks, computer resources and communication devices as also data and information in the electronic form.

So the fundamental conclusion is that cyber legal frameworks are directly applicable to the Darknet. While this appears to be a very attractive proposition, the fact still remains that the majority of the cyber legal frameworks have never been drafted keeping in mind the Darknet. Consequently, majority of the cyber legal frameworks do not have adequate mechanisms and processes and procedures on how to deal with anonymity on the Darknet.

Legal Issues Concerning Anonymity On The Darknet

Anonymity

In fact, when one looks at the jurisprudential concepts in different countries, one finds that anonymity is not an alien concept. In fact, the concept of anonymity is given legal recognition in various jurisdictions.

Anonymity & Its Legal Recognition

The concept of anonymity is old as human civilization itself. With the passage of time, the jurisprudence has legally recognized the concept of anonymity. Further, the right of anonymity also finds mention in various legislations in different parts of the world. The US has seen lot of growth of jurisprudence in this regard. Lot of privacy advocates advocate that the first Amendment to the US Constitution protects the right of anonymity. The First Amendment, however, does not explicitly guarantee a right to anonymity as such. Nevertheless, the Supreme Court has interpreted its guarantees of freedom of expression and assembly to protect anonymous expression within certain limits. [28]

The US Supreme Court has recognized the right of anonymity in the context of the right to freedom of association. In NAACP v. Alabama ex rel. Patterson, the Supreme Court held that the government may not compel organizations to disclose the identities of their members because it may restrain members' freedom of association.[29]

Beginning in 1960, the court also stated in a series of cases that U.S. citizens had

a right to be anonymous tied to protection of freedom of speech and the press. The general idea expressed in the decisions was that speech on controversial issues could be chilled if people were forced to identify themselves as the speakers. But the Court also has upheld laws requiring that people or corporations disclose their identities in certain situations, such as when they have signed petitions to place referendum issues on election ballots or donated money to a candidate.[30]

In the case entitled Talley v. California, 362 U.S. 60 (1960), the US Supreme Court held that the ability to anonymously distribute ideas goes to the core of free speech. The Court stated that anonymity has furthered freedom of expression throughout American history by allowing persecuted individuals and groups to disseminate their viewpoints.[31]

Anonymous communications have an important place in political and social discourse. The US Supreme Court has ruled repeatedly that the right to anonymous free speech is protected by the First Amendment. A frequently cited 1995 Supreme Court ruling in McIntyre v. Ohio Elections Commission reads:

*Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.****[32]***

In the case entitled McIntyre v. Ohio Elections Commission, the Court held that the ability to publish anonymously is guaranteed under the First Amendment unless a prevailing governmental interest overrides concerns for liberty.[33]

In other jurisdictions, we have seen that courts have not taken uniform approaches, while dealing with the concept of anonymity.

Courts in some nations have interpreted their constitutions as guaranteeing at least a limited right to speak and publish anonymously. In 2012, the South Korean Constitutional Court struck down a law passed in 2007 that required Internet users to verify their identities when they posted online comments.[34] The court said that the regulation violated free speech rights because anonymous

comments allowed people to express unpopular views without fear, and the regulation could chill such speech.[35]

In Canada, anonymity is sometimes recognized as tied to privacy interests, although there is no generalized constitutional right to privacy.[36]

In the Netherlands, as in Canada, there is no general constitutional right of anonymity, but it might be implied by the right to free expression, the right to personal and data privacy[37]

From the perusal of the aforesaid, it is thus clear that the law regarding online anonymity is largely unsettled around the world. Because the Internet is by nature a global medium, such a lack of consensus causes some concern, but anonymity also joins a long list of legal issues that are unresolved regarding the Internet and its global reach.[38]

While the anonymity has to be respected, there is increase in convergence of thought process that anonymity cannot itself become a tool for engaging in criminal or illegal activities. In that regard, there is an increasing recognition of the significance of anonymity as a challenge.

Anonymity is the greatest challenge in the evolving, measurable, interactive one-to-one world we live and market in. Piercing the veil of anonymity is critical to deliver personal, customized super-relevant interactions which lead to sales and ultimately help build valuable on-going customer relationships. Privacy and perceived value guard the unknowns. Consumers and business people are anxious about revealing themselves because they don't trust us.[39]

In fact, the concept of anonymity is significant for legal jurisprudence in different parts of the world. In fact, the John Doe jurisprudence that has evolved across the world is nothing but an implicit recognition of the anonymity of distinct legal entities whose identity is not known at the time of filing the lawsuit. However, as and when the identity of the said user is known, the said user with its real actual identity is impleaded in the legal actions. As such, the John Doe action is also nothing but a manifestation of legally recognizing the

concept of anonymity.

