PAVAN DUGGAL

Cyber Law
Global Trends in 2014

In the year 2014, Cyberlaws may have to tackle several issues ranging from increased thrust in cost-effective interception surveillance to providing far more protection and preservation of individual stakeholder's online privacy in the digital and the mobile ecosystem and also protection from increasing cyber attacks.

THE advent of the Internet, the mobile and the digital ecosystems have ushered all of us in a new irreversible era in our lives. A digital platform has been added which runs our lives, more or less, in terms of keeping in touch with friends and relatives, communicating with business peers and clients, seeking and providing services, digging out information, and even providing e-governance.

The year 2013 has seen numerous events unfold in the field of cyberspace. So there is a need for appreciating the constantly emerging new cyberlaw trends in the new paradigms that we are living in.

The author is no soothsayer and as such it is impossible to predict accurately as to what will be the relevant trends that will impact cyberlaw development in 2014. However, based on the existing realities of 2013, given the way our technology is moving, it is possible to look at and identify certain emerging important cyberlaw trends that are likely to have significant impact upon on the growth of cyber legal jurisprudence across the world in 2014.

The biggest cyberlaw trend in 2014 would be the enhanced frequency and instances of interception, surveillance and monitoring across the world. The recent Snowden revelations regarding the US surveillance programme PRISM have exhibited how networks and computer systems of legal entities outside a particular jurisdiction have been subjected to surveillance without the knowledge of such legal entities.

This being the case, 2014 is likely to witness an increased thrust in cost-effective interception surveillance, monitoring and decryption under the gazing eyes of other sovereign nations. Many countries are likely to put in place stringent regulatory regimes which will aim to prevent/curb the unauthorized access to their network and further make such acts as penal offences. However, the challenge will be to ensure as to how continued interception, monitoring and surveillance is to be regulated in a manner so as to give a semblance of respect to the rights and obligations of individual users of computer systems and digital ecosystems.

It will also be important to check the interception and surveillance being

(Courtesy: www.eolii.com)

Edward Snowden, who came to international attention after disclosing to several media outlets thousands of classified documents

The biggest cyberlaw trend in 2014 would be the enhanced frequency and instances of interception, surveillance and monitoring across the world.

carried out outside the territorial boundaries of countries and effectively regulate them within a legal framework.

Connected with this trend is the increased need for providing far more protection and preservation of individual stakeholder's online privacy in the digital and the mobile ecosystem.

Given the Snowden revelations, the fragmentation of the Internet is likely to be accelerated as different countries are coming up with their own secure national networks, thereby by-passing the dangers of surveillance and monitoring from foreign shores. In such a scenario, the fragmentation of the Internet is further likely to bring forward various legal, policy and regulatory issues, which are likely to be addressed during the year 2014.

Fragmentation of the Internet and interception, monitoring and surveillance are likely to bring in active focus the issue of the interplay of the online sovereignty of nations vis-à-vis activities of interception, monitoring and surveillance in cyberspace. Questions like where would the online sovereignty of nations begin and end are important issues that will have to be addressed. 2014 would be an interesting year to see how this important trend unfolds with the passage of time.

Another significantly important cyberlaw trend of the year 2014 is likely to be the increased thrust on cyber security policy issues. Nations are expected to come up with national legislative measures to further protect and preserve cyber security. Given the fact that the dark Internet has already established itself as a formidable force, and cyber crimes as services are now being provided on networks, clearly protection and preservation of the cyber security of a country's national networks as also its critical information infrastructure are going to be topmost priorities in 2014.

There is no denying the fact that all the aforesaid trends are important significant factors, which will have a bearing on the growth and further evolution of the international Cyberlaw ecosystem in the year 2014.

Cyber crime reports have revealed that 2014 will experience more cyber attacks and corporations will have to conduct more boardroom scrutiny to manage their data supply chains (http://www.siasat.com/english/news/2014-experience-more-cyber-crimes-report). As such, 2014 will see an increase in the demand for providing effective remedy in order to protect victims from cyber criminal attacks and offences.

