V.I.P. PROTECTION
Information Services

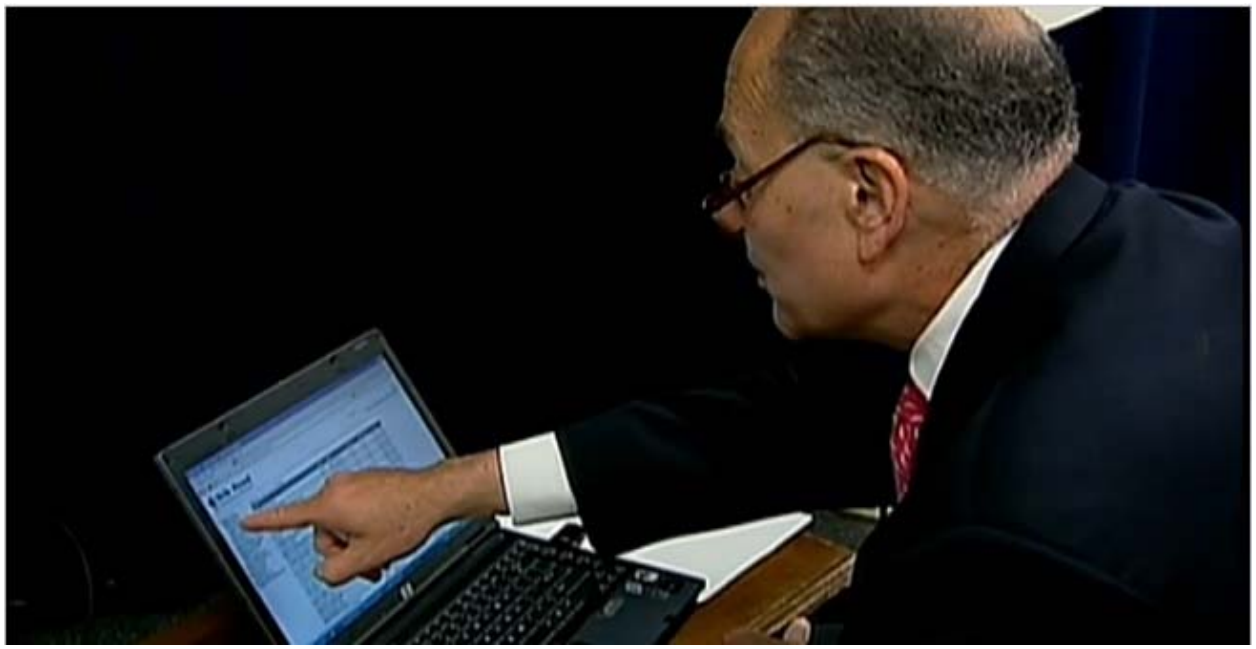
Office: 1-855-569-0070
www.vip-protection.ca www.sandexecutiveservices.com

Los Angeles, California, United States of America, March 25th, 2015

The Silk Road:

Analysis of the Dark Web site and the innovative methods utilized by its operators and users to maintain anonymity online

1. Press Conference: Senator Schumer blows the lid off the Silk Road



Senator Chuck Schumer checks out the Silk Road

On Sunday, June 5, 2011, U.S. Senator Charles "Chuck" Schumer held a news conference in which he called upon federal authorities to shut down a secretive market for illicit drugs operating online with anonymous sales and untraceable currency via a website called the *Silk Road* located in what is known as the *Deep Web*. Senator Schumer had been prompted to take this action by stunning reports made public several days earlier by the blog known as Gawker along with other news media.

Gawker had led off its coverage of the Silk Road with the following sensational rhetoric:

Making small talk with your pot dealer sucks. Buying cocaine can get you shot. What if you could buy and sell drugs online like books or light bulbs? Now you can: Welcome to Silk Road.

