BAOU
Education for All

Dr. Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-203
Human Rights And Cyber Security Laws

Post Graduate Diploma in

Cyber Law

(PGDCL)

2021

Human Rights and Cyber Security Laws

Dr. Babasaheb Ambedkar Open University

Human Rights and Cyber Security Laws

Course Writer

Dr. DeeshaKhaire — Faculty of Law, Gujarat National Law University, Gandhinagar

Content Reviewer

Dr Peter Ladis — Faculty of Law, Chankaya National Law University, Patna, Bihar

Content Editor

Prof. (Dr.) Nilesh K. Modi — Professor & Director, School of Computer Science Dr.Babasaheb Ambedkar Open University, Ahmedabad

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. 2021

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Block-1: Cyber Security And Human Rights

UNIT-1
Introduction to Cyber Security And Human Rights 05

UNIT-2
International Trend In Ensuring Human Rights 11

UNIT-3
Case Study- USA 21

UNIT-4
Role of Civil Society 33

Block-2: Case Studies / Data Protection

UNIT-1
Equifax Data Breach: Case Study 41

UNIT-2
What's Up WithWhatsapp? A Transatlantic View On Privacy And Merger Enforcement In Digital Markets 48

UNIT-3
Facebook Data Theft In Indonesia 58

UNIT-4
Yahoo Data Breach 66

Block-3:Indian Laws And Cyber Security

UNIT-1
Privacy And Cyber Law 75

UNIT-2
Data Protection Bill 83

UNIT-3
Cyber Crimes And The Law: Evaluation Of The Information Technology Act, 2000 92

UNIT-4
Cyber Stalking And The Plight Of Women In India — A Legal Perspective 99

Block-4: Cyber Terrorism

UNIT-1
CyberTerrorism: An Analysis With An Indian Perspective 107

UNIT-2
The Cyber Terrorism Conundrum And 'Protected' Systems 114

UNIT-3
Countering Cyber Terrorism Effectively 120

UNIT-4
Assessing The Risks Of Cyber Terrorism, Cyber War And Other Cyber Threats 127

Block-1

CYBER SECURITY AND HUMAN RIGHTS

Unit 1:INTRODUCTION TO CYBER SECURITY AND HUMAN RIGHTS

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Adopting Cyber Security approaches which interrupt Human Rights

1.4 Applying a Human Rights Approach to Cyber Security

1.5 Privacy and Freedom of Expression

1.6 A Distributed-Governance Approach to Cyber Security

1.7 Roles of Stakeholders in Cyber security

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible Answers

1.11 Activity

1.1 LEARNING OBJECTIVES

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

- what the cyber security approaches affecting human rights are.
- how to apply human rights approach to cyber security.
- privacy and freedom of expression.

1.2 INTRODUCTION

Cyber security is the frame of technologies, procedures and practices intended to defend networks, computers, programs and data from spasm, harm or unauthorized access. Elaborately it is the defence of computer systems from the stealing and injury to their hardware, software or information, as well as from commotion or misdirection of the amenities they deliver. Cyber security comprises governing physical entree to the hardware, as well as shielding alongside harm that may come via network entree, data and code injection. Also, owing to negligence by operators, whether intentional, accidental, IT security is vulnerable to being deceived into differing from protected measures through numerous approaches. The arena is of mounting reputation due to the cumulative dependence on computer systems and the Internet, wireless networks such as Bluetooth and Wi-Fi, the development of "smart" devices, comprising smartphones, televisions and tiny devices as part of the Internet of Things. Safeguarding cyber security necessitates synchronised pains through an information system.[1]

Human rights define rights intrinsic for every human, irrespective of race, gender, ethnic group, civilization, linguistic, religious conviction, or slightly extra position. Human rights comprise the right to lifespan and independence, freedom from bondage and torment, freedom of estimation and appearance, the right to effort and tutoring, and many more. Everybody is permitted to these rights, deprived of discernment. They are usually unstated as unchallengeable fundamental rights "to which a person is integrally permitted merely because she or he is a human being". They are pertinent ubiquitously and at each time in the intellect of being universal, and they are egalitarian in the wisdom of being the identical for everybody. They are observed as necessitating compassion and the rule of law and striking a compulsion on persons to esteem the human rights of others, and it is usually deliberated that they should not be taken away excluding as a result of due procedure based on precise environments.[2] If campaigners would like to triumph in contest for detainment in the Internet permitted and exposed, resulting in progressively vibrant which becomes necessity to disseminate them familiarly through the extents of cyber safety and cyber scrutiny. Worldwide state-funded cyber intelligence is assumed in delivery of the identical chronicles of cyber conflict and a cyber weapons contest; chronicles that came to existence castoff around in a few portions within the universe to embolden inhabitants for crafting on domestic permissions because of better

[1]Paul, Subrata&Mitra, Anirban& Mishra, Brojo.(2017). Cyber Security and Human Rights.CSI Communications. 41. 34-35.

[2]E A Fischer, "Cyber security issues and challenges: In brief," Congressional Research Service 2016, 2016.

wisdom of safety. Within India, we can't imagine for the entree of cellular devices else Internet acquaintances, comprising in cyber cafes, deprived of authorised documentation, and together ISPs and cyber cafes stand compulsory for preservation thorough records comprising operators' glancing antiquity. The fate chronicles which habitually escort these actions lure additional forte after identical actual development in the extent cyber-crime – where prevails numerous viruses besides added kinds of malevolent cypher in transmission, through a million persons flattering injured by cyber-crime daily. Therefore, although cyber security hasn't been a novel anxiety, over previous ages this originated in progressively govern besides ambition in Internet strategy besides supremacy program, in addition to worldwide strategy treatise extra sketchily. Cyber security approaches requisitely intended then applied by a manner such that it becomes reliable through global human rights regulation – besides frequently this was not the scenario, by way of realised in the investigation commands. On additional arenas, States establishes for being in arrears of coercions for instance cyber-attacks intended on human rights protectors' otherwise radical antagonism. It's consequently significant being wider human rights communal twitches appealing along with dissertations extra carefully, for unloading announced intimidations in addition to the hypothetical answers then safeguard human rights values remain supported midst cyber security showground also.

1.3ADOPTING CYBER SECURITY APPROACHES WHICH INTERRUPT HUMAN RIGHTS

With usage of encumbered, vague linguistic certainly elaborates extensive significances, by way of numerous governments consume imprecise interior besides exterior fears by way of influences to defend always better savings within cyber weapons besides bulk shadowing arrangements, also eternally superior administrative resistor in Internet plus own peoples. Owing to intellect in fright entrenched by cyber security accounts partakes troubled necessity of accurately also obviously authenticate probability besides features of hazards impending. Similarly assumed growth of imprint describing replies remain suitable besides genuine. Other threatening "security" actions include evolving supposed "Internet kill switches", confining usage of encryption, realising purifying besides obstructive apparatuses then announcing actual term strategies.[3] These methods frequently stance fears towards civic authorisations, so far these incline toward absence in jurisdictive omission in addition to communal information wherein magistrate on efficacy. Whereas boomingly that these advance safety, these commonly jeopardy obliterating the assistances which Internet carries.[4]

1.4APPLYING A HUMAN RIGHTS APPROACH TO CYBER SECURITY

The hearsays of UN Distinct Rapporteur delivers decent sympathetic about what way liberty of appearance smears. "International Principles on Communications

[3]Margaret Rouse, "Cyber security", http://whatis.techtarget.com/definition/ cyber security, retrieved: November, 2016.