The John Doe jurisprudence is also ultimately based on the thought process that the anonymous John Doe must be identified and hence the focus of the John Doe jurisprudence is ultimately to pierce the anonymity veil, behind which the anonymous John Doe is hiding. In fact, the piercing of the said anonymity veil on the superficial web is far simpler, when compared with piercing the anonymity veil on the Darknet.

The important question that comes up for consideration is how can anonymity on the Darknet be appropriately addressed by legal frameworks? This question assumes a lot of significance since large amount of cybercriminal activity gets done in the dark net. Darknet today is a fertile marketplace for a variety of cyber criminal activities.

As per THE TOR DARK NET report published by the Global Commission on Internet Governance, it has been reported that Darknet is now increasingly being used for a variety of purposes like Abuse, Anonymity, Bitcoin, Blog, Books, Chat, Counterfeit, Directory, Drugs, Forum, Fraud, Gambling, Guns, Hosting, Market, News, Pornography, Search, Whistleblower, Wiki.[40]

Invariably, cybercriminals, who want to hide their footprints behind the various levels of anonymity and encryption, often tend to use Darknet. When one examines the early days, the TOR network was primarily developed as a means for providing a fertile platform for people for legitimate uses in order to hide their identity for expressing political dissent and other view points and for providing the place where a person could be free to express his own opinions without any fear of retribution or punishment.

But just as the TOR network allowed legitimate people to hide their identities and continue to express their dissenting political thought processes, it also allowed a wonderful opportunity for cyber criminals to hide behind the levels and layers of anonymity so as to engage in cyber criminal activities. No wonder, by and large people started hiding behind the levels of anonymity provided by the Tor network and started conducting activities with impunity. As such, catching cybercriminals became increasingly very difficult on the Darknet.

It is in this regard that the question, that is increasingly being asked is, can the anonymity veil on the Darknet be pierced? Before one proceeds forward in this

direction, it is important to understand a similar debate that took place in the context of the superficial web. Earlier, when the Internet came along and people were enamored by the Internet, most of the users thought that the Internet was a Wild-Wild-West, where they could do anything illegal, which they were unable to do in the physical world. However as time passed by, it became crystal clear that the Internet was not a Wild-Wild-West but a place, where the rule of law principles applied with equal vigour. Consequently, with the evolution of Cyberlaw as a distinct jurisprudence, in different countries, courts, through their orders, pierced the anonymity veil on the Internet, so as to ensure that the real identity of offenders could be brought to the forefront for law-enforcement agencies with the help of the logs and the respective information from intermediaries and service providers.

Today a similar kind of dilemma is being repeated in the context of the Darknet. Large numbers of users of the Darknet distinctly believe that Darknet is also completely anonymous and that because it is anonymous, it allows people to believe that the Darknet is the Wild-Wild-West. According to an Edward Snowden leak in October 2013, the NSA, during a top-secret presentation in 2012, considered Tor a threat. "Tor stinks," reads the title of one NSA slide. "We will never be able to de-anonymize all Tor users [but] we can de-anonymize a very small fraction. " (When contacted by Rolling Stone, the NSA declined to comment.) In another of Snowden's revelations, Britain's intelligence agency, the Government Communications Headquarters, dismissed the democratic potential of Tor as "pseudo-legitimate uses" that paled next to the "bad people" who ruled the Darknet.[41]

A perusal of the existing information in the public domain would clearly show that while the law-enforcement agencies have been able to de-anonymize some users, they are not able to de-anonymize all TOR users for all times to come.

It has been reported that an Italian surveillance tech company, *Hacking Team*, has offered to help the FBI remove its encryption obstacles. In an email, CEO and founder David Vincenzetti suggested he could solve the FBI’s Darknet dilemma.[42]

It thus becomes important to appreciate the current advances of technology. There have been reports which point out that now increasingly, there are vulnerabilities that have been discovered in the TOR network.

In fact, this has had such an impact that Agora, one of the underground Darknet websites, has decided to close its website on the darknet till such time they are able to find appropriate answer to the said vulnerabilities. At the time of writing, the Agora market place has still not gone live on the Darknet.

