Canadian Journal of Law and Technology

Volume 15 | Number 1 Article 7

1-1-2017

The Dark Web: Some Thoughts for an Educated Debate

Vanessa Henri

The Dark Web:
Some Thoughts for An Educated Debate

Vanessa Henri, LL.B, LL.M[*]

Abstract

The "dark web" is a part of cyberspace that is only accessible through an anonymity software, such as The Onion Router. This encrypted network has prompted important legal challenges. As jurisprudence develops, many factors are at risk of inhibiting users' right to privacy. Misunderstandings of the dark web's functioning or myths regarding its veil of anonymity has justified invasive criminal investigations that has threatened users' right to remain anonymous online. This article discusses these challenges while analyzing current legal developments in the United States and Canada.

> Sector by sector the state is being cut out of the equation and power is being returned to the individual. I don't think anyone can comprehend the magnitude of the revolution we are in. I think it will be looked back on as an epoch in the evolution of mankind.[1]
>
> — Ross Ulbright (Dead Pirate Roberts, administrator of Silk Road)

Over the last decade the "dark web" has emerged in the media as a site of anarchy, where criminals can conduct their business in impunity. Headlines about worldwide drug markets[2] and online pedophilic communities[3] have prompted questions as to whether a wider range of power for law enforcement is necessary in order to combat crime in the digital world.[4]

[*] D.C.L. Candidate, McGill University. The author wishes to thank the Quebec Bar Foundation which funded the publication of this article and further researches on cyber criminality, legislative intervention and the dark web.

[1] Andy Greenberg, "An interview with a digital drug lord: The Silk Road's Dread Pirate Roberts (Q&A)," *Forbes* (14 August 2013), online: < www.forbes.com > .

[2] See most recently "Why China's plan to build a new Silk Road runs through Singapore," *Bloomberg* (14 August 2016), online: < www.bloomberg.com > ; Max Plenke, "Drug sales on the dark web have tripled since the demise of Silk Road," *Business Insider* (12 August 2016), online: < www.businessinsider.com > ; "Despite Silk Road's demise, more illicit drugs are being bought online," *Sputnik News* (14 August 2016), online: < www.sputniknews.com > ; Curtis Silver, "Illicit online drug sales triple in absence of Silk Road," *Forbes* (11 August 2016), online: < www.forbes.com > .

[3] See most recently Bob Brenzing, "Grand rapids man sentenced for trading child porn on 'dark web'," *Fox17 West Michigan* (21 July 2016), online: < www.fox17online.com > .

[4] See David Kushner, "The Darknet: is the Government destroying the 'Wild West of the Internet'?," *Rolling Stone* (22 October 2015), online: < www.rollingstone.com > ; Steve Ranger, "Hacking by police 'inevitable' thanks to use of encryption," *ZD Net* (11 June 2015), online: < www.zdnet.com > .

Nonetheless, the dark web hosts more than just criminals. The most popular software to access this network, The Onion Router (Tor), has about 2.5 million users daily[5], including students, researchers, journalists, human rights workers and members of the parliament or law enforcement who need to protect sensitive information. Following Snowden's revelations on the activities of the National Security Agency, many felt their privacy was not protected on the internet. Others use the dark web to avoid the surveillance of totalitarian governments such as China's communist party, which use the Great Firewall of China as the main means of internet censorship.

In today's high-tech world, the right to privacy is perceived as a safeguard against the threat of a big-brother type of government — a threat which was specifically recognized by the Supreme Court of Canada in *R v Duarte*.[6] This right, while not protected explicitly by the *Canadian Charter of Rights and Freedoms*,[7] is manifested in s. 8 of this document, which protects against unreasonable searches and seizures. In addition, privacy is crucial to freedom of speech[8] in the sense that anonymity encourages individuals to speak freely.

The literature has suggested that technological changes have impacted human rights, particularly the right to privacy.[9] Precisely, this is demonstrated by the emergence of stricter standards regarding the handling of personal information and the necessity of due diligence concerning protection of this data.[10] In criminal matters, especially in dark web cases, the right to privacy is at risk of being engulfed by the perception that enlarging law enforcement's reach is beneficial and required.