[4]Gasser Morrie, "Building a Secure Computer System (PDF)". Van Nostrand Reinhold. Pp. 3.ISBN 0-442-23022-2.Retrieved on 6 September 2015.

Surveillance and Human Rights", labels chief philosophies of human rights method to cyber security equally defined by a collection of municipal civilization societies, business besides world-wide specialists.[5]

1.5PRIVACY AND FREEDOM OF EXPRESSION

Though additional human rights remain pertinent, two human rights specifically leads to the formation of structure chunks in rights- regarding tactics of cyber security. First comes right to privacy, freedom in keeping everyone's information and communiqué left after predatory judgements of management, industries or extra peoples. Right to privacy becomes an essential constituent over expansion of a people specific safety strategy. Though it's inadequate still because it unconsumed the necessities aimed at existence protected operational in method being elaborated. Privacy is inhibited when someone becomes deprived of the privacy in transportations or mechanism concluded evidence around them. Over valuation in cyber security strategies identical physique willingly specified over functional pleasure with every inhabitants of the right to freedom of countenance. Additional dominant right, freedom of countenance, inhibited whenever an act averts somebody after looking for, getting or communicating somewhat appearance except those could be legally imperfect, besides movements which "anxieties", i.e. disheartens else constrains, which countenance.

1.6A DISTRIBUTED-GOVERNANCE APPROACH TO CYBER SECURITY

Though cyber threats are frequently actual, present dissertation hereby consuming a diversity of undesirable influences, affecting the Internet domination programme absent after making an available and allowing atmosphere and concerning discovery novel, and progressively federal, systems of knowledge and controller. An important characteristic of the cyber security dissertation exists in the idea of an influential besides caring Public provided that his peoples through safety, similar to the pre-Internet stage. Nonetheless this account takes a pew nervously along realism of Internet's behaviour that stands as world-wide network of evidence that is unto a great amount for indicators of private segment. Neither fears nor explanations are consequently by way of effortlessly distinct, positioned before bounded as similar to past. Through a disseminated methodology, supremacy preparations purposefully consensus numerous performers precise parts besides errands at cyber security field, nonetheless being accomplished in a manner when none solitary performers are capable of regulating this field except the others approve and cooperate.[6] The other metier of such a tactic becomes permit users to redo the distinction between the operators as an important performer in this expanse. Certainly, because intimidations remain rapidly changeable over Internet atmosphere, finest resistance will frequently be consuming knowledgeable operators can themselves undertake bright conclusions; although present governance preparations consist of slight area

[5]Nickel, James, "Human Rights". The Stanford Encyclopedia of Philosophy (Fall 2010 ed.).

[6]Anja Kovacs and Dixie Hawtin, "Cyber Security and Online Human Rights" Internet Democracy Project, Global Partners and Associates, November 2017.

for it. Totalling, in pointing multiple-layers of payments and stabilities, this tactic can be additional probable in sustenance of human rights.

1.7ROLES OF STAKEHOLDERS IN CYBER SECURITY

In talking about the multilateral and multi-stakeholder ways in which cyber security is addressed, it is important to understand what role different stakeholders play in these discussions. Ideally, governments, the private sector, civil society, and the technical community would all play equal roles in creating and implementing cyber security policies and decisions, but realistically this isn't always the case. Traditionally, governments play the primary role in creating the public policies and laws that regulate and determine cyber security measures domestically, sometimes with non-governmental input, but usually from private cyber security firms or industry. In addition, governments are also capable of launching and supporting cyberattacks of their own against other countries, and they are the only stakeholder guaranteed a say in the ITU and other international multilateral bodies. On the international stage, a handful of governments (previously mentioned) have pushed for increasing the role of governments and intergovernmental organisations in cyber security. Private sector companies, including ISPs and the IT sector are crucial because of their role in creating and maintaining the technologies (computers, tablets, etc.) on which cyber security issues arise. Governments often consult these companies when making public policy decisions in order to ensure that cyber security standards can be applied to various technologies. At the same time, the number of cyber security firms in the private sector is quickly growing, and they often profit from strict cyber security policies. Similar to private sector companies, the technical community has the technical expertise and understanding of the Internet and is often cited by governments when developing cyber security policies. The technical community, including the Internet Engineering Taskforce also works independent of governments and politically-motivated cyber security measures to help ensure the security of the Internet's critical infrastructure. Similar to other areas of Internet governance, civil society's role in cyber security has just begun to take off in recent years. On the one hand, civil society groups have pushed for further inclusion at international discussions and domestic policymaking meetings, but others are calling for civil society to create their own positive agenda for cyber security policy and norm making. Civil society has a unique role in being able to advocate for cyber security policies from a human rights-based approach. In 2011, CitizenLab developed a report outlining the possible role for civil society in cyber security, and in 2013, the Association for Progressive Communications created a similar agenda. Both reports emphasise the importance of civil society in bringing to light human rights considerations in all cyber security related discussions, but also address the need for civil society to call for evidence based cyber security decisions and practices.

1.8 LET'S SUM UP

The intention of this chapter is to highlight some key developments relating to the current climate around cyber security and human rights in order to set the stage for a dynamic and in-depth discussion.

1.9FURTHER READING

- Selma Dilek, HüseyinÇakır and Mustafa Aydın, ”Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015.
- Margaret Rouse, “Cyber security”, http://whatis.techtarget.com/definition/ cyber security, retrieved: November, 2016.
- Gasser Morrie, “Building a Secure Computer System (PDF)”. Van Nostrand Reinhold. Pp. 3. ISBN 0-442-23022-2. Retrieved on 6 September 2015.
- Rouse Margaret, “Social engineering definition”. TechTarget. Retrieved on 6 September 2015.
- James Nickel, Thomas Pogge, M.B.E. Smith, and Leif Wenar, “Stanford Encyclopaedia of Philosophy, Human Rights “, December 13, 2013, Retrieved on August 14, 2014.
- Nickel, James, “Human Rights”. The Stanford Encyclopaedia of Philosophy (Fall 2010 ed.).
- The United Nations, Office of the High Commissioner of Human Rights, What are human rights? http:// www.ohchr.org/en/issues/pages/ whatarehumanrights.aspx, Retrieved August 14, 2014.

1.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber security?**

   Cyber security is the frame of technologies, procedures and practices intended to defend networks, computers, programs and data from spasm, harm or unauthorized access**.**

2. **What are Human Rights?**

   Human rights define rights intrinsic for every human, irrespective of race, gender, ethnic group, civilization, linguistic, religious conviction, or slightly extra position.

1.11 ACTIVITY

1. Discuss about the intermingled relations between cyber security and human rights along with your opinion on the same. (1500-2000 words)

2

Unit 2: INTERNATIONAL TREND IN ENSURING HUMAN RIGHTS

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Deconstructing Cyber Security

2.4 Human Rights violation in Cyber Space

2.5 A Human-Centric Perspective on Cyber Security

2.6 Let's sum up

2.7 Further reading

2.8 Check your progress: Possible Answers

2.9 Activity

2.1 LEARNING OBJECTIVES

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

- cyber security in the International scenario
- human rights' violation of cyber space
- cyber security in a human centric perspective

2.2 INTRODUCTION

The evolution of cyberspace has had an influence on nearly every area of human life over the last two decades. Cyberspace's growth in the tempo, frequency, and variety of interactions has changed the way communities communicate, businesses provide services, and individuals are regulated. Big Data and the Internet of Things (IOT) are now having an effect on a wide variety of social events. The cyber realm is now posing an increasing range of security challenges. Critical national infrastructures are vulnerable to cyberattacks, and cyber-espionage and cybercrime pose a threat to the global economy. Worms, malware, advanced Distributed Denial of Service (DDoS) attacks, and spam have lost billions of dollars to the global economy. Cyber attacks on Estonia's online banking infrastructure and the use of the Stuxnet worm to damage Iran's nuclear program show how important cyberspace is for national security.[7] States have naturally identified cyberspace as a modern area of war in their military and security doctrines. The concept of national security dominates the electronic security conversation. This pattern can be seen in the publication of national security strategies and official reports, the creation of cyber-commands and Computer Emergency Response Teams (CERTS), the amount of money spending to protect cyberspace, and the talk of a cyber-arms race. While this policy is justified to a significant degree, it is still flawed in that it ignores the human rights of approximately 2.7 billion Internet users. The evolution of Internet filtering tactics, as well as Edward Snowden's disclosures regarding the US National Security Agency's (NSA) global surveillance program, have shown that Internet freedom, anonymity, and personal data are continuously under threat. Interception and monitoring of citizen communications are commonplace. As a result, cyber defense can not only counter challenges to the state and private sector, but also (if not first and foremost) human needs.