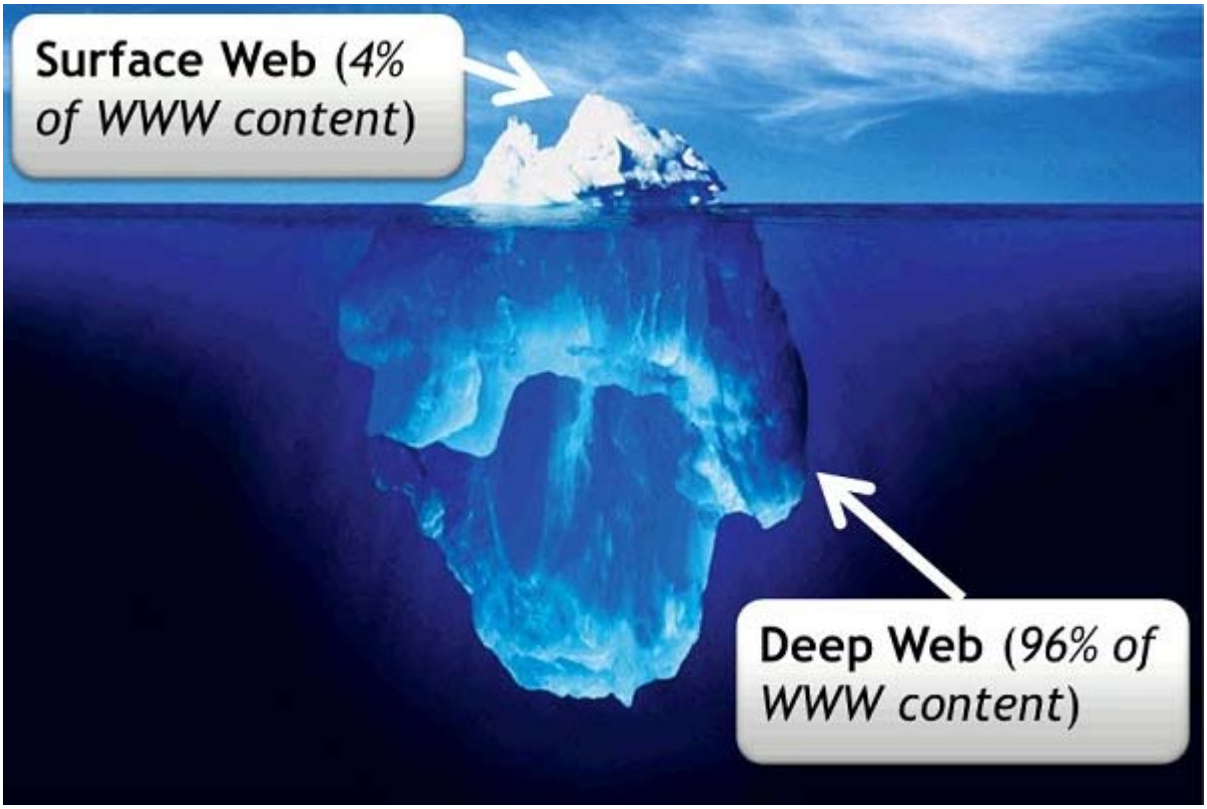
The public outrage created by these news reports had compelled Senator Schumer to describe the Silk Road at his news conference with some sensational rhetoric of his own:

"Literally, it allows buyers and users to sell illegal drugs online, including heroin, cocaine, and meth, and users do sell by hiding their identities through a program that makes them virtually untraceable," Schumer said at a news conference Sunday. "It's a certifiable one-stop shop for illegal drugs that represents the most brazen attempt to peddle drugs online that we have ever seen. It's more brazen than anything else by light-years."

But how were buyers and users able to hide their identities? And how were they able to conduct untraceable financial transactions? What is the Deep Web? This document endeavours to answer such questions below.

2. What is the Deep Web? What about the Dark Web?

The Deep Web is that portion of the World Wide Web that is not indexed by standard search engines like Google. Standard search engines utilize programs known as crawlers or spiders to gather information, and this method works well if the given database being searched has been designed to respond to the queries made by such programs. But if the developer of a website chooses not to design the site to respond to such queries, the site's database will be ignored by standard search engines. So, if we think of the total World Wide Web as an iceberg, Deep Web sites are "deep", meaning they are beneath the "surface" of the water. Above the surface is where sites that are designed to respond to standard search engines reside, and so we refer to that portion of the Web as the Surface Web. Note that the size of the Deep Web is vastly greater than that of the Surface Web by orders of magnitude, so the analogy of the iceberg is indeed apt.

