itworldcanada.com

Understanding Canadian cybersecurity laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)

Melissa Lukings and Arash Habibi Lashkari

31-40 minutes

The rapid growth of encryption technology has revolutionized the online marketplace and helped to enable the creation of anonymous online networks, like the Dark Net — a hidden forum for which has attracted individuals who wish to engage in criminal activities while remaining anonymous and untraceable. Cybercriminal activity, unlike typical localized or neighbourhood crimes, is not confined by national or provincial borders or limited by physical geography. The fairly recent creation and development of cryptocurrencies, through the Dark Net, has created the possibility of full transactional anonymity for those involved in criminal activities both on- and offline. For the most part, crime hidden on the Dark Web (accessed via the Dark Net) or committing using the Dark Net is not a novel crime; it is an established crime the commission of which is being facilitated through the use of anonymous encrypted networks. Rather than

being a unique section of the Canadian criminal law, the Dark Web merely acts as a different forum for activities that were already criminalized outside of the context of the Dark Web. The difficulty in creating laws to regulate Dark Web/Dark Net activity arises from the dual issues of detection/tracing and legal jurisdiction within an essentially-unlimited and fully anonymous global encrypted network.

In our past articles, we have discussed the foundations of Canadian data privacy laws and the specific legislation which applies to governments and commercial enterprises in relation to cybersecurity and privacy protection. We have considered how Canadian privacy laws and regulations apply to governments, corporations, organizations. We have considered some small-scale peer-to-peer cyber-specific criminal activities and privacy intrusions involving the large-scale distribution of intimate images. Links to our previous articles in the Understanding Canadian Cybersecurity Laws series can be found here:

- **Understanding Canadian Cybersecurity Laws: The Foundations (Article 1)**
- **Understanding Canadian Cybersecurity Laws: Privacy and Access to Information — the Acts (Article 2)**
- **Understanding Canadian Cybersecurity Laws: Privacy Protection in the Modern Marketplace — PIPEDA (Article 3)**
- **Understanding Canadian Cybersecurity Laws: Interpersonal Privacy and Cybercrime — Criminal Code of Canada (Article 4)**
- **Understanding Canadian Cybersecurity Laws: "Insert Something Clever Here" — Canada's Anti-Spam Legislation**

[(Article 5)]

- [Understanding Canadian Cybersecurity Laws: Peer-to-Peer Privacy Protection — “Intrusion Upon Seclusion” and the Protection of Intimate Images (Article 6)]

In this article, we will discuss the legal issues relating to encrypted online criminal activities, specifically those involving or facilitated by the use of Dark Web browsers and cryptocurrencies (such as TOR and Bitcoin, respectively) which provide anonymity to both parties in an illegal transaction. Cybercriminal activity is not confined by national borders or limited by geography so the main legal issues which stem from hidden online criminal activities are the inherent difficulties of detection/tracing on encrypted networks and the legal puzzle of navigating jurisdictional authority and balancing foreign and domestic relations, treaties between nations, and potentially conflicting interests on the international stage.

In law, the term **“jurisdiction”** refers to the practical authority to administer justice which is granted to a legal body based on the type and locational circumstances of the case. In more casual terms, “jurisdiction” can also refer to a specific geographic area, however, when we consider online activities, there is not necessarily a defined geographic area to distinguish which authority has the legal jurisdiction over that medium. In Canada, legal jurisdictional divisions are considered locally, provincially, and federally. It can also refer to the powers of the executive and legislative branches of government to analyze and allocate resources to promote and serve the best interests of the people who are governed within that jurisdiction. To better understand how legal jurisdiction applies to encrypted online criminal activities,

it is necessary to consider the context and nature of the Deep Web and the Dark Web/Dark Net.

Differentiating the dark web from the deep web

We have previously discussed the distinction between cyber-dependent, cyber-enabled, and computer-supported crimes. To refresh: **"cyber-dependent crimes"** are crimes which can only be committed using a computer, a computer network, or other technology; **"cyber-enabled crimes"** are those which can be committed without the use of technology, but are increased in their scale or reach by the use of a computer, network, or other technology; and **"computer-supported crimes"** are those in which the use of the computer or network is only incidental to the actual commission of the crime. The Dark Web is the medium in which these three classifications of cybercrime all converge. But first: definitions.

A **"net"** refers to a network that includes several computers, servers, and connectors (e.g. a switch, hub, router, etc.). The network of computers can be either Intra-net or Inter-net. **"Intra-net"** is a private network such as your home network, a company or university network, or any other private network. An Intra-net is naturally private until the user makes it public. At that point the now-public Intra-net connects to other Intra-nets within the larger Inter-net. The **"Inter-net"** (or "internet") is the larger network of all of these Intra-nets when they are made publicly available.