2.3DECONSTRUCTING CYBER SECURITY

Cyberspace has become an inseparable part of human civilization, and our reliance on its technology is becoming all the time. When addressing a contentious topic like cyber defense, the reader should keep the following in mind. First and foremost, there is no explicit understanding of what constitutes cyber defense, owing in part to

[7] Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance by Andrew N. Liaropoulos (University of Piraeus, Greece)

the lack of a widely agreed definition of cyberspace.[8] Cyberspace is a concept with a nebulous meaning that is commonly used as a synonym for the Internet or the World Wide Web. Daniel Kuehl describes cyberspace as "a global realm within the knowledge world whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to generate, store, alter, share, and manipulate information through interdependent and interconnected networks using information communication technologies," according to one common concept.[9]When it comes to cyber security, the key issue is whether one sees cyberspace as a global network involving only hardware, applications, and information systems, or as a network involving individuals and the vast variety of social activities that take place within it. The second problem is that there are several words used to characterize various facets of cyber security. Scholars and government officials frequently use terminology like information security, ICT security, network security, Internet security, and essential information technology privacy. This language encompasses a wide range of risk categories and levels in cyberspace, posing valid questions regarding the referent object of cyber protection. The fact that all of the aforementioned words take on different meanings when put in a political context adds to the semantic complexity. In each nation, the conceptions of state control in cyberspace, approaches to solving the attribution dilemma, methods of establishing cyber deterrence, and the fine line between information security and internet censorship differ. States will have diverse interests when it comes to meeting the security needs of government, business, and people in the cyber domain because they have distinct national goals and capacities in cyberspace.[10] National security interests in cyberspace may include not only combating hackers, criminals, terrorists, or other governments, but also controlling or even manipulating knowledge traffic and records, depending on the situation. The final point to consider, and one that is often overlooked, is that security was not a top priority in the early stages of cyberspace growth. Its architecture was built on the principles of simplicity and transparency rather than protection and durability.

The aim of the original design of APRANET and the subsequent information architecture was to build an open environment in which researchers could exchange ideas without being constrained by time or distance. The Internet's promise was to be a place where people could openly communicate, monitor news, and exchange knowledge and ideas. Any national security agenda should aim to provide a safe atmosphere for its people. Given the fact that modern democracies depend on the operation of ICTs, it is only natural to believe that one of the goals of any national cyber security strategy will be to provide a safe cyber environment for its people. This goal translates into the defense of vital national infrastructures in policy terms.[11] As a result, states are building offensive and defensive cyber-weapons in order to protect their cyber assets. Offense-defence theory, deterrent theory, center of gravity, arms race, and doom scenarios are all included in the related security and military doctrines. States view cyber defense as a zero-sum game because they

[8]Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and ApuKapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.ACM, Seoul, 3523–3532.

[9]Jeffrey Bardzell and ShaowenBardzell. 2016. Humanistic HCI. Interactions 33, 2 (2016), 20–29.

[10]Matt Bishop. 2018. Computer security: Art and science. Addison-Wesley, Boston.

[11]Matt Blaze. 2019. Testimony of Prof. Matt Blaze. https://www.mattblaze.org/papers/blaze-homelandsecurity-20191119.pdf

emphasize the technological and military dimensions of cyberspace rather than the socio-political ones. States are caught in a classic security challenge in their attempts to protect cyberspace. The chaos that remains in the world community is the source of this security problem. States unconsciously make other states feel less comfortable by attempting to improve their states' defense, typically by enhancing military capability. As a consequence, there is a never-ending cycle of security-insecurity. This conundrum can be deconstructed into a two-level strategic game.[12]

In the most basic level, the perception question arises from a lack of knowledge regarding the motivations, intentions, and capacities of other actors. Decision-makers at the second level must decide how to react. The solution dilemma does not begin until the understanding dilemma has been resolved. Uncertainty and distrust are prevalent in cyberspace, much as they are in the physical world. States are concerned about other parties' intentions and cyber technologies, so they build offensive and defensive cyber-weapons. More instability is provided because there is little to deter states from trespassing on the digital boundaries of other states. The dilemma of meaning and the dilemma of answer result from this spiral of uncertainty. The current approach to cyber security, on both the public and private levels, is focused on the defense of vital national infrastructures (public and private) rather than citizen rights. Cyber attacks against information infrastructures, as well as worms and viruses, are viewed as cyber threats rather than breaches of privacy and/or freedom of speech at the interpretation stage. The 'human' factor as a security target is not only downplayed, but it is also included in the threat continuum (hackers, for instance). A possible national (cyber) challenge is anybody with a device linked to the Internet and the requisite technological skills. Similarly, at the response stage, the aim is to secure vital national infrastructures rather than people's right to obtain access to cyberspace services and use them according to their needs and desires. The cyber security problem not only causes a vortex of instability between states on a global scale, but it also has negative consequences within states.

Cyber technologies built to protect and safeguard a country's vital national resources are also used against its own people. Citizens are caught in a "liberty vs protection" paradox, where they must give up civil rights in exchange for greater security. In other words, policymakers use cyber protection as an excuse to track, manipulate, and attack web information. The aim of the Cyber Intelligence Sharing and Protection Act (CISPA), for example, was to allow the US government and businesses to defend the nation's information technology from international cyber attacks. CISPA allows businesses to give the government confidential consumer details without a warrant. Private businesses gather large amounts of personal data (customer preferences), and policymakers can access these private databanks with a single click. Another example is the use of cryptography to safeguard our personal information when communicating. The prohibition of encrypted messages could be seen as a violation of both the right to privacy and online anonymity, but it could also be justified for national security reasons.

Encryption, as a result of technology, is neither good nor evil. Citizens and terrorists both use the same encryption that shields governments and companies. Citizens are not the winners, but rather the casualties, of national cyber protection measures in

[12]Cerf, V. (2011).The Battle for Internet Openness.IEEE Internet Computing. 15 (5), 104

such situations. The cyber arms race has resulted in a reduction in Internet freedom within states. Filtering systems that block access to specific websites, encryption restrictions, the invention of Internet kill switches, and monitoring systems to track online activity are all tactics that have a significant impact on privacy, confidentiality, and therefore security. The use of counter-censorship tactics during the Arab Spring and the Snowden disclosures regarding the NSA's global surveillance in the name of counterterrorism are also dramatic illustrations of cyberspace's dark side.