Right To Hide On Darknet

Another important principle that needs to go in the direction of the development of anonymity jurisprudence on the Darknet deals with the right to hide. The right to hide is often considered as part of the bundle of rights that people have. However, there is growing clarity that people do not have a right to hide behind the layers or encryption levels of anonymity on the Darknet so as to perpetuate and engage in cybercriminal activities as a matter of right. In fact, such an exercise runs contrary to established cannons and principles of jurisprudence in different parts of the world.

Another important principle that needs to be considered is that the law-enforcement agencies only need to have limited rights and grounds to pierce anonymity veil on the Internet provided it is proved that the said anonymity veil is being used or abused by the said stakeholders for the purposes of engaging in completely illegal or criminal activities.

However, anonymity on the Darknet is not absolute and is only relative. It has been reported that Tor has a few serious issues with it that do need to be addressed. The most critical is a lack of end-to-end encryption. This means anyone who can sniff the traffic from an exit node can see EVERYTHING. They still have to trace packets back and forth to determine a location, but all the encryption is gone.[43]

Power Of Courts To Pierce Anonymity Veil On Darknet

Another important legal issue that arises for consideration concerns the power of the courts to pass orders directing piercing of anonymity veil on the Darknet. First and foremost, it needs to be appreciated that courts of law have intrinsic powers to pass various orders and that would include the powers to pass orders directing the piercing of the anonymity veil on the Darknet. However, the bigger issue is how will such court orders be effectively enforced. This is so

because of the intrinsic manner in which technology of TOR actually functions. As such, judicial agencies have to be mindful of the fact that they do not need to pass any orders which become mere paper tiger orders or which will not be capable of being effectively implemented.

Privacy and Anonymity on the Darknet

Most activists view the government's battle against the Darknet as the new Reefer Madness, a misguided attack on something becoming increasingly endangered: privacy and anonymity online.[44]

Privacy is big issue as far as the Darknet is concerned and that is why more and more people are increasingly adopting encryption tools for the purposes of protecting their data and personal privacy.

An important issue which requires mentioning is can anonymity on the Darknet protect personal privacy? Can anonymity on the Darknet protect data privacy? The answers to both these questions appear to be in the affirmative at the time of writing. This is so because when a person's identity is hidden behind various layers of anonymity, the said hiding itself ensures that his personal privacy as also data privacy is intrinsically protected. However, when one examines the legal frameworks existing in different parts of the world, one realizes that the existing legal frameworks on privacy often do not shed much light on the interconnection between privacy and anonymity.

Given the fact that anonymity is an integral part of the TOR browser, it is therefore essential that anonymity needs to be recognized as an important tool for protection and preservation of personal and data privacy. However, how should law deal with the interconnection between anonymity on the Darknet on the one hand and protection and preservation of personal and data privacy on the other hand, is an important question that needs to be appropriately addressed by various stakeholders with the passage of time.

While different countries may adopt different approaches, it will be imperative that the intrinsic connection between anonymity on the one hand and data privacy and personal privacy protection on the other, is intrinsically recognized.

Intermediaries , Anonymity And The Darknet

Intermediaries have also got a connection with piercing the anonymity veil on the Darknet. This becomes evident , given the emerging geo-political realities of the world. Ongoing trends in law, policy, and technology threaten anonymity as never before, undermining our ability to speak and read freely online. These trends also undermine national security and critical infrastructure by making communication among individuals, organizations, corporations, and governments more vulnerable to analysis.[45]

Intermediaries have an integral role in contributing information and data for analysis by law enforcement agencies. In different parts of the world, intermediaries and service providers have been straddled with responsibilities to provide data, logs and information, as and when so demanded by the law enforcement agencies.

However, while the obligations of the intermediaries can be fulfilled in the context of the superficial web, Darknet present distinct challenges in this regard.

Clearly, the role of intermediaries becomes very significant in the digital ecosystem . Invariably on the superficial web, it is possible to direct the network service providers and intermediaries to give information about offending activities and the offenders from the logs of the said service providers or intermediaries. Invariably logs, that are created on the superficial web, provide various traces to identify the real identity of the offenders.