A **"web-page"** is a page in a publicly available server, called a **"web-server"**, which contains data and information. Combining

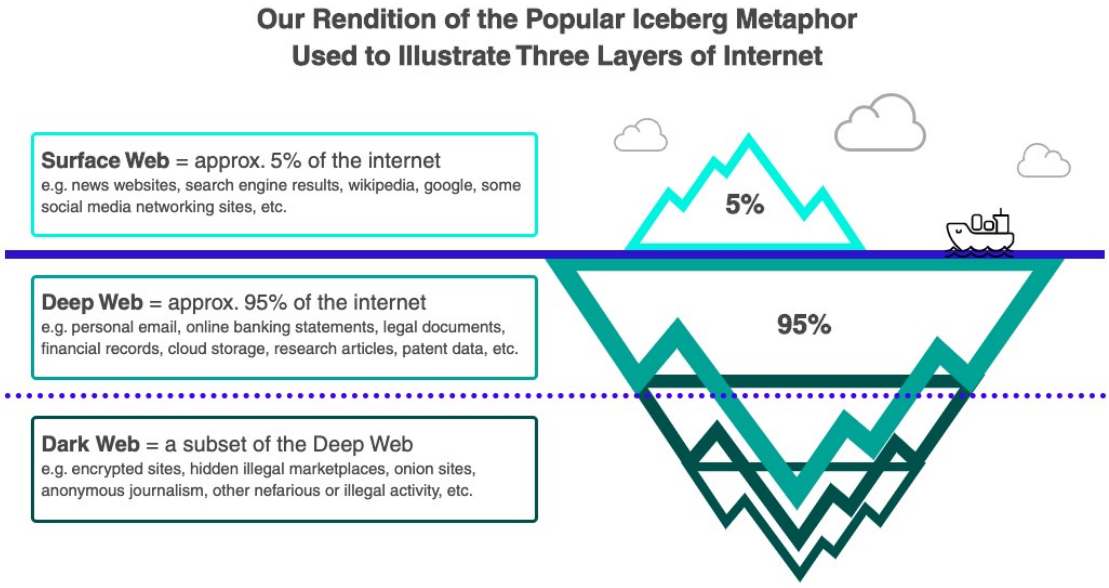
several web-pages together creates a **“web-site”**. Thus, a **“web”** is a collection of web-sites which could be legal or illegal. When you pay for your internet connection through your **“Internet Service Provider”** (or **“ISP”**), the ISP gives you the ability to connect to the public Inter-net through their Intra-net.

Depending on the level or lack of accessibility, the type of web being accessed falls within one of the layered categories of the internet: **Surface Web**, **Deep Web**, and **Dark Web**. To browse the Surface Web-sites in the Internet-Web (WWW) you need to use a browser like Firefox, Chrome, Safari, or Internet Explorer. To access the Dark Web, you need to use an anonymous encrypted browser like The Onion Router (called **“TOR”**).

The **“Surface Web”** (or “Clear Web”) refers to your standard internet browsing experience. The Surface Web includes indexed websites which are accessible through traditional search engines and internet browsers. Anything that you can find through a simple keyword search is considered to be Surface Web content and can be accessed through a typical internet connection. Examples of Surface Web sites include Google, Reddit, Facebook, Yahoo, Wikipedia, and many news sites.

The **“Deep Web”** and **“Deep Net”** refer to the content and internet websites that exist and can be accessed on an encrypted network through the use of a password or other login credential. It includes all unindexed sites; those which are not publicly accessible through a standard internet search on a typical internet browser. In most cases, these unindexed sites are not accessible because they are password-protected, encrypted, or require a login to gain access. Network administrators can connect to the Deep Web using the Deep Net when they have the username and password

and use the assigned IPs.



Click to enlarge.

The creation of the Deep Web in the 1970s was originally intended to protect and isolate networks from the Advanced Research Projects Agency Network and to hide the locations and IP addresses of US military operations for security purposes. Much of the content on the Deep Web comprises academic resources, patent information and large scale databases which are maintained by universities, governmental organizations, and other institutions. Examples of Deep Web content include online banking, personal email accounts, libraries, user databases, members-only sites, and other similar content which requires a password, login, or specific credential in order to gain access.

The **"Dark Web"** is the part of the greater unindexed Deep Web which is both encrypted and anonymized, thus making it an attractive medium of communicating and transacting for the purpose of engaging in illegal activities. Reported illegal Dark Web activities include: illegal file sharing; intellectual property theft; drug and weapons dealing; trading in other illegal goods or criminalized

services; human trafficking; accessing, creating and distributing child pornography; and, allegedly, a myriad of just about anything else you could imagine.