The International Telecommunication Union (February 2013) estimates that there are 6.8 billion mobile subscriptions worldwide. That is equivalent to 96 percent of the world population (7.1 billion according to the ITU) (http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a). Kaspersky in their security bulletin for 2013 stated that the mobile world is one the fastest-developing IT security areas (Kaspersky Security Bulletin 2013).

As mobile crime continues to grow at a rapid pace in the year 2014, the relevant stakeholders will call upon the

DIGITAL COIN

THE latest mode of money transaction is Bitcoin. Bitcoin or Crypto currency is a form of digital currency, created and held electronically. No one controls it. Bitcoins are not printed.

A software developer Satoshi Nakamoto proposed Bitcoin in 2009 as an electronic payment system based on mathematical proof. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.

Bitcoin is different from normal currencies. It can be used to buy things electronically. In that sense, it is like conventional dollars, euros, or yen, which are also traded digitally. However, Bitcoin's important characteristics are that it is decentralized, easy to set up, anonymous in nature, completely transparent, transaction fees are miniscule, transaction is faster, non-repudiable, easy storage, hassle-free payment.

No single institution controls the Bitcoin network which puts some people at ease. At the moment, the largest full trading exchanges accessible to everyone are Mt. Gox (Japan), Bitstamp (US), BTC-e (Bulgaria), and Kraken (US). The world's largest Bitcoin exchange is BTC China.

Bitcoin Issue Rights do not rest with central banks – rather it is created digitally, by a community of people that anyone can join. Bitcoins are 'mined', using computing power in a distributed network. This network also processes transactions made with the virtual currency, effectively making Bitcoin its own payment network.

As per the Bitcoin protocol – the rules that make Bitcoin work – only 21 million Bitcoins can ever be created by miners. Bitcoin circulation is based on mathematics. Around the world, people are using software programs that follow a mathematical formula to produce Bitcoins. The mathematical formula is freely available by using open source software.

Bitcoin circulation takes place through the exchange platform that is distributed across thousands of computers, peer-to-peer style. In order to expand the total supply of Bitcoins, users also run complex algorithms on this peer-to-peer network to solve cryptographic puzzles. Each time a puzzle is solved additional Bitcoins get credited to the accounts of those who solved the puzzle. That is how the "money supply," as it were, expands in the Bitcoin market.

However, each new puzzle gets incrementally harder to crack. The system is designed in such a way that it can limit the growth of the supply of Bitcoins. The overall supply of Bitcoin in the system therefore grows at a slow and pre-ordained rate. There are currently 10.8 million Bitcoins in the system, and this will cap out at 21 million coins in just over 125 years.

Logo of Bitcoin
(Source: http://en.wikipedia.org/wiki/File:Bitcoin_logo.svg)

Unlike bank accounts, the Bitcoin accounts are called 'wallets' which are available in two ways – a software wallet stored on the hard drive of any computer, or an online web-based service. The popular CoinBase is a wallet service that trades dollars for Bitcoins, and has web and mobile (Android) apps. Blockchain.info is another popular online wallet option but it has only mobile solution available for both Android and iOS.

Other sites for wallet services are:

- MultiBit, a secure, lightweight, international Bitcoin wallet for Windows,

governments of the world to effectively strengthen their cyber legal systems and regimes to cover and regulate the newly emerging mobile threats and mobile crimes.

The resurgent interest in privacy is likely to be another trend of 2014. Google's chief internet evangelist Vint Cerf has stated that "privacy may actually be an anomaly" (http://motherboard.vice.com/blog/googles-top-execs-are-saying-the-opposite-things-about-privacy). The author has already, in one his tweets stated in the context of cyberspace that "Privacy is on its death bed, counting its last breaths...in a cold technology environment…" (http://lnkd.in/dUViBSk).

As mobile crime continues to grow at a rapid pace in the year 2014, the relevant stakeholders will call upon the governments of the world to effectively strengthen their cyber legal systems to regulate mobile crimes.

As technology will only erode the basic essentials of the concept of privacy in the digital ecosystem, the year 2014 is likely to see more calls from different stakeholders as well as the governments of the world to protect and preserve as also strengthen the legal regimes to help protect not just data privacy but also personal privacy of the relevant stakeholders.