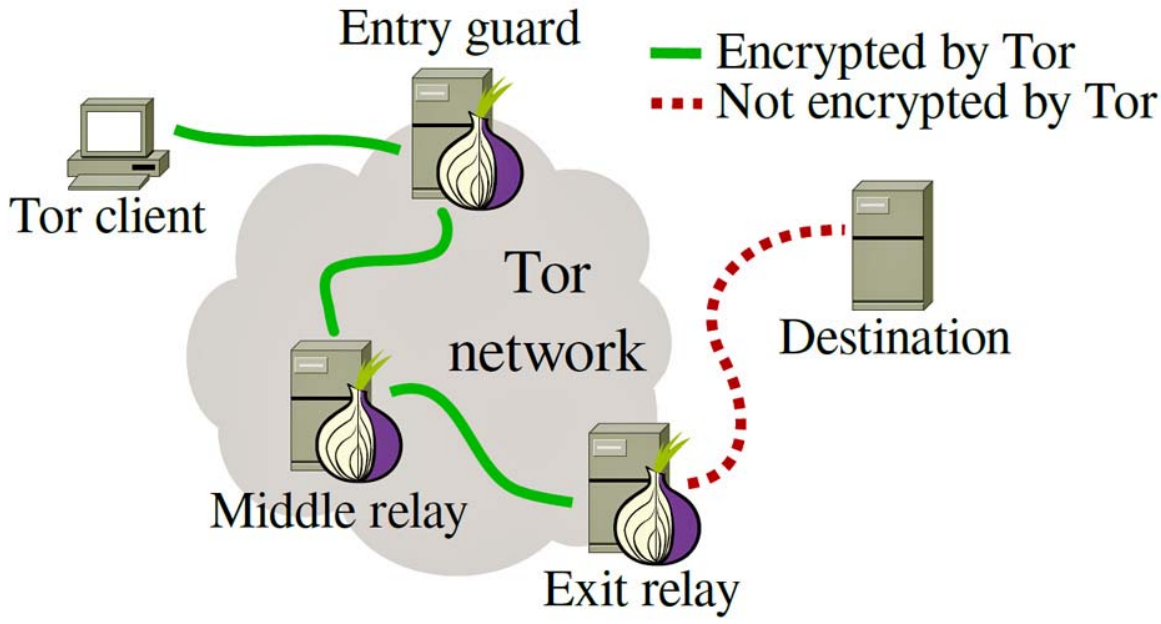


The creator of the Silk Road, a man we now know to be Ross Ulbricht, made his controversial website part of the Deep Web by design for obvious reasons, namely to help him evade capture and prosecution by U.S. law enforcement agencies as he planned the site to be a marketplace for illicit drugs.

One should note the technical difference between the Deep Web and something else known as the *Dark Web*. The Dark Web is a subsection of the Deep Web made up of private networks called "darknets." A "darknet" is a private network of Deep Web sites where connections are made only between trusted peers or "friends" using non-standard protocols and ports. The collection of all darknets forms the Dark Web. Despite this technical difference, however, the terms Deep Web and Dark Web do seem to be used interchangeably in news media reports. The Silk Road is referred to as part of the Deep Web and/or the Dark Web by many sources.

3. How did Ulbricht and his users hide their identities while communicating online? Answer: ***Tor***

The key to anonymity for Ulbricht and the users who bought and sold illicit drugs on the Silk Road was a computer program known as *Tor*. What is Tor?



Tor is free software produced by a company called *The Tor Project, Inc.* for the purpose of encrypting online communications and sending them across a free, worldwide, volunteer network consisting of more than six

thousand relays. The name "Tor" is an acronym for the project's original name, *The Onion Router*. In an onion network, information is put through several layers of encryption, like the layers of an onion. The Tor software sends a user's traffic through the Tor network in order to shield the user's location and data from any potential network surveillance or traffic analysis. As many people now know, a device that is connected to the internet is identified by what is known as an IP address. As long as Ulbricht and his users utilized Tor, the true IP addresses of their devices remained effectively concealed from law enforcement agencies and also from each other. Ergo, Tor made them anonymous.

However, it is important to note that Tor was not intended for criminal purposes when it was launched. Rather, it was intended to enable individual users to protect their privacy while communicating online, and also provide individuals with the freedom and ability to conduct confidential online communications. The fact that Ulbricht and the users of the Silk Road utilized Tor for criminal activities does not make Tor itself evil by design. In the same fashion that "guns don't kill people; people kill people", Tor software and the Silk Road Deep Web site didn't buy or sell illicit drugs; Ulbricht and the Silk Road users bought and sold illicit drugs and used Tor software to hide their online communications. In fact, the U.S. Navy currently uses Tor for intelligence gathering and covert operations in parts of the Middle East. Law enforcement agencies themselves often use Tor to conceal government IP addresses while conducting undercover sting investigations. And the potential for Tor to assist law-abiding citizens in maintaining their online privacy and protecting themselves from identity theft and other types of online attacks is indisputable.