This perception is fueled by law-officials' misunderstandings relating to the technological aspects of the dark web and of its apparent impenetrability. Indeed, judges do not have the credentials nor the experience regarding the dark web and its functionality thereby forcing them to blindly trust the expertise provided by forensics and technology experts. While Canadian courts have yet to be confronted with the issue of expectations of privacy in the dark web,[11] American courts, on the other hand, have developed a rich jurisprudence which

[5] Larry Hardesty, "Shoring up Tor—Researchers mount successful attacks against popular anonymity network—and show how to prevent them," *MIT News* (26 July 2016), online .

[6] *R v Duarte*, [1990] 1 SCR 30, 1990 CarswellOnt 77 *sub nom. R v Sanelli.*

[7] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

[8] *Charter*, *ibid*, s. 2.

[9] See *R v Spencer*, 2014 SCC 43, 2014 CarswellSask 343 at para 1 [*Spencer*].

[10] See e.g., Manitoba which has recently enacted a private sector privacy statute (*Personal Information Protection and Identity Theft Prevention Act,* SM 2013, c 17) and the federal government which enacted Canada's anti-spam legislation, see *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities,* SC 2010, c 23.

helps to raise some useful questioning as to how Canadian courts should handle the matter.

I. MISUNDERSTANDINGS CHARACTERIZING LEGAL PRECEDENTS

It is typical for western justice systems to enlist the services of qualified experts in order to better understand a foreign subject, such as those pertaining to science and forensics. The experts' role is to provide the judge with the necessary information allowing them to make a sound judgement based on expertise, common practice and accepted beliefs. Realistically, judges and lawyers cannot be expected to become computer engineers or experts in the dark web within a few hours. In reality, the knowledge they will have access to depends on the questions asked by the interrogating lawyer and on the perspectives endorsed by the expert questioned. As a result, current jurisprudence is characterized by misconceptions of different orders, and include those pertaining to the functioning of the dark web (e.g. how it manages to protect users' anonymity) and to its impenetrability (e.g. the authorities' capability (or lack thereof) of conducting criminal investigations). This contributes to the erosion of privacy in the dark web.

(a) Functioning

Cyberspace is commonly divided between three "layers". The first is known as "surface web", and refers to the static websites that are typically accessible through mainstream search engines. The second layer, the "deep web" or "invisible web" refers to content that cannot be indexed by search engines. These include online databases such as CanLII or Jstor.[12]

The third layer, the "dark web", is an alternative network in which search engines' crawlers are completely ineffective; hidden websites are listed in directories (e.g. DeepDotWeb, PasteBin, AnonBin) or on dedicated Reddit's threads. The network can only be accessed through special software such as "The Onion Router", "I2P, "Freenet" and "Riffle".[13]

Each software uses different algorithms to guarantee users' privacy. Tor, for instance, is based on military grade encryption, asymmetric encryption and layers of protection ("the Onion technology"). When an information travels through the Tor network, it is stripped of its header (the addressing information about the sender). The header is then encrypted and referred to as "the packet

[11] Though the recent decision *Spencer*, *supra* note 10, established a useful precedent on privacy in cyberspace that is likely to influence future decisions implying the dark web.

[12] Ryan Dube, "Journey Into The Hidden Web: A Guide For New Researchers," *MakeUseOf* (31 October 2014), online: < www.makeuseof.com > .

[13] Jannal Kagel, "An Up-to-Date Layman's Guide to Accessing the Deep Web," *FC Technology* (10 September 2015), online: < www.fastcompany.com > .

wrapper". The encrypted packet is routed through many relays (or servers), in a private networking pathway:

> The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.[14]

In other words, each relay will decrypt and encrypt again the data packet wrapper, hence hiding the message, but also its metadata.

Tor lets users navigate the web anonymously, but also allows the creation and hosting of anonymous websites by hiding the location of the server. Originally created for military and intelligence sharing purposes, Tor has gained popularity with many groups, including criminal organizations, which profit from the anonymity of the network to engage in illicit activities such as prostitution, child pornography and others. Some of these criminals were caught by the authorities using new investigative techniques on the dark web, which are now under legal scrutiny.