2.4HUMAN RIGHTS VIOLATIONS IN CYBERSPACE

Individuals around the world are constantly at risk of human rights violations related to cyberspace. Governments employ a variety of measures that violate freedom of expression and the right to privacy, like targeting dissident voices, internet filtering practises or even disconnecting access to ICTs. Below are some examples of cyber surveillance and online censorship. In 2009, the re-election in Iran of President Mahmoud Ahmadinejad led to a social uprising of young Iranians, claiming that the votes were manipulated and calling for an investigation on the voting fraud. Iranians used social media, mainly Twitter to disseminate information about the protests. During the social uprising in Iran, social networking sites were blocked by the regime and the intelligence and security services managed to identify and close down the activities of those promoting dissent. In Tunisia, the self-immolation of the 26-year-old fruit and vegetable seller Mohamed Bouazizi on 17 December 2010, triggered nationwide protests against the oppressive government of Ben Ali.[13] The regime responded by disrupting the flow of information in social media, by hacking e-mail and Facebook accounts. Likewise in Egypt, the protesters demanded Mubarak's resignation and the reinstitution of democracy. The protesters used social media not only to spread the message, but also to share content like online maps and encryption techniques. The regime soon realized the importance of social media for its political survival and intensified the online censorship.

The Egyptian police monitored social networks, email accounts of dissidents as well as Skype and arrested dissidents that were responsible for coordinating the protests. In late January 2011, the regime, in a desperate move to control the information flow, decided to cut off access to Internet for a few days. In January 2010, Google announced that a computer attack originating from China had penetrated its corporate infrastructure and stolen information from its computers, most likely source code. The attacks also targeted Gmail accounts of some human rights activists and infiltrated the networks of 33 companies. A recent study by the European Parliament titled 'Surveillance and censorship: The impact of technologies on human rights' mentions a variety of measures that states use in order to control the information flow. One such measure that aims to discourage citizens from creating their own blogs and expressing their opinions, is the mandatory registration of online media with pubic authority. In Saudi Arabia, only citizens that can produce 'documents testifying to good conduct' and with a high school diploma are allowed to start their own blog or website.

Likewise in Belarus, websites must register using the national domain and be hosted on national territory. Another option is the control of the telecommunications industry

[13]Liaropoulos, Andrew. "In Search of a Social Contract for Cybersecurity." European Conference on Cyber Warfare and Security, Academic Conferences International Limited, July 2019, p. 282.

by governments. China has developed a set of technical solutions like the Great Firewall to block online content from foreign servers. Pakistan is blocking thousands of websites as part of its policies against terrorism, blasphemy and pornography. In Turkey, Google and Facebook were asked to remove political content during the Gezi park protests in 2013 and Twitter and YouTube were blocked before the elections in March 2014. The Snowden revelations about the mass surveillance programs conducted by the 'Five Eyes' (USA, UK, Canada, Australia and New Zealand) demonstrated the magnitude of human rights violations in the digital sphere and the rise of the surveillance state. In particular, the PRISM program enabled NSA to have direct access to the servers of Apple, Facebook, Google, Microsoft, Skype, Yahoo, Twitter and YouTube. The working relationship between intelligence and security agencies on the one hand and private sector one the other hand, raises a number of ethical and legal questions regarding electronic surveillance, citizen privacy and national security.

The Snowden disclosures also accentuated the role of Big Data. The capabilities that Big Data practices offer, are transforming the way surveillance is conducted. Personal data are not collected for limited and transparent purposes, whether that is public safety or national security. The traditional police and intelligence methods of identifying targets and then collecting data was reversed with Big Data. Instead, evidence is still being gathered until a decision is made about the full scope of their current and future applications. Big Data algorithms, according to the logic, would help us to predict behaviours and events. Big Data analysis' pre-emptive reasoning is undermining current regulatory processes that are built on an after-the-fact scheme of fines and punishments.[14]

2.5A HUMAN-CENTRIC PERSPECTIVE ON CYBER SECURITY

Based on the above review, it can be concluded that existing cyber security strategies do not provide consumers with a safe cyberspace. A quick glance at the press and official papers demonstrates that cyberspace is not a secure environment. In stark contrast to early expectations, the Internet is increasingly becoming a weapon of totalitarian rule. In the 1990s, the so-called cyber-utopians were unable to anticipate how effective the Internet would be for propaganda, how states (both democratic and authoritarian) would use cyberspace for surveillance, or how sophisticated censorship would become.[15]It is unfounded to believe that technology (and therefore ICT) empowers citizens rather than state oppressors. On the Internet, maintaining anonymity seems to be difficult. Governments and companies are amassing vast amounts of personal information. Users' accounts are detailed on search engines and online social networking platforms like Google and Facebook, and mobile phone providers use GPS systems to monitor and find their users. All private data is stored, and people's online behaviour and consumer habits are correlated and passed from companies to governments, most of the time without the knowledge and consent of the users. The transparency reports of Google, Microsoft

[14]Surveillance, Snowden, and Big Data: Capacitieshttps://journals.sagepub.com/doi/full/10.1177/2053951714541861

[15]Liaropoulos, Andrew. "Cyber-Security: A Human-Centric Approach." European Conference on Cyber Warfare and Security, Academic Conferences International Limited, July 2015, p. 189.

and Twitter show that most of the requests to companies for user data originate from liberal democracies. Companies who make tools for social network mining, mobile phone monitoring, and data manipulation are signing deals with democracies and authoritarian regimes all over the world. The cyber security industry, as the military-industrial complex before it, is amplifying the arms race in cyberspace and thereby empowering the cyber surveillance state. A issue that eventually arises is whether a different approach to cyber security will help us to avoid the cyber security challenge while still ensuring human rights safety.[16] Would an anthropocentric approach be useful in addressing the need of humans in the cyber realm? Safeguarding human needs in any domain, including cyberspace, raises once more the question about the meaning of security. The term 'security' is usually associated with the absence of threats to scarce values which might threaten the survival of the referent object.[17]

Security can be seen in both a positive and negative light. Security is described as the absence of threats to core human values in the negative sense, and policies and practices that protect and enable people to exercise their rights openly and safely in the positive sense. It is this positive conception of security that seems to be undervalued in the current cyber security discourse. States have historically viewed security in negative terms; and, thus, they also view cyber security as mainly the absence of harm. "Cyber security strategies should not only play a protective role, but also a supporting role, by ultimately placing the empowerment and well-being of people at their center," Kovacs and Hawtin argue. What we want people to be able to do is to be fearless as long as they honour the human rights of others."Human rights include freedom of expression, freedom of speech, freedom of thought, and the right to privacy, as protected by the United Nations' Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). It's worth noting that the UN Human Rights Council agreed in July 2012 that people's online rights must be secured in the same way that they are offline (Green & Rossini, 2015, p. 8). So how can states strike a balance between the protection of critical information infrastructure and data flows on the one hand and the right to privacy and online anonymity on the other? And who will be responsible for protecting, implementing and enforcing human rights in cyberspace?

In response to these questions, we need to note the following. First, the governance of cyberspace is still under construction. In particular, cyberspace lacks a single forum or international organization that is responsible for regulating its activities. As a result, governance is spread throughout technical standard setting fora, private sector organizations, civil society groups, states and international organizations.[18] Governance ranges from developing norms and codes of conduct, to signing international treaties and imposing regulations. Over the past years, there have been attempts both at the national and the international level to address human rights' concerns in cyberspace. States have passed laws and taken initiatives to counter cyber threats, but an international treaty that would regulate activities in cyberspace is still absent.

