International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-2, December 2020

Adaptiveness of Traditional Judicial Systems to Digital Forms of Evidence

Banipriya Mishra, Supriya Mishra

Abstract*: *"Digital India" scheme announced by current administration initially had many detractors. But with its finger on the correct pulse of Young, Emergent India, much facilitations were provided with the sole aim to bridge technology with the masses. Hence today smart phones, laptops and computers have become house-hold names even in previously inaccessible areas. But on the down-side we also see a severe increase in crimes committed using computers and internet. Technology is an ever-changing phenomenon. It keeps changing, updating and even reviving itself. Crime has parallelly evolved with the evolution of newer technologies and high-end equipments and tool. With the metamorphosis of criminal-activities from physical world to digital realm, a perpetrator can easily plan, execute and accomplish a crime without being actually physically present at the site of crime, thus making it difficult for investigators, law enforcement officials and traditional legal systems completely depending on physical evidence to recognize the real culprit or to determine guilt and decide the degree of punishment. Using a desktop system or a laptop or even a Smartphone, the criminal can exploit the power of internet, Bluetooth ,Wi-Fi technologies , 4G data-transfer speeds and web-servers to execute an unlawful act sitting miles away from the place where the actual crime happens thereafter leaving absolutely no physical trail of the execution of the offence. Under these conditions, it becomes imperative to utilize digital footprints as they are the only way to determine the factuality of execution of an unlawful act and to identify the real culprit. As the guiding principle of IPC goes "Innocent until proven guilty", digital footprints have to be given their rightful due in the existing Judicial system to help in confirming execution of an unlawful act, detecting the actual culprit and determining the amount of punishment. This paper attempts to highlight the significance of digital footprints and usage of the same by the existing Justice Systems to corroborate, attest and substantiate the execution of an unlawful act.

Keywords: Digital, Footprints, Justice, crime, real, culprit, internet, world-wide web, dark-web.

I. INTRODUCTION

Globalization essentially revolves around the various contradictions which are viewed amongst the approach process of different communities towards a particular subject in question. It is frequently referred to as a set of contradictory processes consisting of both flows and counter flows; efforts to open up the world for trade, production and consumption go hand in hand with measures to constrict this through fences, borders and other types of barriers[11] Simple descriptions of globalization tend to run as follows "Globalization refers to the growing interconnectedness and integration of people, goods and finance" [2]

"Innovation" in information and technology is easily framed within a narrative of advancement: users now have Skype, Face book and Twitter to allow us to stay connected and informed. Information Technology ostensibly serves as the antidote to isolation and ignorance. A plethora of websites including Amazon and PayPal allows us to run our household to a large extent online. No more queuing up at post office as our affairs are sorted swiftly and effortlessly online. Finally through dedicated websites and chat rooms we find new friends, soul mates or a support network way beyond our street, village or country. The story here is that Information and Technology has enhanced our life beyond compare; a story of advancement and achievement[3] It has thus forayed to the initiation of the term "digitalization". Digitalization has majorly evolved around the last quarter of the 20th Century throughout the globe. The proliferation and integration of computers into every aspect of economic activity and society has inevitably resulted in a growth of criminality involving computers. The computer may constitute the instrument of the crime, such as in murder and fraud; the object of crime, such as the theft of processor chips; or the subject of the crime, such as hacking and distributing viruses. Though there has been a significant development in the field of computer technologies across the globe but the legal fraternity is still struggling to demarcate the boundaries for keeping a check over the upsurge in crimes committed by usage of digital techniques and devices. "Internet" is now holding an extremely dominant position as an environment facilitating connectivity between computers across the globe regarding any discussion about computers and their usage as the "network of networks". Thus with the rise in usage of internet the issues about commitment of crime by using computers as a medium has also increased[4]. The law enforcement officers all around the globe majorly confront with the problems which are technical, legal, operational and jurisdictional in nature which can be tackled by the conjoined mutual efforts

Revised Manuscript Received on December 25, 2020.
* Correspondence Author
Banipriya Mishra*, KIIT School of Law,KIIT University, Bhubaneswar, Odisha , India . Email: banipriya.mishra@gmail.com
Supriya Mishra, Lecturer in Information Technology, Skill Development & Technical Education Deptt, Government of Orissa, Bhubaneswar, Odisha , India. Email: supriyamishra8@gmail.com

[1]Globalization and the challenge to criminology –Edited by Francis Pakes – Routledge –Edition -13, Chapter – 1 Globalization and Criminology An agenda of engagement
[2] (Held , 1995)
[3]Globalization and the challenge to criminology –Edited by Francis Pakes – Routledge –Edition -13, Chapter – 1 Globalization and Criminology An agenda of engagement

[4] Oxford 6th edition – Computer Law – The Law and Regulation of Information Technology – Chapter 12- Computer Crime and Information misuse – Ian Walden

of all the countries simultaneously in dealing equitably with the crimes committed by usage of "network environment". Crimes committed through the usage of digital devices have thus become a cross border country crimes with no universally accepted norms and regulations attached to them which is helping the cyber offenders to carry on their illegal activities without any hindrance giving them vent to target maximum people around the globe with minimum expenditure and just a mere clicking of a button.