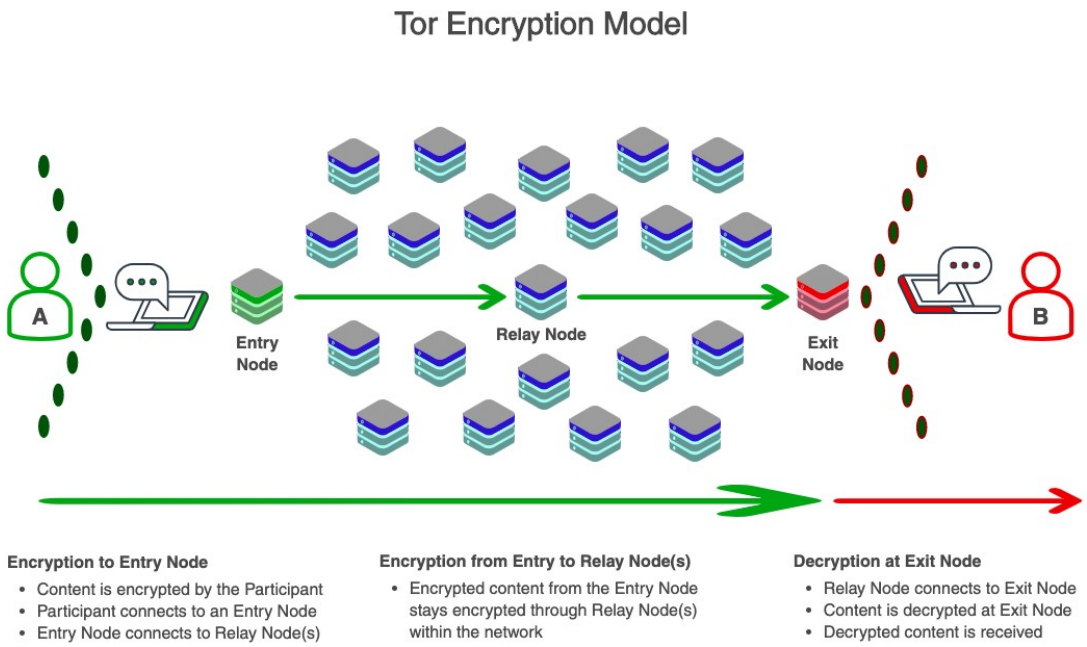
In recent years, illegal Dark Web marketplaces have acted as a catalyst for the development of cryptocurrencies because online exchanges which are completed using cryptocurrency protect the identity of both the buyer and the seller in the transactions, which can be highly desirable for both parties. The anonymity of cryptocurrency also helps in preventing the build up of a “paper trail” of traceable evidence from being created while engaged in illegal activities. Without clear, definitive, traceable evidence to tie an individual or group to a crime, the anonymized Dark Web enables people who are engaging in online criminal activities to better evade detection and identification by law enforcement.

The **“Dark Net”** refers to the unused address space of the internet which is not speculated to interact with other computers in the world. It is “Dark” because of its inherently anonymous nature, virtual marketplace, and use of cryptocurrency. The Dark Web could be accessible through the Dark Net, beyond the reach of the World Wide Web search engines.

The Dark Net is a network of IPs that attackers can use as a medium for illegal activities, such as connecting to the Dark Web to access illegal content without detection and identification or to execute large scale cyber-attack scenarios with 100% anonymity. As an example, potential cyber-attacker could use thousands of unassigned IPs in the Dark Net to prepare a DDoS attack on a large organization knowing that no one will be able to trace the attack back to them.

Together, the Dark Web and Dark Net provide anonymous and encrypted access to hidden and potentially illegal, web content within the larger Deep Web.

“TOR” or **“The Onion Router”** is a commonly-used encrypted browser which can be used to connect the user to the Dark Net and allow access to the Dark Web. The TOR model uses encryption from the user point of contact to the Entry Node, through an unknown Relay Node, to an Exit Node, where it is then decrypted at the receiving end. The onion is used as a metaphor as it compares peeling back each layer of encryption to peeling off the layers of protective outer skin on an onion.



Click to enlarge.

Deep dark legal questions, simplified

While some tech-savvy internet users prefer the encrypted browsing option to guarantee their privacy and anonymity and/or to prevent tracking or monitoring software from collecting data about their online activities and behaviours, many other internet users

are unfamiliar with browsers like TOR and so are unsure of the legal implications of using such a browser. We have created a list of commonly asked questions about the law and the Dark Web to try to answer the easiest questions in the most straightforward way.