4. How were Ulbricht and his users able to conduct untraceable financial transactions? Answer: ***Bitcoin***

The users of the Silk Road conducted their online transactions in a digital "cryptocurrency" known as Bitcoin. What is Bitcoin?

Bitcoin is an online payment system which utilizes peer-to-peer transactions, meaning users deal directly with one another and there is no central authority of any kind. Transactions are verified by nodes on the network and recorded in a publicly distributed ledger called the block chain. The block chain ledger uses its own unit of accounting, namely the bitcoin. Bitcoin was released in January of 2009 and, although at the beginning of 2013, we saw one bitcoin (XBT) trading at a price of around $13 in U.S. dollars (USD), bitcoin is currently (at the time of this writing) trading on the open currency markets at a value of **1.00 XBT = 247.46 USD** according to XE Currency Converter (http://www.xe.com). As the users of the Silk Road dealt directly with one another in peer-to-peer bitcoin transactions, they left no traces of their transactions in any bank or financial institution of any kind.

5. How big was Silk Road?

Doing business in bitcoins and communicating via the Tor network allowed Ulbricht and the users of the Silk Road to create, in the words of Senator Chuck Schumer, "the most brazen attempt to peddle drugs online that we have ever seen." Research conducted by Carnegie Mellon computer security professor Nicolas Christin while the site was still active indicated that, at its peak, the Silk Road was doing between **$30 million and $45 million per year** in sales.

Screen capture of the Silk Road in operation

When the FBI announced the arrest of Ulbricht in October of 2013, they estimated that the site had done **$1.2 billion in total sales** since its inception in February of 2011. However, as Ulbricht's trial began in January of this year, prosecutors scaled that estimated figure back to **$200 million**. Note that Ulbricht charged 10 to 12 percent on each transaction that took place on the Silk Road. Even with the scaled-back figure, Ulbricht became rich very fast.

Ross Ulbricht

6. So, if Ulbricht's techniques were so effective, how did they catch him?

On Wednesday, February 4, 2015, nearly four years after Senator Schumer's press conference, 30-year-old Ross Ulbricht was convicted of all seven crimes he was charged with, including narcotics and money laundering conspiracies and a "kingpin" charge usually reserved for mafia dons and drug cartel leaders. His trial lasted less than a month and it took the jury only 3.5 hours to return the guilty verdicts. Ulbricht's minimum sentence will be 30 years in prison; the maximum is life. Ulbricht's legal team has declared their intent to appeal his convictions.

The Dread Pirate Roberts

Prior to his arrest, Ulbricht was known only by his online alias, Dread Pirate Roberts, a name he took from a character in the 1987 movie, "The Princess Bride." Ulbricht was arrested in a public library in San Francisco in October of 2013. When he was arrested by the FBI, his fingers were on the keyboard of his laptop and he was logged into the "mastermind" user account belonging to the Silk Road. The FBI seized the laptop and found it to be a goldmine of evidence for Ulbricht's prosecution. The seized laptop contained a journal, a daily logbook, and thousands of pages of private chat logs that chronicled Ulbricht's years of planning, launching, and operating the Silk Road. Investigators were also able to trace $13.4 million worth of bitcoin transactions to the bitcoin "wallets" stored on the laptop. But how did the FBI track down Ulbricht in that library?

According to the evidence presented at trial by Ulbricht's prosecutors, the FBI discovered the Silk Road's true IP address in June of 2013 and traced it to a server located in a data center in Reykjavik, Iceland. After the FBI enlisted the cooperation of police in Reykjavik, those same police accessed and secretly copied the server's data,

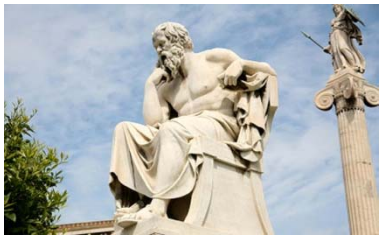
and then passed the data on to the FBI. The information contained within the server data was sufficient to lead the FBI to Ulbricht in the library, and Ulbricht's seized laptop became the prize piece of evidence at trial.