Since 2010, the Groups of Governmental Experts (GCEs) have been appointed by the UN General Assembly to report on the nature of cyber threats and their implications for national and international security. In their reports, the GCEs

[16]Bajaj, K. (2014) 'Cyberspace: Post Snowden', Strategic Analysis, Vol.38, No.4, pp.582-587

[17]Jervis, R. (1978) 'Cooperation under the Security Dilemma', World Politics, Vol.30, No.2, pp.167-214.

[18]Dilipraj, E. (2014) 'Internet Governance: The shift from monopoly to multi-party', National Defence and Aerospace Power, 99/14.

emphasized that states have to respect human rights and fundamental freedoms when addressing cyber security issues. Likewise, in 2013, the European Commission adopted the 'Cyber security strategy of the European Union: an open, safe and secure cyberspace' which states that EU's core values apply as much in the digital as in the physical world and that cyber security is only effective when based on fundamental rights and freedoms.

Despite the above positive developments, there is still no law enforcement mechanism that can ensure the protection of human rights in cyberspace. For example, there is no universal consensus on what constitutes personal data in cyberspace. The EU treats IP addresses as part of personal data, whereas the US does not. Likewise, in terms of data privacy, the EU applies a strict and top-down regulation system, where governments play a leading role, whereas the US relies more on industry self-regulation mechanisms. Another point to consider regarding the protection of human rights in cyberspace is the future demographic trends. Nowadays, only 30% of world population has regular access to the Internet.[19] The next billions of Internet users are coming from states in the Global South that embrace a Westphalian understanding of state and national security. Many of these states have authoritarian and autocratic regimes that have already developed cyber surveillance programs, at the expense of human rights. Pushing the global agenda for a human-centric understanding of cyber security, is not a priority for these states. Second, in the absence of global governance, the state is the sole player with the authority and capacity to meet human needs. This isn't meant to minimize the relevance of a human-centered approach to cyber security; rather, it's meant to put the debate in perspective. International and private players (international government and civil society) can be included in this sense, but states cannot be excluded. The defense of a state's territories, sovereignty, and people is described as national security. That notion expresses the reality of the pre-Internet era. Cyberspace is different from the other physical domains (land, sea, air, and space) against which states have to safeguard. Cyberspace is a transnational domain in which states are trying to overcome the border paradox and exercise their sovereignty.[20]

The oxymoron is that states have a responsibility to protect their people in cyberspace, but they make them feel vulnerable by infringing their online human rights. Because of the potential for violence, framing the defense of human rights in cyberspace as a national security problem may be counterproductive. States must recognize that people should be able to take advantage of the advantages of cyberspace rather than being the targets of widespread and illegal cyber surveillance. Protecting privacy and freedom of speech, as well as limiting unjustified public-private exchange of personal data, should be included on policymakers' electronic security agendas.

2.6 LET'S SUM UP

Various fields have addressed cyber defense. The controversy about the essence of cyber security has been enriched by information technology specialists, judges,

[19]Hare, F. (2010) The Cyber Threat to National Security: Why Can't we Agree?, in Czosseck C. &Podins, K. eds, 2nd International Conference on Cyber Conflict Proceedings, NATO CCD COE Publications, Tallinn.

[20]Mordini, E. (2014) 'Considering the Human Implications of New and Emerging Technologies in the Area of Human Security', Science and Engineering Ethics, Vol.20, Issue 3, pp.617-638.

strategists, and state leaders. State-centricity is the prevailing theme, regardless of its theoretical basis. The new cyber security strategy is ineffective and completely irrelevant, if not aggressive, to people's needs. States are producing cyber (in) security both at the international system and among sub-state players, rather than making cyberspace more stable. The rights of governments have overwhelmed the interests of citizens in this situation, as they have in many others in the past. Indeed, electronic weapons designed to protect a nation's cyber properties are being used against its own civilians. Breaking the "cyber security paradox" and finding a balance between national cyber policy on the one hand and privacy, secrecy, and freedom of expression on the other are enormous challenges. The risks that the idea of a "surveillance regime" entails are not recent.

The fear is that cyberspace will transform this sinister metaphor into reality, or has already done so. Anonymity is vanishing in the era of Big Data and the Internet of Things. By personal ads, companies are using meta-data to form marketing campaigns. Monitoring the entire spectrum of human actions in the digital realm is critical to the role of national security and intelligence services. While the securing of cyberspace is unavoidable, the shape that cyber defense will take in the immediate future is not. In fact, the current securitization of cyberspace is intertwined with the securitization of every part of our lives. Shifting the narrative to human rights is just the first step in ensuring internet users' safety. Securing human interests in a domain devoid of meaningful governance and blurring the boundaries between national and international, public and private, is a conundrum wrapped in a mystery.

2.7FURTHER READING

- Cropf, R., & Bagwell, T. (Eds.). (2016). Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance.
- Dunn Cavelty, M. (2012). The militarization of cyberspace: why less may be better. In C. Czosseck, R. Ottis& K. Ziolkowski (Eds.), Proceedings of the 4th International Conference on Cyber Conflict (pp.141-154). Tallinn, Estonia: CCD COE Publications.
- Betz, D., & Stevens, T. (2011). Cyberspace and the state: toward a strategy for cyber-power. Adelphi Paper 424. Oxfordshire, UK: IISS & Routledge.
- Booth, K., & Wheeler, N. (2008). The security dilemma: fear, cooperation and trust in world politics. New York, USA: Palgrave.
- Brantly, A. F. (2014). The cyber losers. Democracy and Security, 10(2), 132–155.

2.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyberspace?**

Cyberspace is a global realm within the knowledge environment identified by the use of electronics and the electromagnetic spectrum to build, store, alter, share, and manipulate information through interdependent and interconnected networks using information communication technologies.

2.9 ACTIVITY

Analyse the intricacies of cyberspace and its effect on human rights. (1500-2000 words)

3

Unit 3: CASE STUDY- USA

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Cyber Security as Human Rights Issue

3.4 Defense Advanced Research Projects Agency (DARPA)

3.5 The Threat Environment

3.6 New Strategy

3.7 Let's sum up

3.8 Further reading

3.9 Check your progress: Possible Answers

3.10 Activity

3.1 LEARNING OBJECTIVES

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

- cyber security as human rights issue
- Defense Advanced Research Projects Agency (DARPA)
- threat environment of cyberwarfare

3.2 INTRODUCTION

There is no universal definition of cyber security; however, the definition developed by the "Internet Free and Secure" working group of the Freedom Online Coalition (FOC), which was composed of technologists, human rights experts and government, is instructive. Inspired by the International Organization for Standardization 27000 standard, the FOC working group defines cyber security as "the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline."[21]

3.3 CYBER SECURITY AS HUMAN RIGHTS ISSUE

3.3.1 Why cyber security is a human rights issue

Using the FOC definition of cyber security as a basis, it is easy to see how threats to cyber security – or cyber insecurity – can be human rights violations. The denial of availability of information and its underlying infrastructure, in the form of network shutdowns, for example, violates a wide range of rights, including by unduly restricting access to information and the ability of people to express themselves, peacefully assemble and associate, as well as enjoy a range of economic, social and cultural rights. In 2018,196 internet shutdown were documented in 68 countries.

There are countless examples of the confidentiality of information being compromised, whether through data breaches for financial gain, mass government surveillance or targeted attacks on human rights defenders or journalists, in violation of the right to privacy, among other rights. Breaches of the confidentiality of

[21]https://www.apc.org/en/news/why-cyber security-human-rights-issue-and-it-time-start-treating-it-one

communications through surveillance is linked to severe human rights violations, like detention, torture and extrajudicial killings. An example of a particularly egregious case is the surveillance of Saudi dissident Omar Abdulaziz, which contributed to the extrajudicial execution of Saudi journalist Jamal Khashoggi. According to a lawsuit, Abdulaziz's cell phone was targeted by the Saudi Arabian government with spyware, compromising the confidentiality of his communications with Khashoggi about opposition projects in the months leading up to Khashoggi's killing.