- **Question One: Is the Dark Web illegal?**

  No.

  — The Dark Web itself is not illegal. While there are many websites within the Dark Web that specialize in illegal products, marketplaces, activities, or services, for the most part the content on the Dark Web is not illegal. That said, using the Dark Web or Dark Net to engage in criminal activities would absolutely be illegal, however it would be the activity itself that is criminalized; not the Dark Web as a medium.

- **Question Two: Is it illegal for me to access the Dark Web?**

  No, but…

  — The act of simply accessing the Deep or Dark Web is not a criminal offence in Canada. However, an offence of illegally accessing private data in a Deep Web network for which you are not authorized to have access (e.g. hacking, intrusion upon seclusion, privacy breach) could be considered a offence under Canadian laws which we have discussed in previous articles.

- **Question Three: Is it illegal to use an encrypted browser (e.g. TOR) to explore the Dark Web?**

  No.

  — It is not illegal to use an encrypted browser, like TOR, to explore the Dark Web. It is not uncommon for internet users who are

concerned about monitoring and tracing (e.g. journalists, researchers, and patent owners) to use encrypted web browsers to anonymously and confidentially communicate without jeopardizing their personal safety, security, or personal private data. That said, it is illegal to use an encrypted browser to commit a criminal offence. The browser itself is not illegal, but using it as a tool for illegal activities could be a crime.

- **Question Four: Is the Dark Web/Dark Net actively monitored by Canadian law enforcement?**

  Yes, sort of…

  — Canadian law enforcement does try to monitor Dark Web content and activity, however there is no currently available law enforcement software (based on our Surface Web search) that can adequately detect and monitor illegal access, communications, activities, and encrypted content transmitted over the Dark Web.

- **Question Five: Does law enforcement care about the Dark Web/Dark Net?**

  Yes.

  — Law enforcement would like to be able to detect and trace criminal activities done over the Dark Web. Some of the most commonly highlighted goals of law enforcement with regard to the Dark Web are to prevent child pornography, to shutdown illegal marketplaces which provide a forum for exchanging goods or services for (usually) cryptocurrencies, and to combat the problem of global and domestic human trafficking facilitated over encrypted networks.

- **Question Six: Can I get into legal trouble by accessing the**

Dark Web/Dark Net?

Maybe.

— While simply accessing the Dark Web is not a criminal offence, there is a possibility that you will stumble upon sites which host illegal marketplaces for purchasing drugs, weapons, other illegal goods, as well as child pornography, snuff porn, criminals for hire, and human trafficking. If you were to engage with one of these illegal sites and break a law under the Criminal Code of Canada, then you could be charged with a crime and end up in legal trouble.

- **Question Seven: Do I have legal responsibilities on the Deep Web and the Dark Web/Dark Net?**

  Yes.

  — Your responsibilities on the Deep Web and Dark Web are the same as those on the Surface Web, which are similar to the legal responsibilities you have when you are offline, or IRL. As would be the case in other mediums, here are some examples of individual responsibilities with regard to creating and controlling content on the internet:

- If you create or exercise control over content on the internet then you may be responsible for any damage caused by that content.
- If you have control over content which you learn is infringing upon a law or the individual rights of another person and you choose to do-nothing about it then you may be liable for your inaction.
- If you intentionally or knowingly infringe upon the rights of another person then you may be liable for any damages caused as a result.

- If you use the Deep Web/Deep Net or Dark Web/Dark Net to commit an act elsewhere that is illegal in Canada, you may still be held accountable and legally responsible under the Canadian law.
- If you develop or create illegal content in Canada, even if that content is subsequently made available only from a server located outside of Canada, you may still be held criminally responsible.
- If you commit a criminal offence, regardless of whether it takes place on- or offline, then you can be charged for that criminal offence and be held legally responsible.

  The Deep/Dark Web is not a separate or distinct legal realm, but merely an alternative medium for communicating and interacting remotely with others. Criminal activities are illegal regardless of whether they take place in person, at a distance, remotely, or through the use of technology. If you commit a crime then you can be charged for that crime.

Challenges in applying the law

The Dark Web/Dark Net are “dark” because they are hidden. Sites and content on the Dark Web cannot be indexed by a crawling web browser like Google. The IPs on the Dark Net are not assigned to any user, they are anonymous. This makes it definitively difficult for law enforcement to find and access specific Dark Web/Dark Net websites and connection methods, to detect and monitor illegal activities, to trace and localize the source of the illegal activities, and to enforce the applicable Canadian criminal laws on the involved parties.

