

**Election Commission:
Credibility gap**

**EDITORIAL
Modi's burden**



www.indialegalive.com

June 3, 2019

₹ 100

INDIA LEGAL

STORIES THAT COUNT



The Great Oil Spill

America's directive to India not to lift Iranian oil leaves New Delhi with tough choices. It cannot afford to lose US markets or jeopardise its ties with Iran and the crucial Chabahar Port link

Mafioso of the Wired World

It is time to regulate this part of the web which is not accessible through regular browsers and where nefarious activities and cyber attacks are planned
By Na Vijayashankar



Anthony Lawrence

criminals who can use them.

All cyber criminals who get caught by the police are not members of the Dark Web. They only interact with the agents of the Dark Web. Members of the Dark Web make money by selling crimeware and avoid coming on the radar of law enforcement agencies.

The economy of the Dark Web is strong and supported by crypto currencies like Bitcoin. By cultivating friends among the corrupt, Dark Web mafia try to get their under-world currencies like Bitcoin integrated with currencies of the Meta Society so that they can enjoy their ill-gotten wealth.

Unsuspecting and ill-informed persons think that crypto currencies and anonymity are symbols of a free society and should be encouraged. The gullibility of such people is exploited by Dark Web dwellers in getting crime-friendly regulations, making the task of law enforcement difficult. It is essential for the survival of civilised society that we take whatever steps are necessary to regulate this monster so that it is chained and rendered harmless.

The general topography of the internet is that every device has a unique ID issued by a regulatory agency and its identity should be part of every communication that

goes out as data packets. This is the IP address with which we should be able to track every internet activity. The device ID can be optionally a part of such communication. This helps law enforcement detect any activity on the web and enforce law on such players.

The Dark Web, however, creates a system of "Onion Routers" where messages are transmitted with layers and layers of transmission along with strong encryption. The routing is through many dummy systems to hide the IP address. Unravelling it requires several layers of the routing to be peeled (like onion skins) and also decryption. The surface communication that is available

to law enforcement is actually a false IP address and prevents them from identifying the users of the system.

Data accessible in the Dark Web is stored in servers managed by its mafia and is often hosted in countries where the governments are supportive of the criminal activities for their own selfish reasons. Data is encrypted and access is managed through a strong access control system. Many servers of the Dark Web do not provide hosting accounts unless the applicant proves his hacking credentials. Further, the onion routing system hides the identity of the servers in messages.

It may not be out of place to mention here that the origin of the Dark Web concept can be traced to Switzerland which created "Numbered Swiss Bank Accounts" which enabled criminals to hide their wealth. It took years to



The economy of the Dark Web is strong and supported by crypto currencies like Bitcoin (left). The Dark Web also sustains the drug trade, illegal arms trade (below) and bank heists. It creates tools of crime.



UNI

persuade Swiss authorities to cooperate with other nations to reveal secret bank account data at least where criminality is proven. We can, therefore, appreciate how hard it would be to convince rogue nations not to allow hosting of Dark Web servers.

At the user level, there are specialised browsers like "Tor" browsers which can be downloaded by anybody in the Surface Web and used. A combination of the Tor browser and the secure hosting in a friendly rogue country can help Dark Web activities to be technically enabled.

Despite the difficulty and enormity of the task, there is no excuse not to attempt regulation of the Dark Web with a view to mitigating its adverse impact on society. Some of the solutions that civil society needs to consider along with legal enablement are:

- Choke the economy of the Dark Web by banning crypto currencies at a global level. Let the transactions come to the Surface Web where they can be netted.
- Replace the concept of total anonymity with the concept of "Regulated

Anonymity".

- Regulated Anonymity as a concept is where the identity of a data user is de-identified and the de-identification algorithm is controlled in a decentralised framework that avoids governmental control. But it is still open for law enforcement under a due process which is acceptable both for privacy activists and governments.

- Declare Dark Web activities as "terrorism" and declare the countries which host Dark Web servers as "terror-supporting countries".

- Tighten intermediary regulations to ensure that "agents of the Dark Web" are punished adequately.

- Regulate the use of Tor browsers and other tools of encryption that assist the Dark Web through a system of voluntary registration.

- Create a "Secure Surface Web" where every participant is identified (KYC grade) and transfer all the financial transactions above a reasonable limit from the surface web to a secured Surface Web. This will be a trusted web to be used voluntarily by interested persons.

- Device ID should be made part of the Transmission Control Protocol/IP communication protocol and Surface Web intermediaries should reject packets not accompanied by verifiable device IDs.

There is no doubt that many members of the Surface Web are sympathisers of the Dark Web. And just as removal of corruption and black money in the Meta Society has insurmountable challenges, the war against the Dark Web would also be challenging.

However, challenge need not deter us if our goal is clear—to have a trusted digital society. And here, there is no place for the Dark Web. ■

—The writer is a cyber law and techno-legal information security consultant based in Bengaluru

Twitter: @indialegalmedia
Website: www.indialegalive.com
Contact: editor@indialegalive.com