EMERGING TECHNOLOGIES AND LEGAL CHALLENGES

Hitesh kumar[1]

Kirti meena[2]

Abstract

The world is experiencing a technological and social revolution moving with exponential velocity. Innovative technological trends such as Artificial Intelligence (AI), the Internet of Things (IoT), Blockchain, robotics, 3D printing, nanotechnology, augmented and virtual reality, emerge and converge bringing about a new digital era.

This new digital era is different due to the extensiveness of its scope and the vitality of its impact on human interaction and identity, distribution, production, and consumption systems around the globe. It is pervasive and non-linear; often, its consequences cannot be anticipated with certainty. It is an era where machines learn on their own; self-driving cars communicate with smart transportation infrastructure; smart devices and algorithms respond to and predict human needs and wants.

New governance frameworks, protocols, and policy systems are needed for the new digital era to ensure all-inclusive and equitable benefits. Societies need regulatory approaches that are not only human-led and human-centred, but also nature-led and nature-centred. Government policies need to balance public interests, such as human dignity and identity, trust, nature preservation and climate change, and private sector interests, such as business disruptiveness and profits. As novel business models emerge, such as fintech and the sharing economy, regulators are faced with a host of challenges: rethinking traditional regulatory models, coordination problems, regulatory silos, and the robustness of outdated rules.

What does “new and emerging technologies” mean?

The term “New and Emerging Technologies” (NET) encompasses the most novel, advanced, and prominent innovations that are developed within various fields of current modern technology. The current examples of NET include, for example, zero-emission cars that run on hydrogen, next-generation robotics, genetic engineering techniques, developments in artificial intelligence; nanotechnology, social networking, etc.

[1] Author, Indore Institute of law

[2] Co-author, Indore Institute of law

The scope of the term "New and Emerging Technologies" (NET) has been in a process of continuous expansion. Two decades ago, most NET were related to artificial intelligence machines. The popularity of augmented reality, nanotechnology, Internet of Things, and 3D printing started growing at the beginning of the current century.

Irrespectively of their type, NET have serious social implications. They shape our homes, businesses, and governments. A large number of Facebook's 1,44 billion monthly actively users use social networking at home. One can visit a restaurant in London in which the menus are projected directly onto the tables and orders are submitted digitally to the kitchen. Government authorities have set up facial recognition systems allowing them to identify and monitor people attending public events.

Although NET certainly bring benefits to the humanity, they also pose challenges. For example, the physical objects comprising the Internet of Things can allow hackers to receive far more information about their victims than hackers currently can. The solutions to the challenges posed by NET are three, namely, (1) research, (2) development, and (3) regulation.

The legal issues related to "New and Emerging Technologies" (NET) fall within the scope of the laws regulating the use of data, evidence, creative works, and inventions. We will further focus on four such laws:

- **Privacy law**, i.e., the law that regulates the collection, use, processing, and disclose of personal information. Under most privacy laws, personal information is defined as information which identifies an individual or allows an individual to be identified;
- The **law of evidence**, i.e., the law that governs the proof of facts in legal proceedings;
- **Copyright law**, i.e., the law that governs the ownership and use of creative works
- **Patent law**, i.e., the law that regulates the rights to inventions.

Four major categories of legal issues arising out of the use of NET, namely, privacy issues (Section 2), issues related to gathering evidence (Section 3), copyright issues (Section 4), and patent issues (Section 5). Finally, a conclusion is drawn (Section 6).

I.PRIVACY ISSUES

The privacy issues related to NET can be grouped into two categories, namely, (1) security vulnerabilities threatening the privacy of NET users and (2) the use of NET for unlawful surveillance (see Fig. 1). These two categories are examined in Sections 2.1 and 2.2, respectively. The first category relates to privacy issues caused by security vulnerabilities of

NET. Such security vulnerabilities may include, for example, weak authentication, insufficient encryption, and insecure firmware. The second category of issues refers to the use of NET for unlawful surveillance. For example, thieves may use crowdsensing for detecting when a victim is not at home. The term "crowdsensing" refers to sharing data collected by sensing devices with the aim to measure the phenomena of common interest.