Today there are various ways in which users of the superficial web stand exposed vis-à-vis their identity to law enforcement agencies. Users can be tracked through their online activities in terms of their content being posted, their relevant IP addresses traced, using cookies as also browser finger printing. The law enforcement agencies are increasingly employing new, untested and often unknown techniques to unmask the real identity of people who are hiding behind the anonymity veil.

However, the Darknet as an intrinsic phenomenon is a completely different paradigm altogether. Here, like a relay race, runners tend to hand over the baton to the next runner and then the process repeats. However, the first runner never meets the third runner. In the same analogy, various communications pass through different layers of encryption. In such a scenario where anonymity is built as an integral defacto norm of electronic communication, the bigger issue is

how can law enforce the disclosure of identity of offenders by intermediaries.

On the Darknet using the TOR , it is very difficult for the intermediary or service provider to find out the real identity of the visitor or the user who is using the website or the Darknet platform for the purposes of carrying out and doing any illegal activity.

As such, as technology develops, legal frameworks will have to quickly evolve innovative approaches in this regard. Law needs to recognize the intrinsic role of intermediaries and straddle them with appropriate responsibilities of due diligence.

Another related aspects that merits mention is the entire issue of Intermediary liability. In the context of the superficial web, already different countries have adopted different approaches. A majority of countries follow the US model where under the Communication Decency Act, service providers are often considered as mere 'pipe' providers and in their capacity as service providers have not been made liable for what flows through the 'pipe'. There are other models of intermediary liability in different countries where intermediaries are made liable for third party data or information made available by them. In addition, there are some other jurisdictions like India where in a nuanced manner, by and large the network service providers and intermediaries are not made liable for third-party data information made available by them on their network so long as they fulfill certain minimum parameters including complying with the parameters of law and ensuring documented due diligence while they discharge their obligations under the law.

Case law in this direction is also evolving in different parts of the world.

It is pertinent to note that in 2009, the Swedish courts found that the operators of the Pirate Bay site had criminally infringed Swedish copyright law, and sentenced them to a year in jail and a £2.4million fine.[46]

The Court was categorical that *"...all the defendants were aware that a large number of the website's users were engaged in the unlawful disposal of copyright-protected material. By providing a website with advanced search functions and easy uploading and downloading facilities, and by putting individual file-sharers in touch with one other through the tracker linked to the*

site, the operation run via The Pirate Bay has, in the opinion of the District Court, facilitated and, consequently, aided and abetted these offences."[47]

However, Darknet present distinct challenges in the context of the role of intermediaries.

As such, the entire issue pertaining to intermediary liability in the context of the dark web needs to have a revisit and relook. A majority of the service providers and intermediaries would invariably say that they have no physical control on how the activities of the Darknet can be appropriately monitored by them and in such a scenario, it is impossible for them to monitor the said usage of the Darknet. As such, there is going to be tremendous pushback from the intermediaries and service providers who would want to protest against any cyber legal frameworks, which are going to make them liable for detecting identities of wrongdoers using technologies that anonymize their identity.

The important issue that requires consideration is how can law provide a mechanism for legally piercing the anonymity veil on the Darknet. We have seen in the context of the superficial web of how different courts have been passing orders in John Doe jurisprudence against unknown defendants. The concept of John Doe needs to be further expanded and customized to be made applicable in the context of the Darknet. In this regard, the issue of roles and responsibilities of intermediaries merits detailed discussion and analysis.

As such, these are still early days yet but clearly the entire issue of intermediary liability on the Darknet is a very complicated issue and would need to be have a fresh look at in the coming times, in case, the law wants to be more effective in the direction of appropriately regulating anonymity on the Darknet.

An important principle that needs to evolve in this direction is that the anonymity veil on the Darknet needs to be pierced in case the said anonymity is being used for various illegal criminal purposes. Further, there also needs implicit recognition of the fact that the piercing of the anonymity veil on the Darknet should not be used as a handle to pierce the anonymity of those law abiding citizens who are doing legal activities in the bonafide legitimate manner on the Darknet for the purposes of protecting their identity and privacy.

In fact, the important principle that needs to be recognized is the fact that

anonymity on the Darknet is intrinsically related with protection and privacy of the users on the Darknet. In fact, it is the anonymity of the Darknet which itself ensures data privacy as well as personal privacy of users on the Darknet.

Hence legal frameworks concerning Darknet should be developed keeping in mind that this intrinsic desire for privacy, which is a part of normal human inclination and right, is not trammeled upon under the garb of regulating cybercrime by law enforcement agencies.