While most people are likely to experience some form of cyber insecurity in their lifetime, even people for whom meaningful access to the internet is a challenge, cyber insecurity is not experienced evenly by everyone. Human rights defenders, journalists, and people in positions of marginalisation or vulnerability, because of their religion, ethnicity, sexual orientation or gender identity, for example, can experience particular risk. For example, they are more likely to be targeted by government or lateral surveillance, and the consequences of more broad threats like data breaches or network shutdowns are often more severe for them because of their location within society.

As more people and devices are connected, the risks that come with cyber insecurity will only increase. Unfortunately, governments are either not centring cyber security discussions on human rights, or worse, they are using cyber security as an excuse to exercise more control over the internet.

3.3.2 The securitisation of "cyber"

The development of laws, policy and norms on cyber security tends to take place in highly opaque, securitised settings without the benefit of civil society input or human rights expertise. This runs counter to the multistakeholder approach to internet governance, which relies on the full involvement of governments, the private sector, civil society and international organisations. Critically, this approach excludes the expertise and monitoring required to protect human rights. Often, cyber security discussions happen in the confines of intelligence services, or other government or military agencies that are not subject to public scrutiny or oversight. Cyber security is also sometimes equated with national security, which is characterised as a sacred sphere in which governments can do whatever they want and without public scrutiny, much less oversight. As a result, cyber security law, practices and policies are often divorced from a human rights framework, and susceptible to abuse of power.

3.3.3 International cyber security debates miss the mark

It is well established that international human rights law applies to digital technologies. However, when it comes to cyber security, international human rights law is not central to discussions, if a factor at all. This is partially due to the fact that international discussions on cyber security predominantly respond to the issue of state-on-state attacks and fall under the rubric of international security and disarmament. Nonetheless, the tenor of these discussions, and the norms that stem from them, have implications for how states approach cyber security at the national level. Of particular concern are efforts by the Shanghai Cooperation Organization (SCO), which for years has been working to advance the concept of extending national extending national sovereignty and information control in cyberspace.

The UN has held since 2013 that international law, which includes international humanitarian law and international human rights law, applies in cyberspace. In 2015, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security further elaborated that respect for human rights and fundamental freedoms is seen as being “of central importance” and recommended that states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age.

While the international community has gotten stuck on how international law applies in cyberspace, the focus has primarily been on international humanitarian law. This approach is flawed for several reasons. First, international humanitarian law applies only in times of armed conflict, whereas international human rights law applies at all times (in peace and war). Given that most of the types of cyber insecurity are experienced during peacetime (or at least in the absence of a declared cyber war), international human rights law is more frequently the applicable framework. Second, and relatedly, centring debates on international humanitarian law may somehow advance the belief that states are in a perpetual cyber conflict, leading to an escalation in cyber attacks. Third, international humanitarian law is a legal framework more permissive of harm to the general public than is ordinarily allowed.

International human rights mechanisms provide specific guidance that is relevant for cyber security, and should be drawn on in the development of norms for responsible state behaviour in cyberspace. For example, reports of UN Special Procedures explain why strong encryption is necessary for the confidentiality of information and how network shutdowns are in violation of human rights law and unduly interfere with

the availability of information. There is a well established body of norms under international human rights law, namely the UN Guiding Principles on Business and Human Rights, which spell out the responsibility of the private sector to respect human rights, mitigate adverse effects, and remedy harm. This is a critical point, given that the private sector owns and/or operates most of the infrastructure, hardware and software upon which the internet relies.

3.3.4 Security for whom?

Perhaps the most pernicious threat, is that states exploit the serious nature of cyber security threats to take liberties to enable them to exert their power in cyberspace in ways that directly undermine human rights. When assessing a cyber security framework, it is essential to ask: security for whom? security from what? and security by what means? Too often the answers to these questions reveal that the state defines security as protecting itself from political instability, applies disproportionate measures to ensure its own preservation, and itself becomes the source of insecurity.

To give just a few examples, in Vietnam a cyber security law was passed last year that allows the government to force technology companies to hand over potentially vast amounts of data, including personal information, and to censor users' posts. The previous year in China, a cyber security law was adopted that requires companies to censor "prohibited" information, restricts online anonymity, including by requiring real name registration, and mandates the storage of Chinese users' data within the country. In Israel, the proposed Cyber Security and National Cyber Directorate Bill would give the government sweeping new powers to hack the computers or phones of any person or entity that is defined as a threat to cyber security and to access the device and extract data without a court order. Earlier this year, the Venezuelan government proposed the Constitutional Law of Cyberspace, which declares Venezuelan sovereignty over cyberspace and would require messaging service providers to censor content without a prior judicial order or respect for minimum guarantees for due process among other measures to extend state control of the internet.

Each of these examples demonstrates a government instrumentalising security at the expense of human rights, in particular the rights to privacy, freedom of expression, association and assembly, and incidentally, at the expense of cyber

security, i.e. the availability, confidentiality and integrity of information and its underlying infrastructure.

3.3.5 Putting cyber security on the rights track

In order to safeguard human rights in this digital age, it is time to start treating cyber security as a human rights issue.

First, there is the need to challenge the prevailing view that human rights are an impediment to security. Perhaps the most widely cited example of human rights standing in the way of security is the assertion that encryption, which is critical for exercising the right to privacy, impedes law enforcement in conducting its work. Time and again, governments make the case for building in backdoors and weakening encryption in order to provide access to encrypted communications for law enforcement. However, experts are in agreement that it is not possible to provide access to encrypted communications for one government without doing so for all government and for malicious non-state actors. To put it another way, weakening cyber security for law enforcement purposes cannot be done without weakening security for all, and putting everyone's human rights at risk. This is because cyber security is inexorably linked to human security, which is a fundamental human right. Cyber security and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security.

Second, it is critical to apply human rights-based approaches to cyber security laws, policies and practices. The danger of cyber insecurity should never be a used a pretext to violate human rights. Instead, recognising that individual and collective security is at the core of cyber security means that protection for human rights should be at the centre of cyber security policy development. At the international level, it is imperative to root deliberations on cyber security in international human rights law. The Freedom Online Coalition "Internet Free and Secure" working group developed a set of cyber security and human rights-focused policy recommendations towards ensuring that cyber security policies and practices are based upon and fully consistent with human rights – effectively, that cyber security policies and practices are rights-respecting by design. These recommendations, which have been endorsed by 30 FOC governments and over two dozen NGOs, are a useful starting point for rooting cyber security policies and practices in human rights.

Third, companies must respect human rights, and governments must hold them to account. The UN Guiding Principles on Business and Human Rights provide the necessary framework; however, there is a need for more scrutiny and oversight of technology companies – both of those that provide the hardware and software used for launching cyber attacks and those that serve as the first line of defence in cyber attacks. In addition to conducting human rights impact assessments to identify, understand, assess and address the adverse effects of their policies and practices on the enjoyment of human rights, they should be conducting cyber security due diligence to review the governance, processes and controls that are used to secure the information they process. Companies have advanced self-regulatory initiatives like Microsoft's Cyber security Tech Accord, which aims to respond to cyber security threats that put people's rights at risk, but does not take an explicit human rights framing, and therefore has some gaps.