In this context, judges have been confronted with the technical aspects of the dark web, such as in the recent motion pertaining to the case of *U.S. v Farrell*,[15] in which the defendant was seeking to obtain more information pertaining to the methods used by law enforcements to discover his identity in the dark web. Specifically, in this affair, US District Judge Richard A. Jones stated that:

> In the instant case, it is the Court's understanding that in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations.[16]

While it is true that nodes are operated by volunteers across the world, these individuals typically do not have access to users' IP addresses. Judge Bryan's position, which was also endorsed in *U.S. v Michaud*,[17] was vehemently criticized by researcher and journalist Joshua Kopstein as factually incorrect:

> This makes no sense to anyone with a basic understanding of how Tor works. Just like with any website or service, Tor users do reveal their IP address to an ISP when initially connecting to the Tor network, through an entry point called a guard node. But since Tor bounces data between random nodes located around the world, neither the ISP nor

[14] The Tor Project, online: < www.torproject.org/about/overview > .

[15] *United States v Farrell*, 2016 WL 705197 [Farrell].

[16] *Ibid.*

[17] *United States v Michaud*, 2016 WL 337263 (W.D. Wash Jan 28, 2016) [*Michaud*].

> anyone intercepting traffic can correlate which IPs are accessing which sites.[18]

The various hearings in *U.S. v Michaud* also demonstrate that judges have trouble seizing the authorities' allegations in regards to the way they investigate throughout the dark web.

The *Michaud* affair concerns the use of a Network Investigative Technique (NIT) by law enforcements to de-anonymize the users of a child pornography site titled "Playpen" located in the dark web. "Operation Pacifier" required the FBI to take control of the website during 13 days in order to inject "[m]alicious scripts into pages hosting images of child abuse, which downloaded the NIT to the visitors' computers and returned the machine information, including their true IP addresses, to the FBI."[19] The operation led to more than 135 arrests,[20] many of which are still in the early stages of legal proceedings.

Judge Bryan refused to dismiss the indictment against Michaud, stating that the FBI's use of mass hacking was not shocking. Nonetheless, the court's hearings shed a bright light on the obvious lack of knowledge on the judge's part:

> Judge Bryan: "Do the FBI experts have any way to look at the NIT information other than going to the server?"
> Colin Fieman (Michaud's public defender): "Your Honor, they don't go to the server."
> JB: "Where do they go? How do they get the information?"
> CF: "They get it from Mr. Michaud's computer."
> JB: "They don't have his computer."[21]

It also appears that, at the time, Judge Bryan was not aware that the NIT is in fact a form of hacking: "I suppose there is somebody sitting in a cubicle somewhere with a keyboard doing this stuff. I don't know that. It may be they seed the clouds, and the clouds rain information. I don't know."[22]

In February 2016, Judge Bryan nonetheless approved the defendant's third request to access the source code of the NIT, though not without noting its own technical incomprehension of the subject matter:

> Now, you know, behind that ruling is this: The government hacked into a whole lot of computers on the strength of a very questionable search

[18] Joshua Kopstein, "Confused judge says you have no expectation of privacy when using Tor," *Motherboard* (1 February 2016), online: <www.motherboard.vice.com>.

[19] *Ibid.*

[20] See Gabrielle Banks, "Federal agents sweep child pornography site by hacking 'dark web' site," *Houston Chronicle* (10 April 2016), online: <www.houstonchronicle.com>; Benjamin Vitaris, "More arrests in the playpen case," *DeepDotWeb* (14 April 2016), online: <www.deepdotweb.com>.

[21] Joseph Cox, "Judge in FBI Hacking Case is Unclear on How FBI Hacking Works," *Motherboard* (27 January 2016), online: <www.motherboard.vice.com> [Cox].