Security vulnerabilities threatening the privacy of NET users

The security vulnerabilities of NET can be broadly categorized into (1) security loopholes and (2) security vulnerabilities caused by pre-installed malware. The security loopholes of NET are programming or others flaws which allow a hacker to reduce NET's information assurance. For instance, a weak password may allow the hacker to penetrate into NET by using a dictionary attack, i.e., a technique for defeating the authentication system of a computer system by using a large number of passwords. Other security loopholes of NET include software bugs, lack of security awareness, and weak or non-existent anti-virus programs.

In addition to security loopholes, some NET may have pre-installed malware. Such malware can be preinstalled either (1) by the manufacturer of NET or (1) by a third-party (a non-manufacturer). The pre-installed malware can affect other computers in a network. Thus, a smartwatch containing pre-installed malware can infect a smart kitchen, a smart phone, a household robot, and a smart air conditioner.

Using NET for unlawful surveillance

The following three types of NET are often used for unlawful surveillance:

1. **Beacons**, i.e., tiny wireless transmitters that constantly send radio signals. Beacons can be used by criminals to track the location of the users of mobile devices. For example, a criminal may install malware on victim's computers which collects location information from beacons and sends the collected location information to the criminal.
2. **Social networks**, i.e., platforms allowing their users to build social network relationships. Social networking can be used by criminals to receive unauthorized

access to personal information. For instance, a criminal may create a fake profile in Facebook and send a “friend request” to a victim. By accepting the “friend request,” the victim will allow the criminal to access a tremendous amount of personal information about the victim (e.g., personal data, photos, videos, and location information).

3. **RFID technology**, i.e., the wireless non-contact use of radio-frequency electromagnetic fields to transfer data with the aim to automatically identify and track tags attached to objects. A human implanted RFID chip installed without the knowledge and the authorization of the receiving person will make that person a lifelong object of surveillance.

II .Issues related to gathering evidence through Net

The digital information processed by NET can be used as evidence. However, due to various issues, digital evidence can be ruled inadmissible by courts or considered to be unreliable. The issues related to evidence collected through NET can be divided into two broad categories, namely, (1) general issues related to gathering evidence through NET and (2) issues related to gathering evidence through social networks. The first category encompasses issues which relate to digital evidence in general, e.g., inadmissibility of evidence because it was obtained without authorization and unreliability of evidence due to authentication problems. The second category covers specific issues related to the collection of evidence through social networks, e.g., authenticity and admissibility of evidence collected through social networks.

Issues related to gathering evidence through social networking platforms

The term “social networking platform” means an online application which allows its users to share content in virtual communities. Social networking platforms appeared in the last decade of 20th century. Initially, they allowed people to create personal pages and interact with each other through chat rooms. At the beginning of 21st century, social networking websites, such

as MySpace and LinkedIn, developed comprehensive profile creation tools. Facebook, a social networking platform introduced in 2004, became the largest social networking site in the world.

There are six categories of social networking platforms. These categories are described below.

1. **Social networking platforms connecting people in general** (e.g., Facebook and MySpace) allow various users to connect with each other. For example, consumers may use such platforms to connect with companies.
2. **Social networking platforms connecting professionals** (e.g., LinkedIn, Plaxo, and Xing) are focused on business communications. These platforms are used mainly for communication between professionals.
3. **Social bookmarking websites** (e.g., Digg, Delicious, and StumbleUpon) allow users to add, edit and share bookmarks of web documents.
4. **Internet forums** (e.g., Meetup and Craigslist) provide their users with the opportunity to hold discussions in the form of posted messages.
5. **Business directories** (e.g., Yelp and CitySearch) list business operating within the same business field.
6. **Photo and video sharing platforms** (e.g., YouTube and Flickr) enable users to sell, view, and purchase photos and videos.