As time passes by, there is a need for continued collaboration between the states, the law enforcement agencies and also the intermediaries in order to contribute in the direction of regulating criminal activities onto the Darknet.

Law Enforcement And Anonymity On Darknet

Seen from national governments' standpoint, who are committed towards preventing cybercrime, law enforcement agencies feel handicapped because of the anonymity veil provided on the Darknet. Hence, law enforcement approaches towards targeting criminal activities on the Darknet have been limited and tardy. Law enforcement responses to the Dark Net have configured around traditional strategies of surveillance, interdiction and prosecution, although from a low base of technical capacity, with limited transnational integration and within the constraints imposed by national legislative frameworks.[48]

By and large, the approaches adopted by the law enforcement agencies in the context of the Darknet are more disruptive in nature in terms of shutting down or disrupting the specific criminal activities done on the Darknet. However, that is only a reactive approach. As time passes by, law enforcement agencies would need to come up with more proactive approaches on how to deal with increasing criminal activities done on the Darknet. Also, the law enforcement agencies need to keep in mind the robustness of the Darknet. On one market place on the Darknet being cracked or shut down by the law enforcement agencies, they are ten more which are ready to come within a very short period of time.

There is a need for law on the Darknet to evolve whether in the context of anonymity or in the context of other legal and policy challenges that the Darknet actually presents. Darknets have become a major headache for government agencies such as the FBI, NSA, and the IRS. Rules regarding collection of

evidence of cyber crimes are extremely outdated, and in turn, criminals on Darknets have adapted.[49]

The law enforcement agencies have increasingly started adopting mechanisms of piercing the anonymity veil on the Darknet and targeting cyber criminals. In October 2013, the FBI took a historical step of arresting the operator of the illegal Darknet market place being Silk Road.

In the criminal complaint, the FBI describes that the suspect was identified as the Silk Road operator based on his activities on the open web, including posts about Silk Road on discussion forums, where he registered using his real name and email address. However, it is not publicly known how the FBI identified the IP address of the server hosting the Silk Road. [50]

Various arrests have been made by the different law enforcement agencies by piercing the anonymity veil. Further in November, 2014 the international operation Onymous, which involved LEAs of 16 European countries and the US, led to the shutdown of more than 400 addresses linking to 27 distinct THS, including Silk Road 2.0[51]

Snowden revelations recommended different approaches for monitoring the Darknet sites. Dark web sites go offline and resurface all the time—Chertoff notes that it's "essential to get a snapshot of every new site as soon as it is spotted, for later analysis or to monitor its online activity."[52]

- **Law Needs To Do A Balancing Act**

Tor is used for journalism, whistleblowing, law enforcement investigations and the circumvention of internet censorship, as well as for drug dealing and other crimes. Some of the legitimate uses of the Darknet by its users include Circumventing censorship, Anonymous activism and journalism, Under-cover online surveillance, Protection from criminals and Anonymous peer-to-peer files sharing as also Whistleblowing.

The illegal uses of Darknet are manifold. These include hosting and running of Criminal markets as well as hosting and publishing of Indecent images of

children and Terrorism [53]

There have been several large law enforcement operations against criminal activities on Tor. It is not publicly known how law enforcement agencies de-anonymise criminal Tor users or the extent to which this involves surveillance of non-criminal users. [54]

The bigger issue before legal frameworks across the world is how can the concept of anonymity on the Darknet be legally tackled in such a manner so as to achieve a balancing trick –there is a need for balancing both the legitimate needs of law enforcement agencies to crack on cyber criminal activities on the Darknet and also the rights of privacy and anonymity of legitimate genuine users of the Darknet to use the anonymity levels and protections of Darknet for the purposes of engaging in legitimate bonafide legal activities including political dissent or expression of their thought processes.

At the time of writing, the legal concepts pertaining to the Darknet are only beginning to evolve. In fact, the world over, there is no unanimity on how the legal frameworks on anonymity need to evolve. However, very quickly law-enforcement agencies and other stakeholders in the digital ecosystem have to realize that Darknet as a phenomenon will require universal principles of jurisprudence to be applicable to the Darknet. Countries do have national legislations, but you can't have the said legislations to effectively govern the Darknet in a distinctly sectoral, parochial manner. This is again so because Darknet also brings forward various issues pertaining to jurisdiction. In fact, there are various dark websites, dark servers and hence it is very difficult to find out what is the exact location of the dark website or the dark server. In that case, the Darknet jurisdiction becomes a very important legal challenge that needs to be appropriately addressed by the law-enforcement agencies as also by legal frameworks in the coming times.