[22] *Ibid.*

> warrant. I ruled on the admissibility of that in what I considered to be a very narrow ruling.
>
> Much of the details of this information is lost on me, I am afraid, the technical parts of it, but it comes down to a simple thing. You say you caught me by the use of a computer hacking, so how do you do it? How do you do it? A fair question.[23]

As journalist and expert Joseph Cox highlights that such confusion relating to the dark web often occurs with relation to the authorities' use of NIT, such as with search warrants:

> [A] problem in some NIT cases is that judges have trouble understanding, even in general terms, what hacking tool is, what they do, or how they work. To be clear, this isn't to place all blame on judges. Instead, it's arguably a problem stemming from how the Department of Justice and the FBI have framed and referred to NITs in legal documents, meaning that some judges may not fully realise the power and scope of the searches that they authorise. [. . .] This confusion, in part, arose from the language used in NIT warrants and supporting documents. The word "hack," is never used, and neither is "malware" or "exploit," for that matter. Instead, the procedure of malware being downloaded to a target's computer is largely obfuscated in vague terminology.[24]

This situation is worrying given that judges and lawyers' discomfort with computer sciences encourage them to rely excessively on either sides' observations and prevents them asking relevant questions. Precisely, as it was the case in *U.S. v Michaud* and *U.S. v Farrell*, it reassures judges to endorse the authorities' investigative methods without much criticism,[25] and at the expense of users' right to privacy and anonymity in the dark web.

(b) Impenetrability

Another misconception relating to the dark web arises from the belief that its veil of anonymity is impenetrable, hence justifying methods of investigation that would otherwise be considered highly invasive or too broad for the purpose of a warrant. This perception is inaccurate, as there remains much vulnerability which can be exploited by law enforcement. They usually classify within two

[23] *Michaud*, *supra* note 18, Defendant's third motion to compel (17 February 2016), court hearing at 18.

[24] Cox, *supra* note 22.

[25] See *United States v Matish*, 193 F.Supp.3d 585 (2016), in which the court finds that the source code of the FBI's NIT is not useful to the defense, while at the same noting that the technicalities should be left to computer experts. This, of course, raises questions as to how the court can affirm that the source code is not useful for the defense if it does not have the expertise to understand it: "The Court FINDS *ex parte* and *in camera* inspection of the exploit unnecessary. Such examination would not have assisted the Court in dealing with the issues before it. The technicalities of such an examination are better left to computer experts" [*Matish*].

sometimes overlapping groups: (i) the vulnerabilities pertaining to human errors and (ii) the vulnerabilities arising from the network itself.

(i) Human errors

A critical aspect of maintaining anonymity in the dark web depends on the user. Tor, for instance, requires precautions and changes in habits from its users.[26] Precisely, it "only protects [. . .] applications that are properly configured to send their Internet traffic through Tor," hence why using another browser than the Tor browser is "likely to be unsafe."[27] This means that users cannot navigate the internet like they usually do, such as by watching videos on YouTube. Torrent file-sharing applications are not safe either, given that they "ignore proxy settings and make direct connections even when they are told to use Tor" and therefore "often send out [users'] real IP address."[28] This is also true of browser plugins like Flash, RealPlayer and QuickTime which can be manipulated in revealing IP addresses.[29]

Users may also reveal their personal information when downloading documents off the dark web and subsequently opening them, because "these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them."[30] In order to safely open downloaded content, users must download Tor-friendly applications such as the PDF viewer built into the Tor Browser.

Another source of vulnerability stems from human error. It includes navigating websites that require a user to login. These include websites like Reddit which are risky because it allows observers to "ti[e] many different behaviors (browsing, posting, and commentating) together," hence providing a "rich supply of information" to identify the user.[31]

There are also many other suggestions that may improve anonymity such as placing duct tape on webcam, enabling computer's firewall, and turning off cookies and JavaScript.[32] It is also noteworthy that, by default, TOR "does not prevent somebody watching your Internet traffic from learning that you're using Tor"[33]. To avoid this, users must set Tor bridge relay — a process which requires

[26] "Q&A: The Deep Web, Anonymity, and Law Enforcement," *Trend Micro* (10 September 2015), online: < www.trendmicro.com > (Interview with Martin Roesler, Senior Director of the Trend Micro Forward-Looking Threat Research (FTR) team).

[27] Tor Project, "Want Tor to really work?", online: < www.torproject.org > [Tor Project].

[28] *Ibid.*

[29] *Ibid.*

[30] *Ibid.*

[31] Andre Infante, "5 ways to stay safe from bad Tor exit nodes," *MakeUseOf* (2 July 2015), online: < www.makeuseof.com > [Infante].

[32] Jennal Kagel, "An Up-To-Date Layman's Guide to Accessing the Deep Web," *FC Technology* (10 September 2015), online: < www.fastcompany.com > .