Users of social networking platforms often publish in their profile photos, videos, text, location information, as well as information about their relationship. Such information can be used as evidence in court proceedings. The party who would like to use the evidence does not need to prove each step of the creation of the evidence to guarantee its authenticity. The evidence collected through social networking platforms is not treated differently than the other types of evidence. The most common types of evidence collected through social networking platforms are (1) photos; (2) videos; (3) text; (4) location information; and (5) information about relationships.

Issues related to authenticity of evidence collected through social networking platforms

Social networking evidence that may require authentication includes but is not limited to, (1) social network profiles, (2) social network postings, (3) chats from social networks, and (4) photographs and videos from social networks.

Given the ability of hackers to modify content published on social networking platforms, courts are open to rebuttable evidence. Rebuttable evidence means evidence which repeals, counteracts, or disproves other evidence. For example, a Facebook profile indicating the behaviour patterns of the defendant may have no evidentiary value if there is rebuttable evidence showing that the Facebook profile was not created by the defendant, but by a third party which is not related to the defendant in any way.

Therefore, the authentication of social networking evidence requires answering five questions:

1. When was the evidence collected?
2. How was the evidence collected?
3. Where was the evidence collected?
4. What types of evidence were collected?
5. Who handled the evidence before it was collected?

If no answer to one or more of these questions can be provided, the evidence may be inadmissible.

Issues related to admissibility of evidence collected through social networking platforms

If social networking evidence is collected without authorization or is unreliable, it would be considered inadmissible. The authorization to gather social networking evidence usually takes the form of a warrant (i.e., a specific type of authorization issued by a governmental institution) or a subpoena (i.e., is a legal document obliging a natural or legal person to produce evidence). After the warrant or the subpoena is submitted to the operator of a social networking platform, the operator becomes legally obliged to provide the requested evidence. Most social networking platforms have clearly explained what type of warrants and subpoenas they will consider. For instance, Facebook has published a web page “Law Enforcement & Third-Party Matters” which contains information on how law enforcement authorities and third parties may seek records from Facebook.

To be admissible, social networking evidence must not only be collected with authorization but also reliable. Therefore, a photo posted on a social networking platform may not be reliable evidence if the photo is unclear.

Ethical issues - Examples of ethical issues include (1) obtaining evidence by sending a friend request to an unknown person and (2) obtaining evidence by befriending the person whose evidence will be collected, among others. In U.S. civil litigation, evidence may be admissible even it was obtained unethically. However, some U.S. courts reserved the right to exclude evidence obtained in violation of ethical rules.

Persons who gather evidence in an unethical way risk not only excluding the evidence but also receiving punishments for violation of various ethical rules. For example, the professional rules governing the conduct of attorneys in New York State stress that: "Although a lawyer is not a moral advisor as such, moral and ethical considerations impinge upon most legal questions and may decisively influence how the law will be applied." Therefore, a lawyer who collects evidence in an unethical way may be sanctioned by the bar organization which regulates lawyer's conduct.

III. Copyright issues related to Net

The term "copyright" can be defined as "the exclusive right of the author or producer of a literary, scientific, or artistic work to publish and reproduce it." (Kraak and Ormeling, 2011, p. 182) The copyright issues arising related to NET can be categorized into the following three categories (See Fig. 3):

1. Unlawful use of user-generated content created by NET;
2. Unlawful publication of copyright content on social networks; and
3. Unlawful collection of copyrighted content from social networks.

The first category encompasses the unlawful use of user-generated content created by NET in general. Such issues may arise, for example, from the unlawful use of copyrighted photos taken by wearable devices (e.g., Google Glass and smart watch). Under the Berne Convention for the Protection of Literary and Artistic Works, an international copyright treaty applicable in more than 160 countries, copyrights for creative works are automatically

in force upon their creation. Hence, anyone who copies or distributes digital content taken by NET will probably infringe the copyright law.

The second category includes issues related to the publication of copyrighted content (e.g., videos, photos, and text) on social networks. In some cases, the publication of such content may fall within the scope of the "fair use" doctrine. "Fair use" is a legal doctrine that permits limited use of copyrighted material without obtaining the permission of the copyright holder. In the United States, examples of "fair use" may include, without limitation, criticism, parody, news reporting, commentary. If the person who posted copyrighted content on social networks cannot prove that the "fair use" of content, he/she will be liable for a copyright infringement.