For example, over two million people per day use TOR to access the Dark Web, but we do not yet have a highly accurate solution to

detect the content and behaviours in the users' activities on TOR. In 2014, He Gaofeng and his team from the China Electronic Power Resource proposed an idea which would detect the Browsing, File Transfer and P2P Connection activities in TOR traffic within 600 seconds. Later in 2016, Dr Lashkari and his team from the University of New Brunswick (UNB) proposed a highly accurate solution using network traffic analysis to detect and characterize user behaviours on TOR and VPN within ten seconds.

Few currently-available solutions have coverage which is sophisticated enough to be truly effective at detecting, monitoring, characterizing, and tracing of TOR-based activity. As a result, there is a lot of fear, uncertainty, and doubt concerning the effectiveness of cybersecurity laws in this complex, rapidly-evolving arena. As research in this field continues, there are likely to be novel solutions proposed to deal with criminal activity on the Dark Web. As recently as 2020, Dr Lashkari and his team have proposed a new solution using image processing and AI, called "Deep Image DarkNet" (or "DIDarknet") to detect and characterize user activities. So far these activities include detection and characterization for browsing, chat, email communication, file transfers, streaming, VoIP and P2P, and can already be applied to over eighteen representative applications, including Facebook, Skype, Spotify, and Gmail.

Illegal online marketplaces and jurisdictional considerations

The most popular illegal Dark Web marketplace, called the "Silk Road", was designed to use TOR for user anonymity and Bitcoin

as a similarly-anonymous transactional currency. Silk Road was created and operated by Ross William Ulbricht from 2011 until his arrest in 2013. As Ulbricht is an American citizen and the arrest took place in the United States, he was indicted under the American criminal justice system for a total of seven offences including: conspiracy to launder money, conspiracy to commit computer hacking, conspiracy to traffic narcotics by the means of the internet, and continuing a criminal enterprise. In May 2015, Ross Ulbricht was sentenced to a double life sentence plus forty years without the possibility of parole and was ordered to pay over $180-million (USD) in fines. Pretty much as soon as the government shut down Ulbricht's Silk Road, another individual quickly launched a Silk Road 2.0 and was promptly charged with the same crimes as Ross Ulbricht for his original Silk Road enterprise.

While these Silk Road cases were simplified because the United States had the legal jurisdiction, the often international and cross-jurisdictional nature of the Dark Web makes it essential for criminal investigators to be able to collaborate across law enforcement agencies and without the limitation of borders if our goal is to regulate or enforce law on the Dark Web/Dark Net.

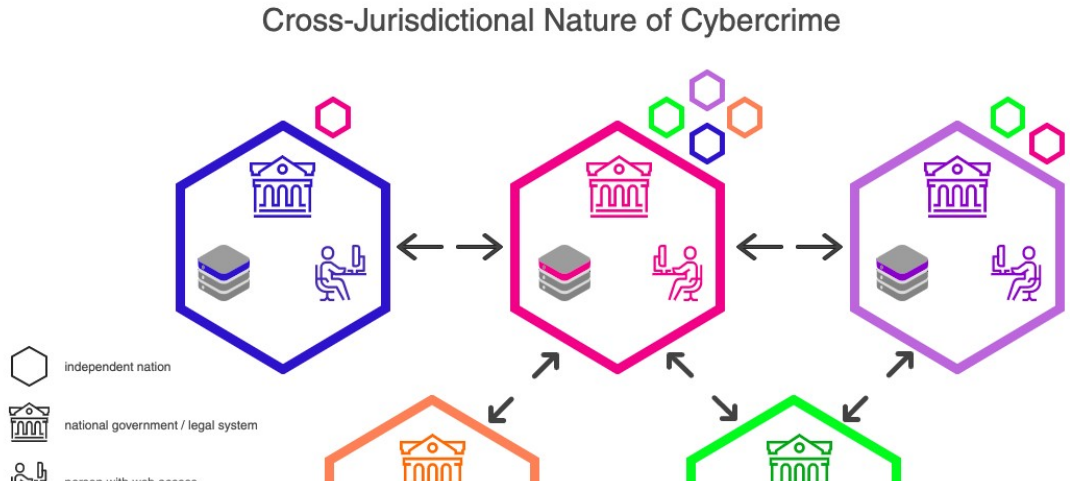
Unlike visible criminal activity on the street, the anonymous nature of the Dark Web/Dark Net makes it challenging for law enforcement to immediately know when a law is being broken or harm is being done. When law enforcement has been notified of illegal transaction, the use of a decentralized network for confirmation and verification of Dark Net transactions, limits the ability of law enforcement to localize an offence to a specific jurisdiction, even when there is very clearly a law being broken