[33] Tor Project, *supra* note 28.

some familiarity with computer sciences. All of these precautions make the use of Tor challenging for regular users.

In addition to these, individuals using the dark web for criminal purposes are susceptible of the same errors than regular criminals. Chelsea Manning, for instance, notoriously shared how she used the dark web to leak information to Wikileaks with another hacker who subsequently reported her to the authorities and handed over the chat log of the conversation. In fact, traditional methods of investigation such as infiltration and the use of informants remain totally relevant for the authorities, as demonstrated in recent arrests and contrary to what was stated in *United States v Matish*.[34]

In the Marco Polo operation, which was followed by numerous arrests in relation to the drug dealing website Silk Road, the Department of Homeland Security (DHS)[35], was able to conduct an effective operation which started with information given by a source. In order to map the operation, the authorities focused on identifying the top one per cent sellers, the moderators and system administrators as their computers or credentials "could open the door to the site's private communications and account details."[36]

More specifically, an undercover agent who worked on building a relationship with the system administrator, Dread Pirate Roberts, was able to take over Curtis Clark Green's account, accessing "the details of sales transactions and information about the Bitcoin accounts of users and administrators — including the account of Silk Road's alleged owner, Ross Ulbricht"[37] (Dread Pirates Roberts).

Eventually, the authorities managed to arrest Ulbricht:

> After authorities intercepted some fake ID's that they say he ordered online, investigators from HSI visited Ulbricht's home in San Francisco. Ulbricht, agents say, had by then made a number of mistakes that allowed them to tie him to Silk Road, including using the name "altoid" to post messages advertising Silk Road to a forum and then using that same name to post to a Bitcoin forum seeking workers for a Bitcoin startup. In the latter message, "altoid" told would-be job applicants to contact him at rossulbricht@gmail.com. A subpoena to Google provided information about the accountholder. Last July, authorities identified an overseas hosting company used to host the Silk Road site and obtained an image of the server, giving them access to all the private messages on the site. [. . .] They've also revealed that they

[34] *Matish, supra* note 26 at 5.

[35] Kim Zetter, "How the feds took down the Silk Road drug wonderland," *Wired* (18 November 2013), online: < www.wired.com >: A multi-agency task force involving investigators from the FBI, DEA, DHS, the IRS, US Postal Inspection, US Secret Service, the Bureau of Alcohol, Tobacco, Firearms and Explosives was eventually formed, with simultaneous operations launched from Baltimore, New York and Chicago [Zetter].

[36] *Ibid.*

[37] *Ibid.*

> found a logbook on his hard drive and a journal that allegedly detailed his day-to-day activities running the site.[38]

Even though Ulbricht still maintains that the real Dread Pirates Robert has framed him, it remains that law enforcement agencies were able to conduct a successful operation on the dark web largely by exploiting human error as well as using traditional methods.

(ii) Network vulnerabilities

The TOR traffic is, in theory, untraceable between the different nodes within the circuit. However, it becomes visible exiting the Tor network through exit nodes (e.g. when users browse the regular internet with the Tor software).[39] Since volunteers around the world run these, research demonstrates that they are susceptible of being used for snooping on users. Rumors in the industry affirm that "70% or more of the TOR gateways are owned by intelligence services."[40] This affirmation is certainly fueled by the funding of TOR by public institutions such as the Department of Homeland Security, but it is likely to be exaggerated.

However, few researches demonstrated how exit nodes may be corrupted for surveillance purposes or to access personal information. In 2015, a security researcher set up a fake website with a Bitcoin theme (a honeypot or honion) and noted "over 600 unexplained page visits, 12 failed log-in attempts and 16 successful ones that hadn't come from [the researcher]."[41] Precisely, out "of about 1400 exit nodes, 16 attempted to seal the password and log in."[42] These numbers are only indicative, keeping in mind that "the trap can only catch the snoopers who are watching, interested in the bait and willing to act on it quickly" thus, "[a]ny snoopers (or snooping software) that didn't want to break cover for a quick Bitcoin would have gone undetected."[43]

In the same line of thought, another researcher was able to use the five Tor exit nodes he set up to intercept "thousands of private emails, instant messages

[38] *Ibid.*

[39] Tor Project, *supra* note 28: "Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include https:// in the URL, and display the proper expected name for the website."