The third category covers issues related to the unlawful collection of copyright content from social networking platforms. For instance, such issues may arise from the use of data mining technologies which automatically collect a large amount of copyrighted user-generated content posted on social networking platforms.

- **Unlawful use of copyrighted user-generated content created by NET**

User-generated content can be defined as content created by the users of online services. Examples of user-generated content include: (1) advertisements, (2) audio, (3) blogs, (4) chats, (5) forums, (6) pins, (7) podcasting, (8) posts, (9) tweets, (10) video, and (11) wikis.

Under the laws of most countries, authors automatically obtain the copyright in their user-generated content upon its creation. The authors do not need to (1) assert the copyright in the user-generated content (e.g., by adding the © symbol) or (2) register their copyrighted content (e.g., by using the services provided by the United States Copyright Office).

- **Unlawful publication of copyrighted content on social networking platforms**

The publication of copyrighted content on social networking platforms without the permission of the copyright holder constitutes a copyright infringement unless such a publication falls within the scope of the "fair use" doctrine. However, there is no a clear-cut line between fair use and copyright infringement. Therefore, the users willing to post copyrighted content on social networking platforms need to consult an intellectual property lawyer before the publication of such copyrighted content. Otherwise, they may be liable for

a copyright infringement. The sanctions for a copyright infringement include, without limitation, fines, and imprisonment.

- **Unlawful collection of copyrighted content from social networking platforms**

The unlawful collection of copyrighted content from social networking platforms constitutes a copyright infringement unless such a collection falls within the scope of the "fair use" doctrine. The automatic collection of a large amount of data from social networking platforms may constitute a severe copyright infringement, punishable by fines and imprisonment.

IV. Patent issues

The term "patent" can be defined as: "an exclusive right or rights provided by a government to an inventor for a certain period of time in exchange for the public disclosure of an invention" (Dimov, 2013). Since most NET are software-based, in this section, we will focus on software patents.

Software patents are a controversial topic. While some countries prohibit the grant of software patents, others allow inventors to receive patents for software. Interestingly, the proponents and the opponents of software patents use the same reasoning to justify their position.

More specifically, the proponents of software patents argue that the prohibition of software patents will "stiff" innovation because the inventors would not have an incentive to invest in software which cannot be protected by a patent. The opponents of software patents argue that software patents "stiff" innovation because the owners of the software patents use them against start-ups which do not have enough financial resources to defend their inventions in court.

Software patents all over the world

Most countries place limits on the patenting of software. However, those limits differ amongst the countries. For example, the European Patent Office does not grant patents for computer programs or computer-implemented business methods that make no technical contribution. In the same vein, the United States Supreme Court stated in Alice Corp. v. CLS

Bank International that: "*merely requiring generic computer implementation fails to transform [an] abstract idea into a patent-eligible invention*."

Although most countries impose limits on patenting software, software patents have been widely granted. A large number of software patents cover NET. For instance, on February 23, 2010, Facebook was granted US Patent No. 7,669,123, which discloses a method for dynamically providing a news feed about a user of a social network.

Software patents in the United States

The United States patent law does not explicitly mention software patents. Hence, the patentability of software invention has been addressed by courts. The history of the United States patent law started with the adoption of the U.S. Constitution. Article I, Section 8 of the U.S. Constitution states: *"The Congress shall have Power (...) to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."* Since the software patents appeared in the 20th century, the U.S. patent law had to be expanded to address such patents. The expansion was done by the U.S. courts in a large number of court decisions. The cases Bilski (Section 5.2.1) and (2) Alice (Section 5.2.2) are two of the most important U.S. cases related to software patents.