Governments can also do more to regulate the technology industry to prevent and mitigate human rights violations as a result of cyber insecurity. For example, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recently called for a moratorium on surveillance technology. Such bold moves are needed not just for the surveillance technology industry, but for the technology sector writ large, to ensure that companies are not profiting off of human rights violations or treating people's data recklessly.

Fourth, cyber security processes need to be multistakeholder and inclusive, as well as multidisciplinary, infused with human rights and technical expertise. This means taking cyber security outside the confines of national security and intelligence agencies and challenging assumptions that cyber security is first and foremost a national security issue. Given that citizens are so often asked to make sacrifices in the name of national security, it is crucial that the bases for those sacrifices are scrutinised for their necessity and proportionality; that there is independent oversight of responses to national security threats to ensure that they are justified; and that there is more transparency as well as public debate to ensure that national security is not being equated with regime security.

Digital technologies present new and unforeseen challenges to human rights and security, which will require more documentation, research and analysis. Until cyber security and human rights are understood and treated as mutually reinforcing and complementary, both will suffer.[22]

[22]https://www.apc.org/en/news/why-cyber security-human-rights-issue-and-it-time-start-treating-it-one

3.4DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)

The United States has unrivalled strategic tools, which it will use to develop superior military capability in cyberspace. The Pentagon has already started to look at how businesses can assist the government in combating the cyber threat. The chief executive officers and chief technical officers of information technology and defense firms now consult annually with senior officials from the Department of Homeland Security, the Office of the Director of National Intelligence, and the Department of Defense as part of the Enduring Security Framework, a public-private collaboration. The science and development agencies of the United States government have now turned their focus to cyber security. The National Cyber Range initiative, established by the Defense Advanced Research Projects Agency, is one of the most significant developments to emerge (DARPA). The Pentagon has had no such capabilities when it comes to cyberwarfare, despite the fact that the US military regularly drills units on target ranges and in a series of simulations.[23]This is why DARPA, which was instrumental in the development of the Internet decades ago, is creating the National Cyber Range, a virtual Internet that will enable the military to test its cyber defense capabilities before deploying them. Malicious applications intended to hack computer networks will also benefit from simulations. The National Laboratories of the Department of Energy have created machine farms that function as automated petri dishes, collecting live viruses from the Internet and monitoring their propagation. These diagnostic and teaching skills will help the US keep ahead of its adversaries' cutting-edge cyber weapons.

DARPA is conducting still more fundamental analysis that might boost the government's ability to attribute threats and blunt intruders' capabilities, reducing the offense-dominant nature of cyberspace. The military may update or retrofit computers, operating systems, and programming languages with cyber security in mind, according to the department, which is asking the scientific community to reconsider the fundamental configuration of the Pentagon's network infrastructure. Complex information technology systems would not improve immediately, but the United States has a good chance to engineer its way out of some of today's most troublesome vulnerabilities over the span of a century. The government must also improve its human resources. The Pentagon has expanded the number of cyber security experts on staff and improved their education. Which requires a rigorous credential program that now graduates three times as many data security experts each year as it did only a few years earlier.[24]

The Pentagon's network managers have been educated in "ethical hacking," which entails using adversarial tactics against the US's own networks in order to detect vulnerabilities before they are used by an attacker, in line with industry standards. And as the US government expands its cyber security workforce, it must

[23]APC, (2019) 'Why cyber security is a human rights issue, and it is time to start treating it like one', retrieved from: https://www.apc.org/en/news/ why-cyber security-human-rights-issue-and-it-time-start-treating-it-one

[24]Krotkov E, Blitch J. The Defense Advanced Research Projects Agency (DARPA) Tactical Mobile Robotics Program. The International Journal of Robotics Research. 1999;18(7):769-776. doi:10.1177/02783649922066457

acknowledge that long-term human resource dynamics are not encouraging. The United States accounts for just 4.5 percent of the global population, and several nations, including China and India, will train more highly skilled computer scientists in the next 20 years than the United States. If the US's cyber edge is based solely on amassing qualified cyber security experts, the US will lose the advantage.[25]
As a result, the US government must approach the cyber security problem in the same way it approaches other military challenges: with an emphasis on superior technology and competitiveness rather than statistics. To supplement the qualified cyber security experts in the US military, high-speed sensors, advanced analytics, and automated systems will be required, and such resources will be accessible only if the US commercial information technology sector remains the world leader, which will necessitate continued developments in research, technology, and education at all levels.

3.5THE THREAT ENVIRONMENT

About all the military does is made possible by information technology: logistics assistance, multinational command and forces, real-time intelligence, and remote operations. Each of these roles is largely reliant on the military's global networking backbone, which includes 15,000 networks and millions of computer machines spread across hundreds of countries' facilities. More than 90,000 employees work full-time to keep the system running. Digital technology in the military has progressed from an administrative instrument for increasing workplace production to a national strategic weapon in its own right in less than a decade. The United States' digital technology today gives it crucial advantages over any foe, but its dependence on information networks still allows adversaries to acquire useful intelligence about US capabilities and activities, obstruct conventional US armies, and threaten the US economy. The Pentagon is concentrating on a few aspects of the cyber challenge as it develops a strategy to fight these threats.[26]
First and foremost, cyberwarfare is asymmetrical. Because of the low cost of computation, US adversaries do not need to develop costly weapons like stealth fighters or aircraft carriers to pose a serious threat to US military capabilities. A dozen dedicated computer programmers will disrupt the United States' global logistics network, rob its operating plans, blind its intelligence capability, or obstruct its ability to deploy weapons on schedule if they discover a loophole to exploit. Because of this, many militaries are improving aggressive cyber capabilities, and over 100 international intelligence agencies are attempting to hack into American networks. Many countries have also shown their ability to undermine parts of the United States' information system.
The US barely gets it right when it comes to predicting when and when armed clashes will occur. It's also difficult to predict cyberattacks, particularly because both state and non-state actors are a threat. More importantly, since information

[25]Pippine J, Hackett D, Watson A. An overview of the Defense Advanced Research Projects Agency's Learning Locomotion program.The International Journal of Robotics Research. 2011;30(2):141-144. doi:10.1177/0278364910387681

[26]Feldstein, S. (2019) 'The Global Expansion of AI Surveillance,' Carnegie Endowment for International Peace, retrieved from: https:// carnegieendowment.org/2019/09/17/global-expansion-of-aisurveillance-pub-79847

technology is increasingly emerging, lawmakers have no historical experience to base their standards on. As a result, the US government must be realistic in its capacity to predict when and how this challenge will manifest; instead, it requires an approach that allows for organizational stability and adaptability.

3.6NEW STRATEGY

The Pentagon has officially accepted cyberspace as a modern area of warfare on a doctrinal level. Despite being a man-made world, cyberspace has become as essential to military operations as ground, sea, air, and space. As a result, the military must be capable of working inside it. The defense department needs an adequate operational framework to support cyberspace operations. The military's cyber security effort has been run by a loose confederation of joint task forces that are geographically and institutionally scattered for many years.[27] Defense Secretary Robert Gates ordered the restructuring of the task forces into a new four-star unit, the US Cyber Command, in June 2009, realizing that the scope of the initiative to defend cyberspace has outgrown the military's current systems. The US Cyber Command launched operations in May 2010 as part of the US Strategic Command. By October, Cyber Command should be fully operational.[28]

There are three missions for Cyber Command. First, it is in charge of the day-to-day security of all defense networks, as well as assisting military and counter-terrorism missions with cyberspace operations. Second, it establishes a transparent and accountable method for coordinating electronic warfare capabilities around the military. From the president of the United States through the secretary of defense, the commander of Strategic Command, the commander of Cyber Command, and on to individual military units around the globe, there is a single chain of command. Cyber Command manages commands within each branch of the military, including the Army Forces Cyber Command, the US Navy's Tenth Fleet, the 24th Air Force, and the Marine Corps Forces Cyberspace Command, to ensure that cyber security issues are a routine part of recruiting and equipping troops. Since military networks are not impenetrable to attack, ensuring that all tactical forces can operate in a degraded knowledge environment is an important part of the training mission.