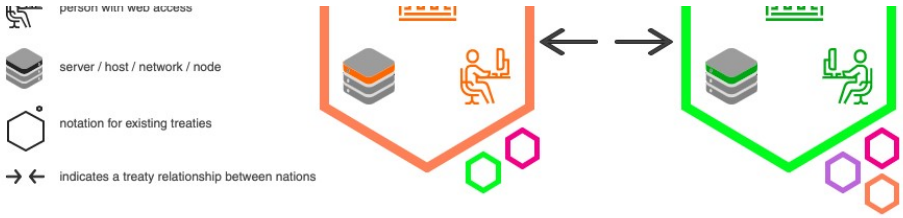
somewhere by someone. Compounding this issue is the inherent cross-jurisdictional and international nature of the Dark Web/Dark Net, which can be hindered by testy international relations, unsigned treaties, and conflicting interests between jurisdictional parties and law enforcement organizations.

When considering cross-jurisdictional criminal activities we must consider whether there are any pre-existing relations between the two (or more) jurisdictions involved, and if so, what the responsibilities of each nation party has within that treaty agreement. As a fun example, if we consider the illustration below, we can see how establishing legal jurisdiction over a specific criminal instance may be additionally complicatedly the cross-jurisdictional nature of cybercrime in the following scenarios below.

Hypothetical One:

Blue Government of Blue Nation detects criminal activity coming from Blue Person within Blue Nation and being received by Pink Person in Pink Nation. Blue Government and Pink Government have a treaty agreement which states that each Nation must inform the other when cross-jurisdictional criminal activity is detected online. Blue Nation informs Pink Nation. Blue Nation and Pink Nation work together. This is the simplest example.





Click to enlarge.

Hypothetical Two:

Blue Government detects criminal activity coming from Blue Person in Blue Nation and being received by Purple Person in Purple Nation. Blue Government and Purple Government do not have a treaty agreement.

- Does Blue Nation have an obligation to inform Purple Nation?
- Does Blue Government have the jurisdictional authority to intervene in Purple Nation for a crime which originated in Blue Nation?

Hypothetical Three:

Blue Government detects criminal activity coming from Purple Person in Purple Nation and being received by Purple Person in Purple Nation. Blue Nation does not have any tie to the criminal activity other than having detected it. Blue Nation and Purple Nation do not have a treaty agreement.

- Does Blue Nation have an obligation to inform Purple Nation?

Hypothetical Four:

Blue Government detects criminal activity coming from Blue Person in Pink Nation and being received by Purple Person in Purple Nation. Pink Government has individual treaty agreements with both Blue Government and Purple Government which state that each Nation must inform the other when cross-jurisdictional

criminal activity is detected online. Blue Government and Purple Government do not have a treaty agreement.

- We know that Blue Nation must inform Pink Nation. Does Blue Nation also have an obligation to inform Purple Nation?
- We know that Pink Government has a treaty with both Blue Government and Purple Government and is aware that there is no existing treaty relationship between Blue Government and Purple Government. Does Pink Nation have an obligation to inform Purple Nation about criminal activity detected between Pink Nation and Purple Nation if that activity was detected and shared to Pink Nation by Blue Nation?
- Does Blue Nation have the jurisdictional authority to intervene in Purple Nation for a crime which originated with Blue Person in Pink Nation?

Hypothetical Five:

Blue Nation and Green Nation have vastly different laws. What is criminalized in Green Nation is not always criminalized in Blue Nation. Purple Government detects criminal activity coming from Green Person in Pink Nation and being received by Purple Person with Blue Server in Blue Nation. The nature of this particular activity is not illegal in Blue Nation.

Purple Government, who detected the activity, has treaties with Pink Government and Green Government which state that each Nation must inform the other when cross-jurisdictional criminal activity is detected online. Green Government has similar treaties with Purple Government, Pink Government, and Orange Government, but not with Blue Government.

Pink Government has treaties with Blue Government, Green Government, Purple Government, and Orange Government.

Blue Government only has a treaty with Pink Government.

- Who has jurisdictional authority?
- Which Nation has the obligation to inform which other Nation(s)?
- Does it matter if the activity is not illegal in Blue Nation?

Cross-jurisdictional considerations add a level of complexity to the issue of detecting, informing, and enforcing laws on encrypted global networks. Where a localized crime may be easy to assign within a legal jurisdiction, where an online crime may pass through multiple jurisdictions can be substantially more complicated.