Electronic Evidence And Anonymity On The Darknet

Another important principle that needs to be considered is what kind of rules for gathering electronic evidence in terms of detection, investigation and prosecution of criminal activities on the Darknet are going to be followed? This is one question that doesn't appear to have a ready-made answer. This is all the

more so since the various layers of anonymity and encryption provided by the TOR itself ensures that it becomes a horrendous and extremely challenging task for the law-enforcement agencies to collect the entire nexus or chain of electronic incriminating evidence by means of which a particular legal entity can be incriminated for illegal or criminal activities done on the Darknet.

Different countries have in place different national electronic evidence legal frameworks. However, majority of the said frameworks would not be applicable in the context of the Darknet, given the fact that it becomes an extremely challenging task for the law-enforcement agency to prove the entire chain of electronic evidence which can help nail down the cybercriminal activities of the cybercriminals on the Darknet. Lot of work in this regard needs to be done with the passage of time. Fortunately some steps in this direction have begun to start happening. INTERPOL in July 2015 started training program for officers.

In July 2015, Interpol held its first-ever training on "identifying the methods and strategies used by organized crime networks and individuals to avoid detection on the Darknet." That same month, FBI Director James Comey explained to a U.S. Senate Judiciary Committee the agency's plight in tracking encrypted communications. "The tools we are asked to use are increasingly ineffective," he said.[55]

It is therefore essential that appropriate international norms pertaining to electronic evidence will have to be revisited and revised keeping in mind the specific customized requirements of the Darknet. Further, national legislations with electronic evidence provisions will also have to be appropriately devised in different jurisdictions., keeping in mind appropriate exigencies on how to deal with the distinct challenges pertaining to production and proof of relevant electronic evidence on the Darknet under normal legal processes.

Legal concepts need to be made far more flexible and robust to allow the development of new legal approaches. The TOR network is a new world. The new world has new parameters. The new world demands and dictates the adoption of new customized approaches to deal appropriately with the same. As such, there will be need for coming up with distinct new legal approaches to deal with electronic evidence related issues and also deal with other legal challenges faced by the Darknet.

Cybersecurity, Anonymity And Darknet

Another important issue that invariably is not getting much attention but will become increasingly very important with the passage of time is the intrinsic dangers and threats that cyber security of nations is facing from anonymity on the Darknet.

Invariably Darknet is being presumed to be just limited to use of the dark network for the purposes of selling drugs, weaponry and all kinds of illegal activities. What the world does not yet appeciate is that the Darknet tomorrow is likely to become the fertile breeding ground for cyber criminals who would go ahead and breach cyber security of computer systems, networks and resources in different parts of the world and try to attack and prejudicially impact the sovereignty of sovereign nations. As such, cyber security breaches will continue to emanate in a massive numbers from the Darknet.

This will invariably also be resorted to as cyber criminals would increasingly realize that it will take quite some time for the law-enforcement agencies to detect the real identity on the Darknet. In such cases, the perpetuators of cyber security breaches would have obliterated their electronic footprints and would have moved miles ahead of law enforcement agencies, without any fear of being caught.

Legal frameworks have to be effectively evolved in such a manner that the Darknet does not become a breeding ground for launching cyber security breaches which aim at not just destabilizing computer networks and resources of corporate and various stakeholders but also which are aimed at destabilizing and prejudicially impacting the sovereignty, integrity and security of sovereign nations. As such, international norms will have to be appropriately evolved to make sure that countries are unanimous in ensuring that Darknet does not become a ground for launching cyber war or cyber terror attacks targeted at specific jurisdictions.

There is a need for new technological protocols in this regard. There is also need for new distinct legal frameworks in this regard. At the time of writing, very less work has been done on legal principles pertaining to anonymity on the Darknet. This is one big area that will have to be addressed as a primary responsibility by legal scholars and jurists as they move forward in the direction of regulating of the onion land or the dark web.

Increasing Scope Of Darknet

Darknet is only going to increase its scope, ambit and applicability. In fact, it is increasingly going to become part of mainstream digital life. As has been stated by Jamie Bartlett speaker on TedTalk, in his speech 'How the mysterious dark net is going mainstream'," The Darknet is no longer a den for dealers and a hideout for whistleblowers; its already going mainstream.… I predict that fairly soon every social media company, every major news outlet and therefore most of you in this audience will be using the dark net too."