- **Bilski case**

Prior to Bilski case, an invention was patentable only if: (1) an invention is implemented by a particular machine or (2) an invention transforms an article from one state to another. In the Bilski case, the U.S. Supreme Court stated that an invention can be patentable even if it is not implemented by a particular machine or transforms an article. Thus, the U.S. Supreme Court opened the door to software patents, including software patents related to NET. The case Bilski resulted in a flood of patent applications for various types of software. Further, the case put the U.S. Patent and Trademark Office (USPTO) in a difficult situation because the USPTO was left without guidelines on the patentability of inventions failing to comply with the "machine-or-transformation" test.

- **Alice case**

In Alice case, which follows Bilski case, the U.S. Supreme Court stated that the implementation of abstract ideas on a computer **was not enough** to transform the ideas into patentable subject matter. Therefore, the Alice case resulted in a significant drop in the number of U.S. software patents. Federal Circuit Judge William Curtis Bryson explained the post-Alice drop in the number of U.S. software patents as follows: *"In short, such patents, although frequently dressed up in the argot of invention, simply describe a problem, announce purely functional steps that purport to solve the problem, and recite standard computer operations to perform some of those steps. The principal flaw in these patents is that they do not contain an "inventive concept" that solves practical problems and ensures that the patent is directed to something "significantly more than" the ineligible abstract idea itself. "*

The future of software patents

There has been an increase in the number of countries which seriously limit the patentability of software. For example, in the United States, such a limit was set by the Alice case in 2014. In New Zealand, computer programs were excluded from patentability in 2013. Similarly, in Germany, the German Parliament adopted in 2013 a motion "against the growing trend of patent offices to grant patents on software programs." In the future, we can expect more and more countries to restrict the patentability of software.

Emerging technologies regulation: the lawfull challenges.

Traditional regulatory structures are complex, fragmented, risk-averse, and adjust slowly to shifting social circumstances, with various public agencies having overlapping authority. On the other hand, a unicorn startup can develop into a company with a global reach in a couple of years, if not months. For instance, Airbnb went from startup in 2008 to a Silicon Valley unicorn in 2011 valued at a billion dollars, based on USD112 million invested by venture capitalists.

Emerging technologies are multifaceted and transcend national boundaries. Since there are no global regulatory standards, coordinating with regulators across borders is a challenge.

There are three key challenges in regulating emerging technologies:

(i) the unpredictable nature of business models that rely on emerging technologies;
(ii) data privacy, security, ownership, and control; and
(iii) the AI conundrum

Emerging technologies present new challenges for the law. Legal concepts developed when lawyers wrote by sputtering candles may not hold up well against the glare of modern lights. Yet, while many things change, other things stay the same. This chapter considers some of the most important technologies of today and tomorrow, and how they could interact with the law:

- user content;
- artificial intelligence;
- inkless, paperless, presence-less signing;

1. User content

It is popular to solicit user content as a means of getting eyeballs on a site or product to earn advertising revenue, or even to develop ideas for a product. This can take the form of online web pages inviting contest entries, review functionality, or even merely allowing user comments on a post. The virality of content can have an outsized commercial and even cultural impact compared to the expense needed – one only needs to consider the ship almost named ‘Boaty McBoatface’ as a result of a public poll held online by the UK’s Natural Environment Research Council.

However, using user content raises very real legal concerns, ranging from ownership of intellectual property to potential civil lawsuits. The necessary implication of permitting external content generation is that there is some loss of control.

2. Artificial intelligence

A self-driving car fails to ‘see’ a truck blocking the road, and collides with it at high speeds, shearing off the roof of the car and killing the human occupant. A supercomputer running automated trading systems raises the value of a portfolio to US$2.5 billion, then racks up losses resulting in a net loss of US$22 million. These stories are not the stuff of

fearmongering technophobes, but actual incidents with very real legal and financial implications, quite aside from the cost in human life.

In the first case, an operator of a Tesla vehicle had activated the car's self-driving system and was travelling at over 100km/h. The system failed to detect a white semi-trailer truck and drove into it. This was the second incident of its kind.