As social media continues to grow, it is likely to bring forward various policy and regulatory aspects which countries of the world would increasingly be required

Typical Bitcoin wallet
(Source:http://thestatelessman.com/2013/06/03/using-bitcoin/)

The popular CoinBase is a wallet service that trades dollars for Bitcoins, and has web and mobile (Android) apps. Blockchain.info is another popular online wallet option but it has only mobile solution available for both Android and iOS.

MacOS and Linux. No blockchain download required.

- Armory (Alpha), an open-source wallet-management platform for the Bitcoin network.
- Electrum, a lightweight Bitcoin client, based on a client-server protocol. No blockchain download required.

In India there are about 2,000 active Bitcoin users. With an exchange within India once again, Buy Sell Bitcoin, the ability to purchase with cash (rupees deposited at HDFC or Axis bank), makes buying Bitcoins possible without having to transfer funds internationally or suffering excessive fees. The huge demand for Bitcoins in India has largely been from speculators hoping to gain from the rising value of the currency. There have been an estimated 29,400 downloads of Bitcoin wallets from Indian IP addresses.

The Reserve Bank of India has stated that it does not immediately intend to regulate Bitcoin and has not yet formulated regulations to govern trading or profits generated from Bitcoins.

Contributed by Mr Bibhuti Narayan Biswal is Principal, Sri Sathya Sai Vidyaniketan, Ganeshvad Sisodra, Near TATA SSL, N.H.-8, Navsari-396463, Gujarat; Email: chem_iway@sify.com

to deal with. Countries are likely to be called upon to revisit their existing cyber legal regimes in order to address the issues of social media. Various countries in different parts of the world have tried and are continuing to address the same in their own respective manner.

Cloud computing will be another growing trend in the year 2014. Cloud has already become a significant buzzword in our lives. While cloud has tremendous advantages, there are a large number of regulatory challenges pertaining to large-scale adoption of cloud computing as a popular technology. The year 2014 is likely to see significant development in the jurisprudence around cloud computing.

As the world moves towards mobility where more and more people own more than one mobile communication device, there is an increase in the number of personal devices being carried to work. BYOD, bring your own device, is indeed a magical phenomenon which helps companies to minimize expenditure in the infrastructure. However, the security, confidentiality and veracity of data as also jurisdiction are important legal challenges that have to be appropriately addressed by the cyber legal regimes in order to enable large and mass scale adoption of BYOD.

The growth of Bitcoins and other virtual currency(s) is yet another trend to watch out for in 2014. In its Security bulletin 2013, Kaspersky has predicted that attacks on Bitcoin pools, exchanges and Bitcoin users will become one of the most high-profile topics of 2014. Bitcoin crimes are likely to emerge as an important significant phenomenon in the year 2014, thereby forcing the relevant stakeholders to look at appropriate legal frameworks which can effectively regulate certain activities.

The advent and adoption of the data analytics at a mass scale requires that appropriate attention is given to issues concerning big data like authenticity, veracity of the data, data collection, data archiving, data retention jurisdiction, privacy, confidentiality and other data collection related issues. The year 2014 will call for creating appropriate legal and regulatory framework in this regard.

The above are important Cyberlaw trends in 2014 in the opinion of the author, given his work in Cyberlaw and given the nature of the existing ground realities and events that have occurred in 2013. It can be possible that some of these trends may or may not see the light of the day in totality or in the manner so envisaged.

However, there is no denying the fact that all the aforesaid trends are important significant factors, which will have a bearing on the growth and further evolution of the international Cyberlaw ecosystem in the year 2014.

Mr Pavan Duggal is Asia's leading Cyberlaw expert and authority and Advocate, Supreme Court of India. Pavan is the President of Cyberlaw Asia, Asia's pioneering organization committed to the passing of dynamic Cyberlaws in the Asian continent and also the President of Cyberlaws.Net, which is Internet's first ever-unique Cyberlaw consultancy. Pavan is also a member of the WIPO Arbitration and Mediation Center Panel of Neutrals. He has been associated with the Ministry of Communication and Information Technology, Government of India on Cyberlaw and Electronic Governance legal issues. Address: S-307, LGF, Greater Kailash-1, New Delhi-110048; Email: pavan@pavanduggal.net, pduggal@vsnl.com and pduggal@gmail.com.