[40] *Supra* note 27.

[41] Mark Stockley, "Can you trust Tor's exit nodes?," *Naked Security* (25 June 2015), online: <www.nakedsecurity.sophos.com> [Stockley].

[42] Infante, *supra* note 32.

[43] Stockley, *supra* note 42. This is even more dramatic that the researcher reported that "Tor's semi-centralized system for purging bad nodes has totally failed to take action against the bad nodes she did identify — they are still operating, and, presumably, still snooping" (original research online: <www.chloe.re/2015/06/20/a-month-with-badonions>).

and email account credentials" from victims that included international embassies, the Indian Ministry of Defense and the Dalai Lama's liaison office. He concluded "that governments were funding expensive, high bandwidth exit nodes for exactly that purpose."[44] Of course, what these researches also demonstrate is that users misunderstand Tor and use it as an end-to-end encryption tool, which it is clearly not.

Researcher Sambuddho Chakravarty of Columbia University was also able to literally crack Tor and identify users with 81.5 per cent accuracy in real-world tests. This is because the research community "knows no practical low-latency design that can reliably stop the attacker from correlating volume and timing information on two sides."[45] This means that "if you visit a fake site that's rigged with, say, illegal drugs or child porn or something and download a relatively large file from it (around 100 MB, he suggests), your identity can be discovered, 81 percent of the time."[46] In fact, another researcher discovered exit nodes located in Russia that were "actively patching binaries users download, adding malware to the files dynamically."[47]

In 2016, other researchers also discovered hundreds of malicious hidden service directories (HSDirs) which are used by users to access hidden websites:

> When set up properly, these directories don't record or log the addresses of the services themselves, allowing the dark web sites to, hopefully, remain undiscovered. But sometimes people deliberately modify their HSDir to keep a record of all the sites it spots.[48]

By setting up honeypots in the Tor network, Guevara Noubir, a professor from the College of Computer and Information Science at Northeastern University, and Amirali Sanatinia, a PhD candidate also from Northeastern, discovered an armada of Tor hidden service directories that are spying on dark web sites. These modified nodes allow whoever is behind them — perhaps law enforcement, hackers or other researchers — to find the addresses of sites that are supposed to be secret.[49]

Most recently, researches by computer scientists at the MIT and the Qatar Computer Research Institute demonstrated that by taking over a guard node, they could identify with 88 per cent accuracy which websites users are accessing.[50]

[44] *Ibid.*

[45] Sambuddho Chakravarty et al., "On the effectiveness of traffic analysis against anonymity networks using flow records," online: Columbia University .

[46] Jason Koebler, "How the NSA (or anyone else) can crack Tor's anonymity," *Motherboard* (19 November 2014), online: < www.motherboard.vice.com > .

[47] See Dennis Fisher, "Researcher finds Tor exit node adding malware to binaries," *Threat Post* (24 October 2014), online: < www.threatpost.com > .

[48] Joseph Cox, "Over 100 snooping Tor nodes have been spying on Dark Web sites," *Motherboard* (1 July 2016), online: < www.motherboard.vice.com > .

[49] *Ibid.*

Reporting these vulnerabilities in the Tor network has led to technical improvements, but it has also prompted computer scientists to come up with an alternative proposition. At the Privacy Enhancing Technologies Symposium in July, researchers at MIT's Computer Science and Artificial Intelligence Laboratory and the École Polytechnique Fédérale de Lausanne presented 'Riffle', a new anonymity scheme which combines current cryptographic methods in a novel manner.[51]

Both human error and technical vulnerability in the dark web are windows that may be exploited by law enforcement to conduct effective and successful criminal investigations; yet, judges are often unaware that authorities may have a choice. This is likely to prompt them to accept warrants which are broader than necessary and endorse methods of investigation which are more intrusive than required. The redaction of obscure applications for warrants does nothing but contribute to a myth that prevents jurists to have an informed debate regarding acceptable searches and seizures in the digital age.