In the second case, an investment fund MMWWVWM Limited (VWM) entered into a contract with a Monaco-based investment firm, Tyndaris SAM (Tyndaris). Tyndaris promised an artificial intelligence (AI) managed investment account, running on a supercomputer capable of applying 'machine learning' to market and social media data, to make emotionless, bias-free decisions. Tyndaris represented that the system had been extensively tested. While initially promising, it quickly lost staggering sums of money. VWM wanted out and claimed for the losses, while Tyndaris claimed for unpaid fees for the use of the system.

In dealing with any AI system, whether as end-user, retailer or developer, there are myriad snares to catch the unwary. We briefly discuss the vexed question of pinning legal liability onto a person when an AI goes awry, and provide suggestions on steps that can be taken by persons dealing with AIs to protect their legal interests

3. Digital signatures and virtual signings

The death-knell of wet-ink signatures has been prophesised for years, but it seems that even covid-19 cannot quite bury this creature. While there are online signing solutions aplenty, there are a number of risks that are unique to such 'contactless' signing of agreements or other documents.

Signatures prepared on an electronic device can broadly be separated into two categories: 'electronic signatures' and 'digital signatures'.

The difference between the two is not just cosmetic. From a technological standpoint, these are very different, requiring different levels of technology to implement. From a legal standpoint, secure electronic signatures are also able to benefit from certain presumptions about authenticity and authorship.

1. Electronic signatures

- When asked what an electronic signature is, most people would point to an image of a traditional wet-ink signature inserted above the signature line in a document, where one would otherwise sign by hand. However, this is not the only form of an electronic signature recognised by the law in Singapore.
- Broadly speaking, the term ‘electronic signature’ can be used to describe any process that indicates acceptance of an agreement or confirmation of the contents of the document.
- Under Singapore’s Electronic Transactions Act 2010 (2020 Rev. Ed.) (ETA), a requirement for a signature can be satisfied through electronic means where:
- a method is used to identify the signatory and to indicate the signatory’s intention in respect of the information contained in the electronic record; and
- this method is as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in light of all the circumstances, including any relevant agreement; or proven in fact to have fulfilled the function above, by itself or together with further evidence.

2. Digital signatures

- Digital signatures are quite different. Using methods such as asymmetric cryptography, hashing functions, and certification from global authorities, these ‘signatures’ are tied to a document and serve as an assurance as to the authenticity of the contents of the document. These can give the recipient of the document a high level of assurance that the document is indeed from the person or entity that it purports to be sent from, and that the contents of the message or document have not been altered or modified.
- However, what this method gains in security, it loses in ease of usage. While an electronic signature can be easily added with rudimentary word processing programs, creating and verifying a secure electronic signature requires specialised software. Fortunately, many document processing solutions now have such software integrated into their functionality.

Conclusion

This paper discussed four categories of legal issues related to NET (i.e., privacy issues, issues related to gathering evidence, copyright issues, and patent issues). These issues can be overcome to a large extent by a joint cooperation between private organizations and governments. The role of each of these two actors for overcoming the aforementioned issues is explained below .The role of government for the development of NET. The governments can enhance the development of NET in two ways, namely, (1) by funding research projects falling within the scope of NET and (2) by adopting regulation of NET which complement the industry self-regulation.

In dealing with cryptocurrencies, it would be prudent to take all available steps to protect oneself, since the legal position is less clear than one would like. For instance, one can choose to deal only in established cryptocurrencies with a visible, capitalised entity that is backing it, and ensure that there are contractual rights against this entity that address the specific risks that the cryptocurrency is being used for (e.g., Byzantine faults, Sybil attacks, forks, or fraud), to have a cause of action against an entity of means. If one has sufficient bargaining power, it may also be desirable to agree on liquidated damages clauses, which could grant certainty by fixing the quantum of damages ahead of time.

As with many new technologies, the law surrounding cryptocurrencies is still in flux. However, the legal issues and commercial realities ultimately have not changed all that much. Businesses and investors alike have the same concerns: what is the nature of the ‘product’ they are trading in, who is responsible when things go wrong, and how are they protected when things go wrong? While it appears that we must wait for definitive pronouncement on these issues, parties dealing in cryptocurrencies should be prepared for protracted, expensive and possibly futile disputes if inadequate risk-management measures are not taken in time.