II. EVOLUTION OF TECHNOLOGY

Technology is so much amalgamated that it has become very difficult for every individual to live off the framework. The evolution of technology has minimized the communication gap between people who are digitally integrated through various digital communication modes giving way to formidable digital footprints to be left behind as trail of evidences for any given momentary activity of an individual.

In Penderhill Holding Limited ao v Ioannis Kloukinas, Civil Appeals 319/11 and 320/11, 13 January 2014 case The Supreme Court at Penderhill , England has clarified that the courts must be propitious in response and adhere to the technical changes that are taking place in the society.

A. Digital Systems

"Modern technology makes certain crimes easier to carry out than ever before, indeed there are certain crimes that exist now that were not possible before computers became generalized to the world population"[5]

The offences committed by usage of "Internet" can generally be categorized into three categories. They are as follows [6]

i. The first category is traditional type revolving around crimes committed using computer as an instrument of crime, referred to as "Computer – related crimes", such as fraud.
ii. The second category concerns "Content – related crimes" where computers and networks are the instrument, but the content itself is illegal such as infringing intellectual property and certain forms of pornography.
iii. The third category is offences that have been established to specifically address activities that attach the integrity, confidentiality and availability of
iv. computer and communication systems such as viruses and other malware referred to as "Computer integrity crime". It is this final category that is most often considered as Computer crime in the public's mind.

"It is thus obvious that computers now play a vital part in the Commission of nearly every form of criminal activity from fraud to murder"[7]

In order to access digital information from the target computer system, the investigators would need owner permission. If they wish to gather the information from the source computer they will need a warrant. Cops plan to use data from IoT devices to prove or disprove alibis, as well as for crime scene investigations. "The crime scene of tomorrow is going to be the Internet of Things," Mark Stokes, Scotland Yard's head of digital, cyber and communications forensics unit as told the Times. According to his reports IoT devices will play a major role in crime scene investigations and the police personnels are being trained to look for "digital footprints"—IoT gadgets that "track or record activities" which will help in proving or disproving alibis and witness statements, as well as the record what occurred during a murder victim's final moments. "Wireless cameras within a device such as the fridge may record the movement of suspects and owners. Doorbells that connect directly to apps on a user's phone can show who has rung the door and the owner

B. Digital Data

Data, as per layman is basically a collection of numbers or letters or a mix of both. But which has the potential to quantify anything ranging from simple statistics to behavioural patterns. Data refers to a collection of organized information that has been collected or gleaned from experience, observation or experiment or a set of ideas. Data may consist of numbers, words or images that represent values of a variable (i.e., a measurable characteristic of an individual or a system that is expected to vary). Primitively data was mostly numerical and used in gaining statistical insights for framing of better convenience for the work force. As computing machines evolved from Abacus to difference engine (Charles Babbage) to the desktops , data also evolved from a mere collection of numbers to a treasure house of details which if analyzed properly had the potential of arming the person in possession of this data with the power of foresight into environmental changes in any business, or research or transaction. As desktops made way for laptops, palmtops, ipads and mobile phones the face and power of data also changed. Modern day computing increased the power of data by leaps and bounds. Data today can provide insight into behavioural characteristics and usage patterns at a societal level. Internet, though initially developed for exchange of information between scientists and researchers located at four different campuses of a university, slowly grew its wings to encapsulate the world population. Article 1(b) of the Council of Europe Convention on Cybercrime (2001) in Budapest (hereafter Budapest Convention) defines computer data as any representation of facts, information or concepts in a form suitable for being processed on computers. The Article 2 of the United Nations Commission on International Trade Law's (UNCITRAL) Model Law on Electronic Commerce with Guide to Enactment[8], which uses "data" and "data message" instead of the terms "electronic evidence" or "digital evidence"[9]The accurate use of terminology in search and seizure warrants in line with enabling legislation is supported in the case of Heaney v S[10], where the ruling was that the description of a suspected crime should be accurately described in line with the enabling legislation, and colloquially used terms should not be applied. The Electronic Communications and Transactions Act describes "data" as the electronic representation of information in any form, and

[5]From Digital Footprints to Digital Journeys, How AI-Powered Analytics Surfaces Insights May 26, 2019 By: Anastacia Ezrets - Cellebrite Analytics Product Manager
[6] Ian Walden ,Computer Crime and Digital Investigations (OUP , 2007)
[7] Ian Walden ,Computer Crime and Digital Investigations (OUP , 2007)

[8]United Nations(UNCITRAL Model Law)
[9]SALRC Issue Paper 27 32
[10]Heaney v S 2016 ZAGPPHC 257 (19 April 2016)

"data messages" as data generated, sent, received or stored by electronic means. But in Part 2 of the UNCITRAL Model Law on Electronic Commerce (1996) it is stated that the concept of data messages is not intended to be limited to communication, but should include computer records and all types of messages that are generated, stored or communicated in a paperless form[11]. But, the definition of "data" is adapted from section 1 of the Electronic Communications and Transactions Act as is "the digital representation of information in any form", and not the "electronic representation of data in any form". Digital devices namely smart phones , computers ,laptops , tablets , phones , printers , smart TVs and devices having a memory capacity which is digital in nature , certain external storage devices such as external hard drives USB flash drives, servers, network components like routers, network devices and clod (which enables storage of data " at multiple data centres in different geographic locations"[12],) are usually used for storage of data which can be obtained in the form of "content" and " non content data" when required to be produced as electronic evidences during judicial proceedings. "Content" comprises of the words used in written communications, the audio files like the texts exchanged through email correspondence, videos, instant messaging systems and social media messages and the "not content" data comprises about the location and identity of individual user and any form of electronic transactional data such as data and information about senders and receivers of users using telecommunication services and varied form of electronic communication services.

C. Evolution Of Internet

Internet

Internet is a group of networks that are physically interconnected and able to act as a single network capable of data communication and information sharing.

The three main characteristics of internet are

(i) Inter operable

(ii) Packet switch

(iii) Data network

History of Internet

Department of Defence Advanced Research Projects Organization (ARPA) created an experimental network ARPANET which originally connected four Universities in 1969.NCSA (National Centre for Super Computing Application) developed TELNET application for remote login in 1972. In 1973 File Transfer Protocol (FTP) was developed to standardize transfer of files between interconnected computers.

Between 1982 and 1983 the desktop computers were developed which were equipped with UNIX that facilitates easy connection to internet through TELNET. The TCP / IP (Transmission Control Protocol / Internet Protocol) suite of protocols was established as the standard protocol on the ARPANET which resulted in using of the term **internet**.TCP/IP is the set of protocols which break data into small packets that facilitates transportation over the internet , specifies the address of the recipient manages actual transfer of the data , verifies the receipt of the data at the recipient end and finally reconstructs the data using all the packets at the recipients end .IP is responsible for data transmission from one node to other and TCP is responsible for verifying correct delivery of data from client to server ie to detect errors and trigger retransmission until the data is completely received. To keep military and non-military networks sites separate the ARPANET was divided into ARPANET and MilNet. National Science Foundation (NSF) connected America's six supercomputing centre together to form the NSFNet which supported the development of smaller networks in order to access the internet in between 1985-86. In 1987 National Science Foundation (NSF) awarded a grant to merit network incorporated (INC) to operate and manage the development of NSFNet in collaboration with IBM and MCI.In 1989 the backbone network (NSFNet) is upgraded to T_1 which means data can be transmitted at the speed of 1.5 billion bits per second. In 1990 the ARPANet was dissolved .In 1991; GOPHER was developed at University of MINNESOTA .It provides a menu based method for locating information on the internet. In 1993, European Laboratory for particle physics in Switzerland (CERN) released the World Wide Web (WWW) developed by Tim Berners -Lee which used HTTP and hypertext . In 1993, NSF Net was also upgraded to T3 which means data can be transmitted at the speed of 45 million bits per second. In 1993-94 graphical web browser Netscape Navigator and Mosaic were developed. In 1995 NSF Net is replaced by a new architecturecalled vBNS (Very High Speed Backbone Network System) which utilizes network service provider and network access points(NAP).

Architecture of the Internet

Web physically consists of host computers containing web browser software and connection to the internet service provider, servers that contain web pages, files and digital data and router and switches to direct the flow of information. The web is a client – server system. A network is basically defined as a group of computers which can communicate with one another either though wired or wireless medium. A host computer normally has a NIC (network interface card) that connects it to the LAN of the organization .This LAN is then connected to the ISP using high speed telephone lines. ISPs connect to larger ISP and the largest ISP maintains fibre optic backbone for an entire country or region. Backbones around the world are connected through undersea cables, fibre optic lines or satellite networks. Therefore it is said that every computer on the internet is connected to every other computer on the internet.

Functioning of Internet

- First we open the web browser and type the address or Uniform Resource Locator (URL) of the website which we access
- The host computer that is the computer which we use to type the URL, requests the web page from the web server that hosts the site.
- The server locates the requested web page and then sends it to the host computers over the internet.
- Finally, the web browser on the host computer interprets the data and displays it on the computer screen.

[12] UNODC, 2013,p.xxv

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

- Therefore Client – Server describes the relationship between two computers on the internet in which one computer that is the client requests for a web page from another computer ie the server which fulfills the request.

III. AFTEREFFECTS OF TECHNOLOGICAL EVOLUTION ON CRIMES AND DIGITAL FOOTPRINTS

"The Common Man" with its introduction to the world of internet though the usage of electronic and digital devices has paved way for them into a new virtual world of information about anything and everything in the eternity at large by just a single swiping or clicking of a button. Virtual world has become a new reality today, the importance of which is gripping over the need of water today. Today, the economic success of a country revolves around on the efficient transport, communication and information linkages and systems. Technologies have also revolutionized consumer behaviour and conventional services. Thus due to Internet, the range of service activities that can be digitized and globalized is expanding, from the processing of insurance claims and tax payments, to the transcription of medical records, to the provision of education via online courses to the expansion of export services.Smartphone tools and apps today proactively provide citizens with useful contextualized information, while supercomputers are able to query vast quantities of unstructured data and suggest solutions to more complex problems. Using magnetic sensors, real-time updates on traffic flow are transmitted, with simultaneous data analysis making second-by-second adjustments possible to avoid bottlenecks.[13] This kind of digital crowd sourcing of information is being applied to virtually every aspect of local governance, and a step-change in the effectiveness of these tools are adding to the potentiality of e-governance and "smart city" innovations, enabling them to shape systems that serve the need and wants of "The Common people" globally and their priorities. We live in a time of information abundance. Dangerous Knowledge – Unwitting or intentional misuse of "information" by State and Non-State Actors is an inescapable peril of our time [14]. Which is helping the criminals in keeping one now step ahead of the police by ensuring they leave no digital footprints behind [15].Digital Footprints extracted from the trails left behind by an individual while surfing internet contains raw data and information about the needs and wants of a him the analysis of which if done smartly gives businesses enough insights to advance services and products as well as personalised and adjusted advertisement that saves time and money. Thus, benefits from behaviour prediction do not stop on fighting crime, but is extended to customer experience for its improvement. "The most striking fact about crime today is who—or rather what—is committing it. It's not people that are committing the crime anymore. Crime has become software. It's crime ware," he writes. Therein lies the danger, not only for the police, but also the public at large"[16]

Thus, as been said above "no one is left behind" the digital age, has virtually made it impossible to avoid leaving a trail of highly sensitive data. Our information is saved not only on our personal laptops and phones, but also on the servers of the companies with which we interact.Every click we make online is recorded and sent through the third parties and are stored on the servers to which Internet has no other alternative. This means that all the data and information uploaded online is saved and is assessable to anyone at large. All our messages, pictures, posts, bank details, documents, location, interests and a lot more can be viewed, gathered, analyzed and used without us noticing it. As in case of **Bates v Post Office Ltd (No. 3) [2019] EWHC 606 (QB)** where the court has enunciated that without emails, notes and records supporting the claim , the chance of success stands next to impossible in which the court had favoured a group of post master and mistress against the Post office as the formal documents found were confusing and contradicting in nature without any relevancy in it leading to the rejection of Post Office witness statements based on human memory . The social media platform has connected almost half of the entire global population enabling people to make their voices heard and for helping people to converse with one another across the world in real time. However, it is also being used to reinforce and support prejudices and for spreading of cacophony, through hate speeches and by spreading of misinformation bringing about public discord giving vent to fragmentation of the societies and communities at large [17] Social media has affected relationships leading to divorce litigation seriously and effectively. A Lawyer to use a digital footprint in the form of social media evidence has to keep in purview and need to have a strong understanding about its admissibility during the judicial proceeding and the legal precedent to be met upon after it. Like in United States social media platforms are being admitted in the Court of Law given that they are not procured illegally. As in the case of **JessicaLaLonde v. Adam LaLonde, No. 2009-CA-002279-MR, 2011 WL 832465 (Ky. Ct. App. Feb. 25, 2011)** where the Court of Appeals of Kentucky has accepted the photos tagged in Face book as evidence while deciding a child custody case where to prove the wife being alcoholic the husband in question had produced the same as evidence to which the court had given its consent quoting that "tagged or being identified in the photograph" does not requires her permission as per the law but her actually being depicted in the photos accurately reflected her to be drinking alcohol which was sufficient enough for the proceeding to meet the standard of accepting and authenticating it. But in Florida post on social media are used in the Court of Law as evidence without any hindrance. But the Courts in New York and California speaks on acceptance of digital footprints as evidences in the same sense , that the social media evidences to be produced in the court of law depends solely on the ability of the lawyer and how it would affect his client in question for a judicial proceeding to set aside equitably .[18] Technology is not only aiding criminal or negative minded people to carry out e-crimes but is concomitantly helping law enforcement officers in penetrating deep into the crimes committed pertinently in ultimately resolving it with the

[13]Wheatley, 2013
[14]By Rasmus Kleis Nielsen , Cover story – The Vulnerable Indian, India Today , November -18,2019
[15]National Police Chiefs' Council, UK chair Sara Thornton
[16] Marc Goodman puts succinctly in his book Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It

[17]https://www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html
[18]Practice Panther , https://www.natlawreview.com/article/family-law-social-media-evidence-divorce-cases?amp

criminal in question being caught , which is evident from the case of paedophile Matthew Falder – who used the dark web of the virtual world for committing 137 offences on 46 victims but was caught by the National Crime Agency as said by Lynne Owen , Director General of National Crime Agency , United Kingdom Even Metropolitan Police Commissioner Cressida Dick, UK has expressed her deep concern about the rampant increase of usage of electronic and digital devices and its effect on the society which is adding to the cephalalgy of law enforcement in dealing with the vast complex data bounded by certain legal and ethical challenges which requires immediate action as they are constantly being criticized for working in thin air to a certain extent. Technological innovation has disclosed the current legal fallacies and has laid down its unwillingness to cope up with the exponential rise and forays into technology and innovations .Thus, to cope up with the current situation the Supreme Court in United States of America has reinterpreted its constitutional laws in two cases which were steered up by the influence of digital technologies which were impacting it. In **South Dakota v. Wayfair, Inc.585 U.S. ___ (2018)** the court has provided for an overruling of its jurisprudence by granting the State Governments for collection of taxes from internet based commercial activities and

In **Carpenter v. United States No. 16-402, 585 U.S. ____ (2018)**, the court has held the law enforcement responsible for violating the fourth amendment to the United States Constitution where the collection of cell site location period of more than six months required a search warrant to which the government had answered that the Fourth Amendment cannot be applied in this case as the suspect had no reasonable expectation of privacy in information shared with a third party. The Court in the above case was not overruling the third party doctrine but was rejecting "mechanically applying" the principles laid down by the government to data and information about an individual's location generated automatically by cell phones, and digital devices which have become indispensable in current world. The issues revolving around crimes committed by using digital devices have exponentially risen and has been a major cause of worry and pose as a challenge for all kinds of stakeholders and the law enforcement professionals all around globe during the Covid -19 pandemic .The rapid pace with which the internet is making way through with its sophistication , capacity building , its speedy communication , it has provided various opportunities to the numerous players in the virtual world comprising of e-criminals, terrorists , motivated offenders, law breakers an easy opportunity to carry out their criminal activities enough to be considered as a priority for national security. The advancement in digital technologies have not only underpinned and proliferated the achievements made in accomplishing the sustainable development goals starting from ending of extreme poverty to minimizing the cases related to maternal and infant mortality , in promotion of sustainable farming to decent work and for achieving universal literacy which can make world a more peaceful , fairer and just place to live but along with it they have also eroded the security , privacy and have fuelled inequality in the society at large. Thus , we as individuals as society as organization have to make a choice about the way we will be tackling and managing with the new technologies at large which will be affecting our living either positively or negatively.[19]

IV. LEGISLATIVE OUTLOOK ON DIGITAL FOOTPRINTS – GLOBALLY

The lure of accessibility of internet worldwide through usage of digital devices has become irresistible and an individual through the virtual world can put any form of information or data or carry out any form of electronic transaction in it from any corner of the world which can be used against him in any lawsuit in case of pursuit of conviction during any legal proceeding. Some commentators have heralded the emergence of the Internet as signalling a near –evisceration of traditional choice of law analysis[20]. As users and system operators (sysops) encounter conflicts and seek to resolve disputes, they take action to establish rules and decide individual cases which may involve parties from various jurisdictions. All this creates a new form of law on a global basis which can be enforced by a combination of sysop's ultimately banishing the unruly users.

Though the legislation involving Digital Footprint is still in a nascent and in a very contradictory stage, stuck between the National security design for data security and Data privacy legislation issues, the major concern of the countries all around the globe is to work towards implementing digital footprint privacy protection law which would directly help the law enforcement authorities in different sovereign states to work effectively and efficiently in dealing with digital footprints privacy violation cases which would result in maintenance of proper balance in international data security measures.

A. Legal Acknowledgement Of Digital Footprints

The need to elevate the availability and usefulness of data for supporting in the decision-making process and for holding accountability mechanisms in a case for delivering and reporting is a part of the data revolution efforts which requires ensuring that "no one is left behind."[21] But the efforts of data revolution has been grossly misutilised by criminals or negative minded people to commit crimes easily, cost effectively and secretly, with less time consumption giving vent to the sharp rise in crimes being committed in the virtual world. The requirement of procedures to be opted by the countries nationally and internationally in managing their developmental activities both in the internet world and increase in Artificial Intelligence strategy during the current point of when geopolitical tension has increased is taking a toll on all as all the world powers are divided with their approach towards adopting it. Each country following a different view towards trade, currency, financial rule with contradictory military and geopolitical views is posing as a hindrance in bringing about common approach policy towards digital securitization design and digital privacy law to prevail. Thus "a global commitment for digital cooperation" is a key recommendation by The Secretary General's High Level Panel on Digital Cooperation[22]

[19]https://www.un.org/en/un75/impact-digital-technologies
[20] "Choice –of-Law Theory and Background" at http://www.hewm.com/choice.htm
[21]United Nations, 2014
[22]United Nations 2018
https://www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html

The law on acceptance of electronic messages was first envisaged in The UNCITRAL Model Law on Electronic Commerce (1996) (Report of the United Nations Commission on International Trade Law on the work of its twenty-ninth session[23] which dealt with the admissibility and evidentiary weight of data

messages while Article 9(1) deals with admissibility Article (2) of the same Article deals with evidential weight of data messages

According to Article 9(1) The article mandates that in any legal proceeding, the rules of evidence should not apply to exclude a data message, either, solely because it is a data message (electronic in format) (Article 9(1)(b) or ,if it is the best evidence that the person adducing it could reasonably be expected to obtain , on the grounds that it is not in its original form.[24]

The Model Law mandated the legal requirement of an original data message; this requirement would be met by a data message if it satisfies the two tests laid down in Article 13 which are

a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise, and

b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented)

The presumption as to authenticity and integrity of electronic records operates only in cases of secure electronic records which does not mean that the authenticity and integrity of other electronic records cannot be proved by adducing evidence. It is only that the presumption will not operate in such a case. The UNCITRAL Model Law did not address the question of whether the information system from which the electronic record is collected is located on the premises of the addressee or on other premises, since location of information system was not an operative criterion under the Model Law. The Budapest Convention was the first international treaty, about e-crimes committed through the use of internet and computer by bringing in proximity among prevalent national laws of countries with building in a sense of cooperation amongst them all around the globe by putting together new improved techniques and methods into investigation. The Budapest Convention, brought about in the year 2000, was the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among member nations. It provided for the criminalization of conduct, ranging from illegal accessibility of data and systems interference to computer-related fraud and child pornography. It has provided for procedural law tools to make investigation of e-crime easier and for effective securing of e-evidence in relation to any electronic crime for effective judicial cooperation.But till September, 2019 only 64 states have ratified to the convention as “the promise of cooperation not firm enough,” or that there are grounds for refusal to cooperate as world powerful countries are divided in their legislation making approach. Article 32(b) of The Budapest Convention allows data sharing and provides for transborder accessibility of data which is infringing on national sovereignty of some countries acting as the main reason for disparity among the member countries.[25]

The Secretary- General’s Independent Expert Advisory Group on a Data Revolution for Sustainable Development (IEAG) in The first United Nations World Data Forum held in January 2017 which had brought 1,400 data users and producers from the public and private sectors , policy makers , academia and civil society to delve into and tackle the emerging power of data sustainable development and has made specific recommendations for addressing the challenges which has included encouragement of innovations for filling up data gaps , mobilising the data amongst the developed and developing countries equally , andfor proper coordination among member countries with adept leadership qualities. The United Nations Development Group has issued general guidance on data privacy, data protection and data ethics amongst its member countries the purposes of strengthening operational implementation of their programmes to support the achievement of the 2030 Agenda.[26]

The Canadian Legal reform has made a controversial change in Bill C-51in 2018 making several changes to the way courts deal with sexual assaults in which a defence lawyers has to obtain the court's permission before introducing private records such as texts messages into evidence, and allows complainants to participate in the application hearing making the court proceeding time consuming and trivial in nature.

Online evidences can roughly be divided into that which is publicly available like forum postings which do not require a login to view and that which is private like face book account information but there are scope to obtain both like by firstly capturing the text of the forum posting and then requesting from the forum owner about the account details of the user whose posting it is Section -4.6.2 of Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, March 2012, Police Central e-crime unit It has emphasised upon the investigators that they should be aware of the potential issues which would upsurge while publicly capturing available data including the “footprints” which are left by an individual while assessing a website as it can alert the owner of the site about the interest of the law enforcement in it.The European Union treats the legality in digital footprint privacy as a fundamental human right mostly defeating the constitutional challenge from other legal prospects and thus stands incompatible with the legal infrastructure in United States .

As The U.S. Supreme Court has never recognized information privacy as a fundamental human right that would withstand strict constitutional scrutiny even

[23] (28 May – 13 June 1996) General Assembly, Fifty-first session , Supplement No. 17 (A/51/17) , available at http://www.uncitral.org/english/texts/electcom)

[24] Guide to the enactment of the UNCITRAL Model Law on Electronic Commerce at <http://www .uncitral.org/english/texts/electcom/ml-ec.htm>

[25]Convention on Cybercrime , European Treaty Series - No. 185 , Budapest 23-XI-2001

[26]https://www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html

though it has recognised that physical location tracking is willing to be covered as just a form of information privacy but the privacy in question ultimately rests upon the state laws and federal administrative advice (as The Federal Trade Commission) if the accurate and required digital footprint protection is not covered under federal legislation (United V. Jones , 132 S. Ct, 945 ,949 (2012). But in some places like California even though they have legal policy and strategies for digital footprint privacy protection but it doesn't provide for any sanctions for violations, rendering the legislation in question as meaningless. As in Taiwan where a written consent of an individual in question is required for collection, processing, or using of personal information categorized as sensitive through the consent exception by an individual in question along with the Electronic Signatures Act as it satisfies the requirement in electronic documents.

Generally, the usage of "digital footprint" acts as a raw material for holding accountable an e-criminal in a case committed by the usage of a digital device but the contradictory views of countries upholding data security laws which is the key concern all around the globe against data privacy protection laws is the prime cause of contention posing as hindrance for equitable legislation making .There is a current need for restructuring , rethinking and re orienting various current legal regime at the earliest as new sources of data such as satellite data – new technologies and new analytical approaches if applied appropriately can result in more efficient , agile and evidence based decision making keeping in purview the security measures of nations intact at large.

B.Usage Of Digital Forensics In Judiciary

The escalated usage of digital devices from mobile phones, to GPS connected vehicle, to usage of personal wearable devices has given vent to profusion of data and meta data by which the users leavebehind huge trail of data about their each momentary activities. When any questionable and suspicious criminal case comes into the picture which cannot be solved without the usage of digital form of evidences, the trailed data are derived through the mediation of "digital forensic" techniques and methods.

According to David Nalley, private investigator of Nalley Private Investigators has encapsulated digital forensic study into three fold process which included to preserve and record the state of digital devices which are to be produced during a course of judicial proceeding, to properly analyze the state of digital device and to provide for reporting about the important supporting factual information obtained from the digital devices in question in a case. He has explained data forensic as a scientific process imbibed to the art of data recovery process effectively.[27]

The sudden upsurge in advancement in information technology has provided for easy accessibility of information and data to the users for commencement of criminal activities which has consequently increased the role of digital forensic in fighting with the crimes committed by usage of digital devices .It has become the crux for strategising investigation process to be carried out efficiently providing the law firms and courts to develop new well thought out decisions and to think "out of the box"

Digital forensic technique is providing for in depth knowledge to understand the legal and technical intricacies involved in an e-crime which helps in tracking of IP addresses of criminals involved in committing cases connected with online frauds ,email spamming ,pornography , stalking and for tracking down of terrorists by geographical location identification through the techniques as follows-

a. Cross –drive analysis which is a form of forensic technique that helps in correlating information found on multiple hard drives
b. Live analysis which revolves around examination of computers from within the operating system using custom forensics or existing system administration tools to extract evidence.
c. Deleted files uses various types of modern forensic software having their own tools for recovering out deleted data
d. Stochastic forensics method is mainly used in investigation of data theft cases with the use of stochastic property of the computer system for investigation about the activities lacking digital artefacts.
e. Steganography is the technique which is used to hide data or information inside a picture image or a digital image.

A text message sent to someone via social media, google searches or GPS information , an individual leaves behind plenty of digital footprints which can provide plenty of ammunition in the court room for seta siding of cases as in the case of **State ofKansas, plaintiff, vs. Dennis L. Rader, defendant. Case No. is 2005 CR 498** famous as the BTK Killer, Dennis L. Radar case which was solved after the intervention of digital forensic techniques where "BTK" stood for "bind, torture and kill" and he enjoyed taunting the law enforcement officers during his killing sprees in Wichita which proved to be his fatal flaw as a floppy disk sent to them revealed his true identity which led to his arrest , for pleading him guilty ,and putting a sanction of life time imprisonment which relieved his long terrorized community.

In **People of the State of California v. Conrad Robert Murray(2011)** digital forensic played a major role in the trial of the case. It revolved around the death of Michael Jackson and Dr Conrad Murray was his personal physician and the autopsy reports revealed that the cause of his death was prescription drugs. Investigators during their investigation discovered documents on Dr Murray's computer showing his authorization of lethal amounts of the drugs prescribed and he was thus convicted of involuntary manslaughter for Jackson's death and served two years in prison losing his medical license.

Digital forensic thus revolves around the applicability of appropriate investigation and analysis techniques for gathering and preservation of digital footprints from particular computing devices in a way that it is appropriate for presentation in a court of law.

C.Usage Of Electronic Discovery In Judiciary

[27] govtech.com/em/preparedness/How-Digital-Forensics-Software-is-Bringing-CSI-Type-Work-to-Real-Life.html

Electronic Discovery is a process in which the digital data "is sought, located, secured, and searched with the intent of using it as evidence in a legal case"[28]

Electronic Discovery is primarily focused on retaining data as a matter of record (in the most cost-effective manner) in order to fulfil legal requirements to produce the digital footprint in the form of digital evidence in legal proceedings when compelled to do so by a court.

Electronic discovery has become a very important process to be followed in the entire judiciary system the functioning of which has formalized gradually. The Federal Rules of Civil Procedure (FRCP) is a set of regulations which provides for procedures pertaining to civil legal suits which is to be appropriately followed in the United States court systems It had been amended in the year 2005 for recognising the increasing support of e-discovery process in production of judgments during court proceedings and was amendment in the year 2015 for keeping up of some of the excesses legal gamesmanship which has arose due to the result of 2005 amendments[29]which has mandated attorneys to upkeep their technical knowledge and became familiar with the constant development of technologies which are impacting their practices. These changes come on the heels of a 2012 revision to the American Bar Association's ("ABA") Model rules of Professional Conduct("Model Rules") Rule1.1 adding Comment 8 for maintenance of professional competence they must "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[30]

In the case of **Franklin v. Howard Brown Health Centre, 1:17-cv-8376 (N.D. Ill. Oct. 4, 2018),** which involved claims of workplace discrimination and harassment, revolving around instant messages sent over technology provided by the employer. During discovery, plaintiff's counsel sought the production of email and text messages, but did not refer to "instant messages", and only two such instant messages were produced. It left the defendant to be forced to concede, for which U.S. Magistrate Judge Jeffrey Cole wrote, "that, at the very least, it bollixed its litigation hold—and it has done so to a staggering degree and at every turn." Which revealed that the failure to introduce defensible legal hold lead to significant punishment.

Likewise in the case of **Lawrence v. City of New York, 1:15-cv-8947 (S.D. N.Y. July 27, 2018),** involves accusations that New York Police Department (NYPD) officers had illegally searched the plaintiff's home without a warrant, injuring her, damaging her property, and stealing $1,000 in cash for which she had provided photographic evidences to which she had said that the incident was photographed by her but later she changed her version of her son having taken the photos to which the defendants requested for the smart phones used to capture the images and checked for the metadata and found that 67 out of 70 photos had been taken immediately before they were turned over to the plaintiff's lawyer , that is after two years of occurrence of the incident.

E – discovery is not restricted only to different technologies but also includes blogs, instant messages, voicemails, VOIP, etc. which is making the proactive e-discovery management very critical A strong defensible e-Discovery is the resultant of a perfect collaboration among legal and technical disciplinesspeaking "different languages", thus, the communication gap between them raises the question of bringing about appropriate production of digital footprints in the court of law.

Thus, legal acceptance of digital footprints is highly dependent on proper utilization of digital forensic technique and digital e discovery methods in foraying in accurate deduction through it. But the legislation of digital footprint though in a nascent state is to be used for data securitization purpose as privacy policy though up to a point is of great importance to an individual but can be misutilised by users for criminal activities. So we need a firm legislation system internationally to upkeep the data securitization laws intact taking into consideration the nationalities view point about it which has huge differences and making a liberal legislation to be followed internationally so that it would be accepted by every nation in the world.

V. CONCLUSION

In this paper an analysis of various judicial approaches towards digital footprints has been discussed. In this article we have tried to understand the difference in approaches raised among nations internationally with regard to digital footprints and how the views are been taken up to bring a way forward as countries are still in a crux whether to keep intact the data security regulations for crime prevention or whether to support the data rights in context of human rights which is the main cause of contention for digital footprints to be enacted equitably as the time demands. As said by Alexander Seger[31] "quickly secure electronic evidence" which requires proper adherence with production of equitable digital footprints in the court of law. It has been observed that specific legislation is yet to be developed to deal with digital footprints and there is a requirement of collaboration ofopportunities to share output in cases and investigation with other actors in common region /countries, exchange of expertise and encouraging sharing of data and information among member countriesfor dealing with crimes committed by digital devices in appropriate manner and within a time frame.[32]

REFERENCES

1. Pandey, U. S., Shukla, S. (2011). E-commerce and Mobile Commerce Technologies. India: S. Chand & Company Limited pp. 91–135.
2. Kamath, N. (2014). Law Relating to Computers, Internet & E-commerce: A Guide to Cyberlaws and the Information Technology

[28]Lawton, Stacey, and Dodd, 2014, p. 4, e Discovery in digital forensic investigations. UK Home Office. CAST Publication Number 32/14

[29]https://www.exterro.com/basics-of-e-discovery/

[30]https://onward.justia.com/2017/02/09/states-now-require-tech-competence-lawyers-mean/

[31] Cybercrime Division ,Agora Building , F-67075 Strasbourg Cedex in the Webinar held on 12June 2020on "Cybercrime and terrorism: The criminal justice response"

[32] The webinar held on 12 June 2020 on "Cybercrime and terrorism: The criminal justice response" was a joint initiative of the Cybercrime Programme Office (C-PROC) of the Council of Europe and the UN Office of Counter-Terrorism.

Act, 2000 with Rules, Regulations and Notifications. India: Universal Law Publishing Company Pvt. Limited., ch 3.
3. Sharma, V. (2011). Information Technology Law and Practice. India: Universal Law Publishing., ch. 36.
4. Globalisation and the Challenge to Criminology. (2013). United Kingdom: Taylor & Francis, ch 1.
5. Walden, I. (2016). Computer Crimes and Digital Investigations. United Kingdom: Oxford University Press.

AUTHORS PROFILE

Banipriya Mishra, B Com, LLB,LLM, MBA(Finance)and currently pursuing PhD(Law) at KIIT Deemed University,Bhubaneshwar.I had been working as a Junior Lawyer for 10 years at D.P Misra Associates from November 2009.

Supriya Mishra. B.Tech (IT)-VIT University TN, Executive MBA-IIMCalcutta& M.Tech(IT)-Utkal University with 12 years of work experience at TCSL, IBM India and currently as Lecturer(IT) at SDTE Deptt, Govt. of Orissa after having topped the PSC exam.