Describing the scope of the problem, Virgin explains:

"Tens of thousands of predators use the dark web every day as an exchange for media and information as well as a support group. More concerning than the current size and scope of the activity is the current growth, which has expanded dramatically in the past year. The dark net is also the location where the most extreme activity takes place."

Tens of thousands of paedophiles are using the so-called dark net to trade images of sexual abuse, an investigation by BBC News indicates. One site receives as many as 500 page views per second, its founder says.

GCHQ, the government's listening post sees the dark web as an "ungoverned" part of the internet, one of the "darkest places" inhabited by "the plotters, the proliferators and the paedophiles". It offers, GCHQ's outgoing head Sir Iain Lobban warned, a haven for "the worst aspects of human nature."

The dark side of the Darknet is getting more horrible and is getting extremely large and that appropriate legal frameworks have to be quickly evolved to deal with the dark network.

Conclusion

From the aforesaid discussion, it is thus clear that the Darknet is becoming an integral part of our digital lives.

The deep Web — in particular, networks on the dark Web such as Tor — represents a viable way for malicious actors to exchange goods, legally or

illegally, in an anonymous fashion… It would not be surprising to see the criminal underbelly becoming more fragmented into alternative dark nets or private networks, further complicating the job of investigators. The dark Web has the potential to host an increasingly large number of malicious services and activities and, unfortunately, it will not be long before new large marketplaces emerge.[56]

More and more people are now migrating to the Darknet. Cyber criminal activities have become the defacto norm of the Darknet. In this scenario, a majority of cyber criminals and cyber terrorists are invariably misusing the anonymity veil provided on Darknet. As such, one of the biggest challenges before cyber legal jurisprudence is to come up with appropriate legal frameworks, principles and mechanisms which can help address the challenges raised by anonymity veil on the Darknet and how the said anonymity veil on the Darknet can be appropriately pierced.

Darknet is still at a very early stage of its development. As time passes by, we are likely to see far more enhanced models of Darknet being adopted.

Cyber legal frameworks need to adopt more customized approaches to deal with the challenges of the Darknet. Anonymity on the Darknet is the salient feature of the Darknet and would invariably continue to be misused for a variety of illegal and criminal purposes with the passage of time. Currently, at the time of writing, law-enforcement agencies across the world do not have much clue of how to deal with breaking the anonymity veil on the Darknet. As such, legal frameworks are far-far behind and haven't even begun applying their minds on how the legal framework and principles also need to be so adopted and developed in a manner so as to deal with the legal challenges posed by anonymity on the Darknet. However, this is one area that is becoming increasingly very significant.

The Author in his earlier book “Darknet & Law” has already elaborated various other legal concerns and challenges raised by the Darknet. The legal challenges raised by the anonymity on the Darknet continue to be one of the fundamental challenges that Darknet as a phenomenon and paradigm is throwing up. Current existing position is that there are no international legal frameworks, which are applicable to the Darknet

More legal elastic and robust frameworks will have to be evolved so as to deal with the distinct challenges posed by technology, TOR as also the Darknet in the direction of dealing with the concept of anonymity on the Darknet and in the direction of enabling legal frameworks to pierce the anonymity veil on the Darknet. This is a very complex subject and lot of work has to be done in this regard.

I hope that with the passage of time legal scholars and jurists will start identifying the piercing of anonymity veil as an important legal priority to address. Further as cyber security law as a discipline develops, cyber security law will also have to be increasingly concerned with how to effectively legally regulate the anonymity on the Darknet in such a manner that the same is not misused for the purposes of infiltrating the cyber defenses of nations and also breaching the cyber security of computer systems and computer networks of individuals, corporates, stakeholders and the government as also prejudicially impacting the sovereignty, security and integrity of sovereign nations.

Anonymity on the Darknet will continue to be a major challenge facing legal frameworks in the coming times. It will be interesting to see how the evolution of new jurisprudence in this regard will distinctly evolve with the passage of time.