II. IMPACTS OF THE DARK WEB ON PRIVACY AND OTHER CONSTITUTIONAL GUARANTEES

(a) Analysis of an emerging trend

In the United States, legal cases pertaining to both operations Marco Polo and Pacifier have resulted in a legal trend granting **no reasonable expectations of privacy to users of Tor**. This was explicit in *Michaud*, where Judge Bryan based his opinion on an erroneous premise which presupposes that users had to share their IP with strangers to connect with the network:

> Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers. Again, according to the parties' submissions, such a submission is made despite the understanding communicated by the Tor Project that the Tor network has vulnerabilities and that users might not remain anonymous. Under these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network. In other words, they are taking a significant gamble on any real expectation of privacy under these circumstances.[52]

[50] See Mary-Ann Russon, "MIT cracks Tor anonymity network and identifies hidden servers with 88% accuracy," *International Business Times* (30 July 2015), online: < www.ibtimes.co.uk >.

[51] Larry Hardesty, "Network can protect users' anonymity if all but one of its servers are compromised," *MIT News* (11 July 2016), online: . "The heart of the system is a series of servers called a mixnet. Each server permutes the order in which it receives messages before passing them on to the next. [. . .] Like many anonymity systems, Riffle also uses a technique known as onion encryption. [. . .] To thwart message tampering, Riffle uses a technique called a verifiable shuffle [. . .] the encryption can be done in such a way that the server can generate a mathematical proof that the messages it sends are valid manipulations of the ones it receives."

[52] *Farrell, supra* note 16.

In Judge Bryan's view, IP addresses fall under the third party doctrine according to which there is no expectation of privacy when an information is transmitted to a third party, even unwittingly.[53] This view was the one advanced by the American Department of Justice in his counter-argument recently unsealed. Both the judge and prosecutors "suggest that Michaud voluntarily gave up his true IP address even while using Tor, because his IP could have been correlated with his anonymized connection to the hidden site by 'other means', which they don't specify."[54]

Recent cases have also exposed some of the methods which the law authorities have used in order to investigate in the dark web. As previously discussed, these include traditional ones such as infiltration, but also less-traditional one, such as mass-hacking through drive-by downloads, man-in-the-middle attacks or by corrupting nodes. Many accused have subsequently argued that they are unable to fairly defend themselves in trial without access to the complete source code of the NIT for an expertise of how the software affects computers' security settings.[55]

Other debatable methods have included a subpoena to computer scientists funded by the federal government to research the dark web at Carnegie Mellon University. The subpoena forced the team to hand over the IP addresses it obtained through their academic work.[56] This permitted the authorities to access at least 78 IP addresses, including the one of Brian Richard Farrell, Silk Road 2's administrator. Commentators argued that this was not only unethical, but also contrary to the Fourth Amendment because it constituted a way to bypass the requirement to obtain a warrant in order to breach users' privacy.[57]

(b) Canadian jurisprudence and the future of privacy in the dark web

There are major legal differences between American and Canadian jurisdictions. It is useful to note that in the United States, once an e-mail or a message has been received, it is no longer protected through privacy concerns.[58]

[53] See *Smith v Maryland*, 442 US 735; 99 S Ct 2577 (1979). The judge found that telephone users do not have an interest in the phone numbers that they dial, as the phone company has access to them.

[54] Joshua Kopstein, "Justice Department to Judge: Tor users have no expectations of privacy," *Motherboard* (6 February 2016), online: < www.motherboard.vice.com > [Kopstein].

[55] See *United States v Werdene*, No. 2:15-cr-00434, ECF No 33 (E.D. Pa. 18 May 2016); *United States v Levin*, No. 15-10271, 2016 WL 2596010 (D. Mass May 5, 2016); *United States v Arterbury*, No. 15-cr-182, ECF No. 47 (N.D. Okla., 25 Apr. 2016); *United States v Epich*, No. 15-cr-163, 2016 WL 953269 (E.D. Wis., 14 Mar. 2016); *United States v Stamper*, No. 1:15-cr-109, ECF No. 48 (S.D. Ohio, 19 Feb. 2016); *Michaud, supra* note 18.

[56] Joseph Cox, "Confirmed: Carnegie Mellon University attacked Tor, was subpoenaed by Feds," *Motherboard* (24 February 2016), online: < www.motherboard.vice.com > .