Corporate and legislative considerations

The increasing use of the encryption technology and the Dark Web as a platform for intellectual property infringement as well as commercial and other crime requires governments, businesses, and individuals to be mindful of any current and future potential impact of Dark Web activity in relation to their interests. Often, when private corporate records obtained in data breaches are published and offered for sale, the forum used to leak this stolen data involves the use of the Dark Web/Dark Net.

The Ashley Madison Agency (“Ashley Madison”) is a Canadian online dating service and social networking service which is marketed to people who are married or in relationships. It was founded in 2002 by Darren Morgenstern, with the slogan “Life is short. Have an affair”. On July 15, 2015, the Ashley Madison site was hacked by a group called The Impact Team. This group

claimed that Ashley Madison cybersecurity had always been weak and claimed to have stolen personal information from Ashley Madison's user database, threatening to release names, home addresses, search histories, and personal member credit card numbers if the site was not immediately shut down.

As threatened, the first mass user data release of over 60GB of user information occurred on August 18, 2015 and was later validated by cybersecurity experts. The second successful breach came on August 21, 2015, when the emails of Avid Life Media CEO Noel Biderman were made available in a 19GB online file. Some Ashley Madison users reported receiving extortion mails and requesting payment in Bitcoin to prevent the public release of their personal information and the release of all of their Ashley Madison user account information to their significant other. By August 24, 2015, the Toronto Police Department indicated reports of suicide and many extortion attempts associated with the leak of individual user-profiles and offered a reward of $500,000 CAD for information leading to the arrest of the hackers.

The method of the data leak involved the hacking of the company data, the release of that information on BitTorrent in a compressed archive with the link posted on a Dark website which was accessible through TOR. Following this massive data breach in August 2015, a $576 million class-action lawsuit was filed against the company. In July 2017, Avid Life Media, the parent company of Ashley Madison, agreed to pay $11.2 million to settle the class-action lawsuit on behalf of the approximately 37 million users whose personal details were leaked.

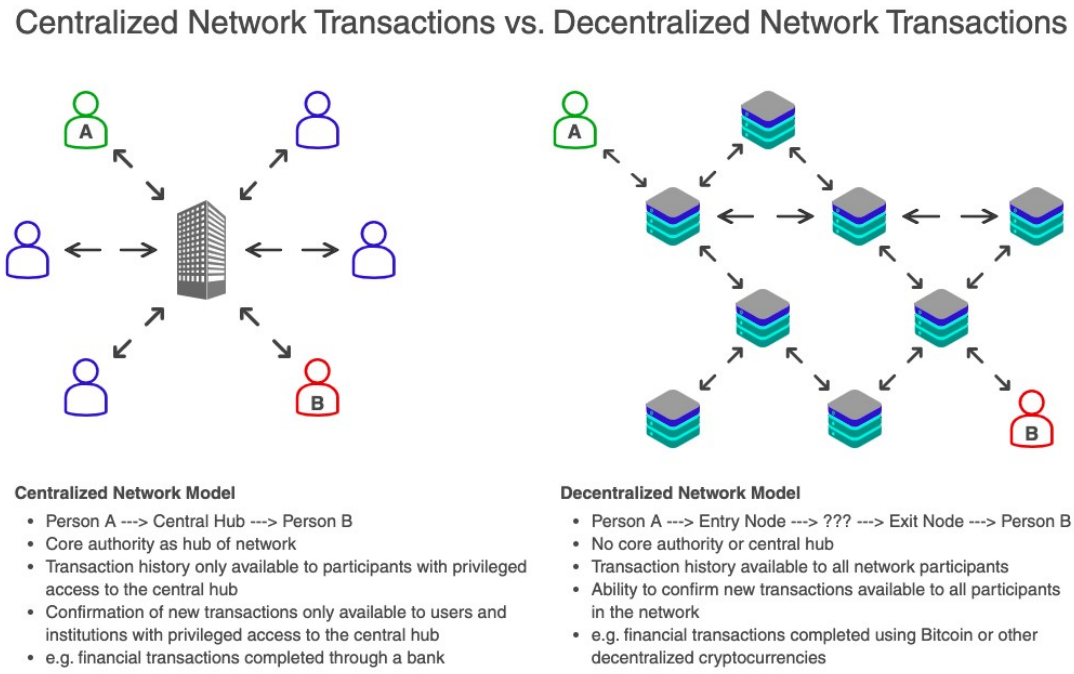
As large-scale malicious data breaches and extortion via data theft is now a reality for companies operating online and using cloud

networks, it is worth considering the question of liability for corporations with respect to data protection and the Dark Web. Certainly at the very least, requiring additional authentication for approved user access to Deep Web material is an obvious initial preventative and protective measure, but it is also important to proactively prepare for what happens when prevention and protection are not enough and irreparable widespread damage is caused from a privacy or data breach of a large magnitude.