Silk Road screen after FBI seizure

Ulbricht's legal team has raised many challenges to the legality of the searches conducted by the FBI, and one very controversial issue is the question: did the FBI or some other agency (such as the NSA) successfully penetrate the Tor network? The FBI says no such penetration occurred. They say, rather, that they used a rather mundane technique to expose a misconfiguration in the Silk Road login page which caused the site to "leak" the site's true IP address and thus the physical location of the site's host server. Information Technology (IT) security experts who have studied the FBI court statements are skeptical. While it appears that the FBI is not lying outright, it seems likely they are not disclosing all the details of their investigative tactics.

One of the skeptical experts is Runa Sandvik, a privacy researcher who has closely followed the story of the Silk Road and worked for the Tor project at the time of the FBI's discovery. "The way [the FBI] describe how they found the real IP address doesn't make sense to anyone who knows a lot about Tor and how web application security works," Sandvik says. "There's definitely something missing here." Another expert is Nik Cubrilovic, an Australian security consultant who has made a hobby of analyzing the Silk Road's security since just after it launched in 2011, and he says, "The way they're trying to make a jury or a judge believe it happened just doesn't make sense technically."

Instead, Cubrilovic and Sandvik both suggest that the FBI took a more aggressive approach to investigating the Silk Road, namely actively attacking the login page with hacking tactics to reveal its IP. They speculate that the FBI used a hacker trick that involves entering programming code into a data entry field. If such an attack is successful, it can trick the site's server into running that code as actual commands, forcing the site to cough up data that could include the computer's IP address. Although this is all just theory and speculation, even if it is correct, it would still not show that the FBI lied to the court. Rather, in leaving out certain details, the statements made by the FBI would then be revealed to have been carefully crafted to be opaque, a strategy that one might consider to be "fair game" in the quest to put the bad guys behind bars. Though this could open an avenue to Ulbricht's legal team to challenge the legality of the FBI searches under the Fourth Amendment, there's no guarantee such a challenge would be successful. It may turn out that Ulbricht's case enters uncharted legal waters over the course of his appeals. It will be interesting to watch as the appeal proceeds.



The matter of Ulbricht's guilt in the court of law, however, is distinct from the question of his guilt (or innocence) in the court of public opinion, and this question is a complicated one. We know Ulbricht created and operated the Silk Road, he has admitted as much. But he and his supporters are making the broader moral argument that, since the buyers and sellers on the Silk Road were all consenting adults, there is no victim of his actions, and, as the old argument goes: no victim, no crime. Addressing this argument is a matter for philosophers and is certainly beyond the scope of this research paper, but no matter how you see Ross Ulbricht: as a swashbuckling Dread Pirate Roberts or as a contemptible criminal, you have to be impressed by the man's innovative use of the latest technologies. There is a great deal of valuable information that can be learned from the story of the Silk Road and such information can certainly be put to effective use in the field of IT security.

V.I.P. PROTECTION
Information Services

Office: 1-855-569-0070
www.vip-protection.ca www.sandexecutiveservices.com

An important question raised by this case for security experts is, did the investigation that led to Ulbricht's capture involve a defeat of the anonymity provided by Tor? While Ulbricht's legal team suggests that it does, the FBI says it did not, and here we can be confident that the FBI is telling the court the whole truth. Our confidence comes from the fact that military and law enforcement continue to utilize Tor for their own covert operations, i.e. they still have confidence in Tor, as well as the fact that it has been widely reported that many new illicit marketplace Deep Web sites have emerged to fill the void created by the FBI's shutdown of the Silk Road. There is already a "Silk Road 3.0" (Silk Road 2.0 was found and shut down by the feds on November 5, 2014) up and running along with many other online "drug bazaars." It appears that, in the wake of Ulbricht's takedown, the revised strategy of the online drug dealers is to decentralize the marketplace by creating many different sites, so that all their eggs are never in one basket.

The protection of privacy and the freedom to communicate confidentially are valuable assets that software like Tor can help to provide, and individuals are right to act to seek to maintain these assets in the digital age. Tor is still evolving, however, like many new technologies, and even Tor's developers warn that it is not invincible to attack. Tor is just one measure, albeit a powerful one, that people can utilize to protect their privacy online. With the ever-evolving nature of technology today, however, it is increasingly important for businesses to acquire expertise in IT security

*****Sources upon request*****

Sincerely yours,

Director of IT & Cyber Division
Toll Free: 1-855-569-0070
www.vip-protection.ca
www.sandexecutiveservices.com