[57] Tor, "Did the FBI Pay a University to Attack Tor Users?c (11 November 2015), online: *Tor* (blog) < blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users > .

This is not true in Canada, where British Columbia's Court of Appeal has established that a sender has reasonable expectation of privacy concerning the fact that his message will be received in confidentiality.[59] This is definitely a factor which may influence the development of a Canadian legal perspective on the dark web.

R v Spencer, a recent decision by the Supreme Court of Canada, has also paved the way for a broader understanding of privacy which may also protect users in the dark web while addressing some of the main critics of *Michaud*, among which a neglect of users' intentions while using a software specifically designed for anonymity:

> But this ignores the fact that people use Tor specifically because they don't want to use the internet "normally," they want to use the internet anonymously. It's true that, like with any website or service, you expose your real IP address to an ISP when connecting to the Tor network. But that network is purposefully designed to bounce data around the globe so that you don't reveal your IP to the site you're connecting to.[60]

Spencer revolves around the police's decision to make a written "law enforcement request" to Shaw demanding the name, address and phone numbers of the customer using an IP address that was involved in the sharing of child pornography. They further used this information to obtain a warrant and search the accused's phone. The defense contended that the police obtaining the subscriber information matching the IP address constituted a search and should have been authorized by a warrant. To answer this question, the court first had to determine whether the accused had an expectation of privacy regarding the information provided by the internet provider to the police.

This is determined by taking into consideration "the totality of the circumstances," including "interrelated factors."[61] For the purpose of the dark web, it is interesting to note how the court underlines that the accused's "subjective expectation of privacy in his online activities can readily be inferred from his use of the network connection to transmit sensitive information: *Cole,* at

[58] See *United States v Lifshitz*, 369 F. 3d 137 (2d Cir. 2004) with some exceptions when the legal duty of confidentiality is involved, see e.g. *United States v Knoll*, 16 F. 3d 1313 at 1321 (2d Cir. 1994).

[59] *R v Pelucco*, 2015 BCCA 370, 2015 CarswellBC 2386, 327 C.C.C. (3d) 151.

[60] Kopstein, *supra* note 55.

[61] *Spencer, supra* note 10 at para 17. These factors were described at the following paragraph: "[18] The wide variety and number of factors that may be considered in assessing the reasonable expectation of privacy "can be grouped under four main headings for analytical convenience: (1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances: Tessling, at para. 32; *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579, at para. 27; *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34, at para. 40."

para 43."[62] Most importantly, ruled to broaden the traditional view of informational privacy as "confidentiality and control of the use of intimate information about oneself" to a view that "account[s] for the role that anonymity plays in protecting privacy interests online":[63]

> [38] To return to informational privacy, it seems to me that privacy in relation to information includes at least three conceptually distinct although overlapping understandings of what privacy is. These are privacy as secrecy, privacy as control and privacy as anonymity.
> [. . .]
> [41] [. . .] In my view, the concept of privacy potentially protected by s. 8 must include this understanding of privacy.[64]

R v Spencer is the first recognition of anonymity as a protected right by the Supreme Court of Canada, which further states its importance in the precise context of internet which "increased both the quality and quantity of information that is stored."[65] The court finally stresses that "the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information"[66] and finally concludes that "there is a reasonable expectation of privacy in the subscriber information."[67] The significance of this case is that Canadian law enforcement *must* obtain warrants to connect IP addresses with personal information, while it is currently not the case in the United States.

Building from *R v Spencer*, Canadian judges are likely to avoid many of the pitfalls characterizing American legal precedents. The judicial community also has a great starting point to engage in an informed debate about the methods of investigation that they judge acceptable and the expectation of privacy users should expect with anonymity tool. The risks of overly broad and obscure warrants pertaining to questionable methods of investigation should not be discarded too easily, and the necessity to guarantee a fair trial to accused should motivate a reflection on how privacy and security can be balanced in a manner which reflects the realities of the dark web rather than common myths.

[62] *Ibid* at para 19.

[63] *Ibid* at para 34.

[64] *Ibid* at paras 38, 41.

[65] *Ibid* at para 46.

[66] *Ibid* at para 47.

[67] *Ibid* at para 66.