Many, if not all, Dark Web encrypted transaction take place using a form of cryptocurrency, like Bitcoin, which has grown in use and popularity since its introduction in 2009. Legislators and corporations may want to consider the widespread social, legal, and financial implications of a growing online world of decentralized currencies, in the form of cryptocurrencies, which can be used to anonymize online transactions on the Surface Web as well as those which are already in place on the Dark Net. As an extra bonus, some cryptocurrencies can also be used (albeit infrequently) for purchases in traditional physical in-person stores and marketplaces, known as “brick and mortar businesses”.

Cryptocurrencies, like Bitcoin, are anonymous and cannot be traced because they are decentralized. This allows a buyer in one region to convert their national currency to a common cryptocurrency and complete an online transaction with a seller in another region using that cryptocurrency. The seller, upon receipt of the cryptocurrency at the end of the transaction, could then convert the cryptocurrency from the buyer into the national currency of their region. The currency conversion on both ends would be done anonymously and encrypted over the Dark Net, circumventing the use of banking institutions for currency

conversion, and essentially eliminating all banking fees related to currency conversion services. By cutting the cost of the conversion service provided by a bank also allows for individuals to send money to family in other countries or regions without having to use a banking and wire transfer service at a highly inflated cost, allowing the individual to retain more of their own money.



Click to enlarge

For businesses who want to connect with the anonymous online market or accept a wider range of international currencies, this could involve expanding current financial services to accept specific cryptocurrencies as payment for both online and in-person transactions or providing a variable conversion rate for specified cryptocurrencies. This would allow a buyer in one region to convert their national currency to a common cryptocurrency, complete an online transaction with a seller in another region using the agreed-upon cryptocurrency. The seller, upon receipt of the cryptocurrency at the end of the transaction, could then convert the

cryptocurrency into the national currency of their region.

In Canada, the law of securities regulation and banking is under the federal division of power. This means that any laws or legislation relating to the regulation and legal exchange of cryptocurrencies (as a security) falls under the federal legal jurisdiction. The main issues facing federal legislators in tackling the cryptocurrency markets are a general lack of understanding and awareness of cryptocurrencies, the perceived complexity of blockchain structure, the lack of a centralized data depository for keeping records of transaction history, the difficulty in tracing and identifying the individual parties on either side of a transaction, the inability to determine the contents or context of a transaction, and the general uncertainty and fear of a notoriously volatile online currency which many in government and law still do not fully understand. We will explore the topic of cryptocurrencies in greater depth in a future article.

Conclusion

With the growth and expansion of the online marketplace, even before the COVID-19 pandemic lockdowns had people switching from in-person to online shopping, we are entering a new frontier of commercial enterprise. The rise in popularity of encryption technology and interest in cryptocurrencies presents a novel medium, or forum, for previously criminalized criminal activities. This advancement has allowed illegal online activities to become truly borderless, as browsing and transactions can now be completed not only with encryption but with full anonymity.

It is now possible, and not at all uncommon, for an individual in

one jurisdiction to connect to a remote server in another jurisdiction, which can then connect to or host content which is not available or highly illegal in the jurisdiction in which the individual is operating. The Dark Web/Dark Net provide access to a hidden realm in which the lack of detection, monitoring and tracing ability of law enforcement enables an absence of accountability for the user.

This technology is powerful and unprecedented. We are more connected to our devices and the online world than ever before. Now, more than ever, it is necessary for corporations and legislators alike to become more aware and informed of encrypted online networks and the risks of massive large scale data hacks and subsequent anonymous Dark Web data dumps. The added complexity of determining legal jurisdictional authority in a naturally cross-jurisdictional and international encrypted and anonymized realm, while ominous and off-putting, is a challenge that must be tackled before international Dark Web/Dark Net cryptocurrency-enabled cross-jurisdictional crimes become more prevalent and we are forced to deal with the influx of class-action lawsuits which may inundate us sooner than we ever thought possible.

In the next article in our Understanding Canadian Cybersecurity Laws series (Article 8), we will discuss the issues and ideas for tailoring future cybersecurity laws in Canada in a digital age.

Would you recommend this article?

Thanks for taking the time to let us know what you think of this article!

We'd love to hear your opinion about this or any other story you read in our publication. **Click this link to send me a note →**

Jim Love, Chief Content Officer, IT World Canada

Related Download

Sponsor: **CanadianCIO**

Cybersecurity Conversations with your Board – A Survival Guide

A SURVIVAL GUIDE BY CLAUDIO SILVESTRI, VICE-PRESIDENT AND CIO, NAV CANADA

Download Now