---

[1] http://www.history.com/topics/inventions/invention-of-the-internet
[2] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[3] file:///D:/2015/AUGUST/DARKNET/misc/POST-PN-488.pdf
[4] http://www.parliament.uk/briefing-papers/POST-PN-488.pdf
[5] https://en.wikipedia.org/wiki/Darknet
[6] http://searchnetworking.techtarget.com/definition/darknet
[7] http://www.webopedia.com/TERM/D/darknet.html
[8] http://www.thefreedictionary.com/darknet
[9] http://www.macmillandictionary.com/dictionary/british/the-darknet
[10] http://www.pcmag.com/encyclopedia/term/40718/darknet
[11] http://www.coinfox.info/2174-global-drugsurvey-bitcoin-dark-net-markets-do-not-make-people-drug-addict

[12] www.parliament.uk/briefing-papers/POST-PN-488.pdf

[13] http://www.rollingstone.com/politics/news/the-battle-for-the-darknet-20151022
[14] POSTNOTE, Number 488 March 2015, House of Parliament
[15] http://www.thewindowsclub.com/darknet-deepnet
[16] https://en.wikipedia.org/wiki/Anonymity
[17] http://www.merriam-webster.com/dictionary/anonymity
[18] http://www.vocabulary.com/dictionary/anonymity
[19] http://www.yourdictionary.com/anonymity
[20] http://null-byte.wonderhowto.com/inspiration/anonymity-darknets-and-staying-out-federal-custody-part-one-deep-web-0133455/
[21] http://www.independent.co.uk/life-style/gadgets-and-tech/news/darknet-what-is-it-and-what-are-the-dangers-of-the-governments-secret-browsing-crackdown-9917649.html

[23] http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1151&context=ism
[24] https://en.wikipedia.org/wiki/Darknet
[25] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet
[26] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet
[27] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet

[28] http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3942&context=flr
[29] http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4914&context=flr
[30] *See, e.g.*, Citizens United v. Federal Election Commission, 558 U.S. 310, 366-71 (2010) (upholding disclaimer and disclosure requirements for corporations sponsoring advertising or other speech favoring or opposing a political candidate).
[31] http://cyber.law.harvard.edu/lesson7/anonymity_cases.html

[32] https://www.eff.org/issues/anonymity

[33] http://cyber.law.harvard.edu/lesson7/anonymity_cases.html
[34] Choe Sang-Hun, *South Korean Court Rejects Online Name Verification Law*, N.Y. TIMES, Aug. 24, 2012,
at A8.
[35] Constitutional Court [Const. Ct.], 2010Hun-Ma47&252 (consol.), Aug. 23, 2012 (S. Kor.).

[36] Carole Lucock & Katie Black, “Anonymity and the Law in Canada,” in Kerr, et al., *supra* note 45.
[37] DUTCH CONST. (GRONDWET) ART. 10 (2008).
[38] Anonymous Online Comments: The Law and Best Media Practices from Around the World- International Press Institute
[39] http://manhattanmarketingmaven.blogs.com/mmm/2005/10/piercing_the_ve.html
[40] https://ourinternet-files.s3.amazonaws.com/publications/no20_0.pdf
[41] http://www.rollingstone.com/politics/news/the-battle-for-the-darknet-20151022
[42] https://medium.com/@CandiceLanier/isis-on-the-darknet-fundraising-networking-plotting-all-out-of-the-reach-of-law-enforcement-246c9d824c6a#.kx4dwiy1v
[43] http://null-byte.wonderhowto.com/inspiration/anonymity-darknets-and-staying-out-federal-custody-part-two-onions-and-daggers-0133474/
[44] http://www.rollingstone.com/politics/news/the-battle-for-the-darknet-20151022

[45] https://www.torproject.org/about/overview.html.en
[46] http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_interm
[47] http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_interm
[48] http://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug
[49] http://ryanwmp2.blogspot.in/2015/04/regulation-of-cybercrime-and-darknet.html
[50] www.parliament.uk/briefing-papers/POST-PN-488.pdf

[51] www.parliament.uk/briefing-papers/POST-PN-488.pdf
[52] http://motherboard.vice.com/read/six-ways-law-enforcement-monitors-the-dark-web
[53] Post Note(Number 488 March 2015) on The darknet and online anonymity published by House of Parliament, parliamentary Office of Science and Technology, UK.
[54] Post Note(Number 488 March 2015) on The darknet and online anonymity published by House of Parliament, parliamentary Office of Science and Technology, UK.
[55] http://www.rollingstone.com/politics/news/the-battle-for-the-darknet-20151022
[56] https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf