Unit 2: Best Practices of Cyber Law across the World

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- How cyber law is being implemented in the countries - USA, UK, Canada and Australia
- The policies and laws which are effective in creating and maintaining a safe cyber space.
- The policies and laws which are the best practices and can be inculcated in our country for reference.

1.2 INTRODUCTION

There are more than 7 billion people in this world with almost 50% on as an internet user. This number keeps on increasing exponentially, every single day. This generation can be called the internet generation and the century being the internet century. For a while we can imagine our lives without food or water but surviving without internet for hours seems impossible. Today we connect with our family, friends, peers and everyone else in the world through the internet

creating and implementing in true sense the idea of a global village without borders. World connectivity has brought about such a revolution that the post-net and pre-net worlds are entirely unrecognizable. With the increasing popularity of online activities, the rate of online crimes has also increased exponentially. While the extent and impact of these crimes vary greatly across the globe but in totality it has become a universal nuisance. From cyber bullying to cyber terrorism, newer technology is providing fertile lands for newer crimes.[23]

Understanding and having knowledge about the cyber law of various countries is extremely crucial because cyber space is not restricted to the territorial understanding of a state, rather is spread across the globe without much demarcations. It touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. cyber activities are not governed by geographical borders, which makes dealing with such crimes all the more confusing and complex and therefore, a lot of cyber-crimes go unreported. Apart from the International law and guidelines in this field, it is also important to understand how the other jurisdictions work in order to check this invisible vast omnipresent space.[24]

1.3 USA

The United States have been a prime sufferer of cyber-crime in the world. However, it has devised a very strong cyber law in place and keeps working and updating that with the very speed of technology transformation. Around sixty percent of cyber cries are filed in the USA have been convicted and sentenced. The cyber laws and privacy system of the States is arguably the oldest, most robust and effective in the world.

The Computer Fraud and Abuse Act of 1986 (CFAA), enacted into law today as United States Code Title 18 Section 1030 (18 U.S.C. §), is the primary federal law governing cybercrime in the United States. n the 1970s and early '80s, many phone phreaks and early computer hackers ran rampant through online systems unhampered by worries of legal complications. CFAA was

[23] Cyber Laws: What Have Different Countries Done <https://unbumf.com/cyber-laws-what-have-different-countries-done-to-prevent-cyber-crime/>

[24] Miguel Mendoza and Miguel Mendoza, 'Challenges And Implications Of Cybersecurity Legislation | Welivesecurity' (*WeLiveSecurity*, 2020) <https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/>

aimed at criminal offences and did not cover civil offences by then. It offered a powerful set of prosecutorial tools to address criminal uses of computer.[25]

It criminalised spreading of malevolent code, trading in passwords or other access control mechanisms etc. The act defines a category of "protected computer" to exclude and safeguard the federal interest but in theory and through princely elucidation all the computers are covered.

The Act has been amended over the years to refine the definitions and to expand coverage into other aspects of cybercrime. Between 1988 and 2008, the law was amended 9 folds. A lot of updates included mounting security to financial institutions and other private computers, including civil actions, adding tampering and attempted extortion, criminalising of taking information off of systems etc.[26]

The important provisions under this law are:

S. No.	Section Number	Act - The Computer Fraud and Abuse Act of 1986 (CFAA)
1	**1028**	**Fraud and related activity in connection with identification documents, authentication features, and information**
2	**1028A**	**Aggravated identity theft**
3	**1029**	**Fraud and related activity in connection with access devices**
4	**1030**	**Fraud and related activity in connection with computers**
5	**1037**	**Fraud and related activity in connection with electronic mail**
6	**1343**	**Fraud by wire, radio, or television**
7	**1362**	**Malicious mischief related to communications lines, stations, or systems**

[25] Kamble, R (2013). CYBER LAW AND INFORMATION TECHNOLOGY. International Journal of Scientific and Engineering Research. 4. 789-794

[26] Eichensehr, Kristen, The Cyber-Law of Nations (January 8, 2014) 103 Geo L J 317 (2015)

8	**1462**	**Importation or transportation of obscene matters**
9	**1465**	**Transportation of obscene matters for sale or distribution**
10	**1466A**	**Obscene visual representation of the sexual abuse of children**
11	**2251**	**Sexual exploitation of children**
12	**2252**	**Certain activities relating to material involving the sexual exploitation of minors**
13	**2252A**	**Certain activities relating to material constituting or containing child pornography**
14	**2252B**	**Misleading domain names on the Internet [to deceive minors**
15	**2252C**	**18 U.S.C. §– Misleading words or digital images on the Internet**
16	**2425**	**Use of interstate facilities to transmit information about a minor**
17	**2319**	**Criminal infringement of a copyright**
18	**2510-2522**	**Interception of wire, oral, or electronic communication**
19	**2701-2712**	**Preservation and disclosure of stored wire and electronic communication**
20	**3121-3127**	**Pen registers and trap and trace devices**

The Electronic Communications Privacy Act, 1986 allows the government to access digital communications such as email, social media messages, information on public cloud databases, and more with a summon. No warrant is required if the items in question are 180 days old or older.

Cyber Intelligence Sharing and Protection Act (CISPA), 2011 was reintroduced in 2015 at the Parliament as an amendment to the National Security Act of 1947. This was set up with the objective of improving cybersecurity by sharing information on potential cyber threats with the federal government.

Children's Online Privacy Protection Act (COPPA), 2012 was implemented in 2013 which mandated websites that gather data on children under the age of thirteen to conform with the Federal Trade Commission (FTC), which governs whether a website is suitable for children by reviewing its language, content, advertising, graphics and features, and intended audience.

It can be concluded that US has some pretty high levels of security when it comes to cyber safety and the cyber laws are much varied and comprehensive. the government has been working to introduce stricter laws to equip organizations to secure the data from the latest cyber threats. In conclusion one can say that USA does set a good example for cyber laws and security across the world.[27]

In the year 2014, these new legislations were introduced:

S. No.	Legislation
1	**National Cybersecurity Protection Act (NCPA)**
1	**Cybersecurity Enhancement Act of 2014 (CEA)**
2	**Federal Information System Modernization Act of 2014 (FISMA 2014)**
3	**Cybersecurity Workforce Assessment Act (CWWA)**
4	**Border Patrol Agent Pay Reform Act (BPAPRA)**

1.4 UK

The United Kingdom has been fighting issues of cyber-crime and cyber security over a lot of years. Most recently the case of ***'Cambridge Analytica'*** also dwelled around the Data Protection laws and brought about a new regulation for the European Union. In UK, there is a demarcation between two types of cyber- crimes. They differentiate between a cyber-enabled crime and a cyber-centric crime. Cyber-centric crimes are things like unauthorised access to computer systems, new crimes brought about through the existence of computers. However, cyber-enabled

[27] WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009), available at <http://www.whitehouse.gov/assets/ documents/Cyberspace_Policy_Review_final.pdf>

crimes are crimes that have always existed, but benefit from the existence of computers such as fraud.[28]

The list of significant legislations specifically for cyber-crimes is:[29]

S. No.	Legislation	Purpose
1.	**Malicious Communications Act 1988**	**It dealt with communication and its malice and offense caused**
2.	**Official Secrets Act 1989**	**It deals with national security**
3.	**Computer Misuse Act 1990**	**It specifies various hacking offences**
4.	**Data Protection Act 1998**	**It implements the Data Protection Directive 1995**
5.	**Communications Act 2003**	**It is the main source of UK telecommunications law**
6.	**Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)**	**It regulated the communication and data protection for electronic communication.**
7.	**Serious Crime Act 2015**	**It defines principles for the protection of data**

The Computer Misuse Act, 1990 (CMA) is the chief piece of UK legislation relating to offences or attacks against computer systems such as hacking or denial of service. The act left space for technological advancement and did not define a 'computer'. In ***DPP v McKeown and, DPP v Jones [1997] 2 Cr App R 155 HL,*** Lord Hoffman defined computer as 'a device for storing, processing and retrieving information'; this means that a mobile smartphone or personal tablet device could also be defined as a computer in the same way as a traditional 'desk-top' computer or 'PC'. There is jurisdiction to prosecute all CMA offences if there is "at least one significant link with the domestic jurisdiction" (England and Wales) in the circumstances of the case."

[28] GOV'T OF KENYA, CYBERSECURITY STRATEGY 12 (2014), available at <http://www.icta.go.ke/wpcontent/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf>

[29] U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 11 (2011), available at <https://www.gov.uk/government/publications/cyber-securitystrategy>

Offences under the Computer Misuse Act are tabled below:

S. No.	Section Number	Act - The Computer Misuse Act, 1990 (CMA)
1	**1**	**Unauthorised access to computer material, it involves 'access without right' along with an intention for such**
5	**2**	**Unauthorised access with intent to commit or facilitate commission of further offences**
6	**3**	**Unauthorised acts with intent to impair the operation of a computer**
7	**3ZA**	**Unauthorised acts which tend to attack the critical national infrastructure**
8	**3A**	**It deals with those who make or supply malware.**

This act has been amended twice, by the Police and Justice Act 2006 and by the Serious Crime Act 2015.

Data Protection Act 1998 creates criminal offences that may be committed alongside cyber-dependent crimes inclusive of procuring or revealing personal data, disclosure of personal data, entailing private data for selling or offering to sell it etc.

Communications Act, 2003 magnifies our understanding of our ambit of malicious and offensive communication. It also includes that when one sends through a 'public electronic communications network' a message or other matter that is 'grossly offensive' or of an 'indecent, obscene or menacing character', it is an offence. To send or false message 'for the purpose of causing annoyance, inconvenience or needless anxiety to another' is also an offence. It involves the acts of cyber bullying, cyber trolling, virtual mobbing etc.[30]

Serious Crime Act 2015 covers processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For monitoring and recording of communications in transit an artificial person must consider the act.

[30] C Matthew, Waxman Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE J INT'L L, volume 421, p 431 – 468 Posted: 2011

Certain other laws relating to this field in this particular jurisdiction are Police and Justice Act 2006, EU Directive 2013/40/EU, Terrorism Act 2000, Regulation of Investigatory Powers Act 2000, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Human Rights Act 1998, Extradition Act 2003, Crime and Courts Act 2013, Telecommunications (Data Protection and Privacy) Regulations 1999 etc.

UK is working towards betterment of cyber security and data protection each day. Presently on May 2018 the General Data Protection Regulation 2016/679 (GDPR) became directly effective in the UK and the Network and Information Security Directive 2016/1148 to be implemented in all member states of the European Union. But Brexit puts everything under much speculation and uncertainty.

1.5 CANADA

Canadian cyber laws are generally principles-based which provides organisations more tractability whilst covering the possible crimes. Canadian approach to Cyber Security is much more comprehensive with a lot of regulations being the responsibility of government agencies as well as private sectors.[31]

There are many legislations and regulations for such including Cybersecurity Best Practices Guide and a Cyber Incident Management Planning Guide 2015 launched by the Investment Industry Regulatory Organization, the Bulletin on Cybersecurity 2016 by Mutual Fund Dealers Association of Canada, Security Self-Assessment Tool by the Office of the Privacy Commissioner of Canada etc.[32]

Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) applies to the private sector to protect personal information within their possession or control. It contains implicit or explicit accountability and security obligations for personal information by federally-regulated organizations. PIPEDA was amended in 2015 was amended to ensure that any breach be reported to Office of the Privacy Commissioner of Canada. Also, the breaches have to be

[31] Eloise F Malone & Michael J Malone, "The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response" (2013) 19:2 Can Foreign Policy J 158 at 171

[32] Greg Weston "Foreign hackers attack Canadian Government", CBC News (16 February 2011), online: [perma.cc/Y4D3-QHLB]

reported and maintained. Knowledge of such crime and failing to report is also an offence under the act.

Bill C-59 Act, 2017 was introduced to enlarge the authorization of the Communications Securities Establishment (CSE). The act allowed the CSE authorities to interfere with foreign online efforts that threaten the country by shielding Canada's networks from foreign cyber threats – both defensively and actively. It would include degrading, disrupting, influencing, responding to or interfering with the capabilities, intentions or activities of a foreign actor.[33]

Canada has created the ***National Cyber Security Strategy*** ***and a National Cybercrime Coordination Unit,*** which coordinates for cyber-crime investigations in the country and partners internationally. They also provide digital investigative advice to Canadian law enforcement; and establish a national reporting mechanism for Canadian citizens and businesses to report cybercrime incidents. Moreover, the Canadian Anti-Fraud Centre mitigates public marketing fraud.

In the year 2012, the Ontario Court of Appeal acknowledged "intrusion upon seclusion", as tort in which "one who intentionally or recklessly intrudes, physically or otherwise, upon the seclusion of another or his or her private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person".

In the year 2016, the Ontario Court of Appeal acknowledged another privacy-related tort in ***Jane Doe 464533 v ND,*** in which, "one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."

Therefore, in Canada apart from considering cyber-crimes as criminal offence, through introducing such torts, the court adopted it as a civil offence too. It helped to establish that with the speeding technology, the need for recognition and laws to move equally fast is significant. Lawsuits involving data breaches also include more traditional allegations, such as claims of negligence, breach of contract and statutory breach.

[33] Public Safety Canada, National Cyber Security Strategy, (Ottawa: Public Safety Canada, 2018), online (pdf): [perma.cc/23W4-5MER] at 2

1.6 SUGGESTIONS DERIVED FROM BEST PRACTICES ACROSS THE WORLD

There is so much to learn from the various countries and practices about safeguarding our nation from cyber-crime and cyber terrorism. To help one understand, here are a few suggestions which can be implemented in India for a betterment in the cyber security world.

1. A tiered cybersecurity policy can be drafted. The written policy will act as a formal guide to all cybersecurity measures used in an organisation. It helps keep everyone on the loop and create a workflow which can be monitored and maintained ensuring that the levels of cyber security are maintained at every level and thereby in the entire organisation and consequently country.
2. Regulating and keeping a backup of data and maintaining a record of all the data is equally important to ensure that the data remains safe, unaltered and non-destroyable. Through regulations it must be ensured that this backed up data is thoroughly protected, encrypted and frequently updated. It is also imperative to divide backup duty among several people to mitigate insider threats.[34]
3. Partnership with other countries helps a lot in dealing with cyber-crimes as the boundary does not restrict such kind of security issues. If a country can partner with other countries and develop a system within themselves to ensure cyber security and protection against cyber-attacks, it will be way more fruitful than processing it individually.
4. Mass awareness to ensure that cyber-security is understood, dealt and tackled individually by each person is extremely crucial to ensure safety from cyber-crimes. Regulation for such can be drafted and trainings at large for public be done to ensure, everyone understand and follows those regulations can help a country at large.[35]

1.7 LET'S SUM UP

In this chapter, we have studied how cyber law is being implemented in countries like USA, UK and Canada. We also studied about the policies and laws which are effective in creating and

[34] Cyberbullying and the Law | MediaSmarts <https://mediasmarts.ca/digital-media-literacy/digital-issues/cyberbulling/cyberbullying-law>

[35] Remarks by Director David Vigneault at the Economic Club https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html

maintaining a safe cyberspace. Finally, we ended out discussion with the best practices that can be inculcated in our country.

1.8 FURTHER READING

- Singh, Umrav. (2016). Cyber Laws in India.
- Cyber Laws of Different Countries - Cyberlaws.Net, Cyberlaws.Net (2019), http://cyberlaws.net/cyber-law-repository/cyber-laws-different-countries/ (last visited Nov 24, 2019).
- Cis-india.org (2019), https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf (last visited Nov 24, 2019).
- (2019), https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=10766&context=theses (last visited Nov 24, 2019).

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is objective of the Computer Fraud and abuse Act, 1986?**

CFAA was aimed at criminal offences and did not cover civil offences by then. It offered a powerful set of prosecutorial tools to address criminal uses of computer.

2. **What does Canadian cyber laws mainly focus on?**

Canadian cyber laws are generally principles-based which provides organizations more tractability whilst covering the possible crimes. Canadian approach to Cyber Security is much more comprehensive with a lot of regulations being the responsibility of government agencies as well as private sectors.

3. **Why was Serious Crimes Act, 2015 introduced?**

Serious Crime Act 2015 covers processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For monitoring and recording of communications in transit an artificial person must consider the act.

1.10 ACTIVITY

Elucidate the different laws and policies introduced by other countries and how it can be implemented in India along with a reason? (1000 – 1500 words)