Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
49/16

LIMITATION OF JURISPRUDENCE IN THE CONTEXT OF CYBER SPACE: IS THERE SEVERITY AND LENIENCY IMBALANCE IN US AND INDIAN CYBER LAWS

Gp Capt Ashish Gupta
Senior Fellow, CAPS

Cyber Legal jurisprudence needs to an evolving process in order to keep it at pace with the technology advances and severity of consequential effects of cybercrimes. The penalty or punishment for cybercrimes needs to have reformative or deterrent effect, commensurate with the seriousness of the criminal behaviour and *consequential* or *intangible damages* from the criminal act. *In cyber realm,* evolution in technologies, policies and standards, social interactions and even changes in cyber *behavioural* responses continuously reshape the contours of cyber landscape. In the context of cyberspace, *jurisprudence is* manifestation of its progression/ proliferation and collective regulatory processes to rein in illegal or unsafe practices and enforce laws.

In 1984, when the computer penetration was still low, proficiency to use computers was not a priority and fledgling computer users rarely encountered *criminal acts*, US Congress enacted a statute designed to criminalize unauthorized access to computers. That law referred to as the **Computer Fraud and Abuse Act (CFAA)** was originally designed to criminalize only important federal interest computer crimes. Now it potentially regulates every use of every computer in the United States and even many millions of computers abroad. The Act has been substantially modified five times.[1] The statute is in the eye of storm since its enactment. Some have termed it as draconian and short sighted while others think of these as progressive and effective.

In US, the debate over the prosecution proceedings and subsequent conviction/ sentence under CFAA has become vociferous and polarized. In one such case, in July 2011, Aaron Swartz was indicted on multiple felony counts

for downloading several million academic articles from a subscription database called JSTOR. It was unclear what Swartz intended to do with the articles, but in post-WikiLeaks US, the apparent zeal with which the case was pursued by US attorney Carmen Ortiz and Massachusetts assistant US attorney Stephen Heymann took many by surprise. Despite the fact that Swartz's made no personal financial gains and there was no discernable victimization of any person, and despite the JSTOR decision of not pursuing charges after he returned the articles, a formal deal to kept Swartz out of prison was rejected. In January 2013, less than three months before the criminal trial was set to begin Swartz hanged himself with his belt in his Brooklyn apartment.[2] The News of his death was received with *a sense of poignant* sadness by many. The BBC Four screened a film '*The Internet's Own Boy'* on story of the life and tragic death of Aaron Swartz. It is believed by many of his followers that he was hounded to suicide by a vindictive US administration at the age of just 26.[3]

In another case, In October 2006, a Missouri woman Lori Drew aged 49, was accused of creating a fictitious character on 'MySpace' to cyberbully a 13-year-old neighbour who then committed suicide. Drew was alleged to have created a fake identity of 16 years old boy on MySpace and with this fake identity cyber-befriended her neighbour Megan Meier, in the suburb of St Louis and exchanged flirtatious emails. She was alleged of using her fake identity to send e-mails that were emotionally cruel and drove Meier to suicide. The federal prosecutors in an attempt to bring charges against Drew invoked CFAA, which is usually applied against hackers seeking to break into computers in order to steal valuable information. In this case the prosecution argues that the servers used by MySpace were violated by Drew who used false information to set up the account and therefore broke the website's terms of service. The charges were thought to be the first of their kind involving a social networking website and have far-reaching implications for the way in which the internet is used. [4]

On 13 April, the CFAA was once again used to sentence Matthew Keys, a former *LA Times* employee to two years in prison on accusation of giving a username and password to a hacker who vandalized an article on the *LA Times* website which stayed defaced for about 40 minutes before it was fixed.[5] Some in the legal fraternity term this as heavy-handed prosecution and have vowed to put combined efforts to help Keys. The CFAA makes it a federal crime to access a "protected computer" but the felony charges in law can only apply if the "value of such use" is US $ 5,000 or more, or if the person accessing the protected computer causes more than US $5,000 in damage. But the loss or damage to data due to acts with criminal intent or the cost of repairing a system cannot be determined in exact monetary terms. In Keys case, prosecutors put the damage of the *LA Times*

vandalism subsequent repairs at US $900,000 but the court finally accepted damages of US $18,000.

In India, [6] the two legislations: **The Information Technology act 2000** and **the I.T. Amendment Act 2008**deal with cyber offenses in Indian judicial system. Under the provisions of both laws, acts of offences committed by using computers as medium and tool are prosecuted. Unlike CFAA, the technology Act takes an approach with intent to regulate electronic conduct within electronic commerce. The US prosecutes cybercrimes by combining numerous laws to achieve a successful criminal filing. India, on the other hand, makes use of a uniform law designed specifically for cybercriminal offences. From the above examples, it is clear that CFAA enforces laws with stern punitive measures, whereas in India the laws are loosely framed and leniently enforced. Theft of intellectual property is a crime in both jurisdictions, however downloading copyrighted material can have serious *financial and punitive repercussions* in US, whereas similar act will be judged with leniency in India. Besides, foreign Internet companies like Google, Facebook, Microsoft, etc. only loosely comply with Indian Laws and adhere to US laws and policies even when US laws are found wanting in Indian context.

In the context of cyber jurisprudence, *there is wide disparity in* provisions of law governing human rights in cyber space and *prosecution* of perpetrators of cybercrimes. The *commensurate* or proportional punishments also fell short in enforcing compliance with the vision of a coherent and ordered cyberspace. The cyber rules and laws need to evolve and applied contextually with *reform and deterrent as their main objectives.* Both US and Indian cyber laws are not *infallible* and are prone to excessive severity (*in the context of U.S. laws* and enforcement mechanisms) or excessive leniency and need to be constantly amended, updated and enforced.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1]Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187, accessed April 27,2016

[2]Elizabeth Day, Aaron Swartz: hacker, genius… martyr?, *The Guardia,* June 2, 2013, https://www.theguardian.com/technology/2013/jun/02/aaron-swartz-hacker-genius-martyr-girlfriend-interview, accessed April 27,2016.

[3]John Naughton, Aaron Swartz stood up for freedom and fairness – and was hounded to his death, *The Guardia,*

February 7, 2015, http://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy, accessed April 27,2016.

[4]Ed Pilkington , Death of 13-year-old prompts cyberbullying test case, *The Guardia* ,June 17, 2008 , http://www.theguardian.com/world/2008/jun/17/usa.news, accessed April 27,2016.

[5] Grant Burningham, The most hated law on the Internet and its many problems, *Newsweek*, April 16, 2016, http://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567, accessed April 27,2016.

[6]Law Today, "Indian vs American Information Technology Law, http://lawtoday.co/indian-vs-american-information-technology-law/, accessed accessed April 27,2016.