The third mission of Cyber Command is to collaborate with a number of allies both within and outside the US government. Representatives from the FBI, the Department of Homeland Security, the Justice Department, and the Defense Information Systems Agency, as well as liaison officers from the intelligence community and allied nations, serve on-site at Cyber Command's Fort Meade headquarters. Cyber Command, in collaboration with the Department of Homeland Security, collaborates closely with private industry to exchange vulnerability intelligence and fix common vulnerabilities. Since information networks link a number of organizations, the United States' defense effort can only be effective if it is organized through the nation, with alliances, and with commercial partners. Given the offensive superiority in cyberspace, US defenses must be flexible. Since

[27]Freedom Online Coalition (FOC), (2015) 'Recommendations for Human Rights based approached to cyber security,' Working Group 1 "An Internet Free and Secure", retrieved from: https://www.freedomonlinecoalition.com/ wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final21Sept-2015.pdf

[28]Front Line Defenders, (no date) 'Security in A Box - Digital Security Tools and Tactics', retrieved from: https://securityinabox.org/en/

milliseconds matter, the US military must react to attacks when they occur, or even before they occur. To deal with this, the Pentagon has deployed a scheme that consists of three interconnected lines of protection, two of which are built on commercial best practices, such as maintaining up-to-date security technologies and firewalls, and sensors that track and map intrusions.

The third line of defense employs federal surveillance resources to provide highly advanced active defenses, and the government is applying all of these defenses in a manner that complies with its duty to defend Americans' civil liberties. The National Security Agency has pioneered programs that rapidly deploy protections to counter intrusions in real time, based on alerts issued by US intelligence capabilities. This active defense networks, which are part tracker, part sentry, and part sharpshooter, mark a significant change in the United States' approach to network defense.[29] They detect and avoid malicious code until it enters military networks by using scanning technologies at the gateway of military networks and the open Internet. Both security and intelligence networks in the ".mil" area are now protected by active defenses. Since certain intrusions will eventually elude detection and go undetected at the border, cyber protections in the United States must be able to track down intruders after they have gained access. This necessitates the need to search inside the military's own networks, and is part of the Pentagon's aggressive defense capabilities. Active security has been made possible by bringing the Department of Defense's joint cyber defense assets under one roof and connecting them to the signals intelligence required to predict intrusions and threats. One of the most significant reasons for the establishment of cyber command was to establish this connection. Because of the pace at which active defense systems must respond, network defense rules of engagement must be established in advance. It's not easy to come up with these protocols. Indeed, defining simple rules of engagement for reacting to cyberattacks has proven to be extremely challenging, and for good reason.

3.7 LET'S SUM UP

The overwhelming complexities of cyber security herald the dawn of a modern era of technology. The United States' greatest asset at this early stage is its understanding of the transition. The current situation reminds me of an urgent letter written to President Franklin D. Roosevelt on the cusp of a modern technical age. It was dated August 2, 1939, and it said, in part, "Certain facets of the current situation seem to necessitate vigilance and, if possible, prompt action on the part of the Administration. As a result, I feel it is my responsibility to put the following facts and suggestions to your notice." "Yours most sincerely, Albert Einstein," the letter read. Following Einstein's warning that breakthroughs in nuclear fission could lead to the creation of an atomic bomb, Roosevelt launched the Manhattan Project, which helped the United States prepare for the atomic age. While the cyber crisis does not have the same existential ramifications as the nuclear era, there are significant parallels. Potential adversaries will use cyberattacks to bypass overwhelming US advantages of traditional military strength in a way that is both instantaneous and difficult to track.

[29]Liaropoulos, A. (2015) 'A Human-Centric Approach to Cyber security: Securing the Human in the Era of Cyberphobia,' Journal of Information Warfare 14 (4), 15–24.

And if such attacks do not result in the same level of deaths as a nuclear attack, they have the potential to paralyze American society. In the long run, hackers' concerted hacking of American universities and companies could deprive the US of its intellectual property and competitive advantage in the global economy. These dangers are prompting the Pentagon to develop a new cyber security policy.
The strategy's main components are to provide an organizational structure for training, equipping, and commanding cyber defense forces; to use layered defenses with a strong core of active defenses; to use military capabilities to support other departments' efforts to secure the networks that run the US' critical infrastructure; and to build collective defenses with US allies. The aim of this policy is to make cyberspace stable so that revolutionary technologies will benefit both national security and economic security in the United States.

3.8FURTHER READING

- Press, 2008). 9 See "Country Profiles," OpenNet Initiative, Internet, https://opennet.net/country-profiles (date accessed: 30 October 2013).
- 2013). II Milton Mueller, Andreas Schmidt, and Bren- den Kuerbis, "Internet Security and Networked Governance in International Relations," International Studies Review 15 (2013), 86-104.
- RonaldDeibert, "Why NSA spying scares the world," 12 June 2013, CNN, Internet, http://www.cnn.com/2013/06/12/opinion/deibert-nsa-surveil-lance (date accessed: 30 October.

3.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How is DARPA contributing in cyber security?**

   DARPA is also working on more basic analysis that could help the government better attribute threats and blunt intruders' capabilities, rendering cyberspace a less offensive area. The military may update or retrofit computers, operating systems, and programming languages with cyber security in mind, according to the department, which is asking the scientific community to reconsider the fundamental configuration of the Pentagon's network infrastructure.

3.10 ACTIVITY

Explain the strategies adopted by Pentagon for cyber security. (1000-1500 words)

4

Unit 4: ROLE OF CIVIL SOCIETY

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Starting with first principles of security

4.4 Opening Up the Black Box

4.5 Shutting the Back Door

4.6 Let's sum up

4.7 Further reading

4.8 Check your progress: Possible Answers

4.9 Activity

4.1 LEARNING OBJECTIVES

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

- the principles of security theory
- open government security programme
- shutting the back door for law enforcement and intelligence agencies

4.2 INTRODUCTION

As cyberspace has become the infra- structure for global communications, the security of the domain has become a top priority. Yet, rarely examined directly are the questions, security for whom and security for what? Although engineers like to think of cyber security as a technical problem requiring a "fix" or "patch," security is always for someone and some purpose and is, therefore, always inherently political. In the absence of considered alternatives, the tendency has been to default to the Realist approach to statecraft and all that it entails. Not surprisingly, we are seeing reflexive policies that involve erecting defensive perimeters to the world outside; solutions that depend on hierarchy, secrecy, and classification; and defense and intelligence agencies taking on leading roles. These approaches result in the gradual erosion of checks and balances on power, self- reinforcing cycles of hostility and suspicions abroad, and a dangerously escalating arms race in cyber- space fuelled by a growing cyber security industrial complex.[30] In book, Black Code, the author has argued that in the headlong rush to security, liberal democratic countries are losing sight of that which they should be securing in the first place: a robust system of checks and balances that, supported by the free flow of information and commerce, cuts across domestic and international divides of like-minded countries and gradually results in the integration of security communities sharing a commitment to the rule of law and human rights. Part of the problem rests with the communities most dependent on the success of such a vision: global civil society.

Those who would consider themselves to be part of global civil society have been among the most persistent watch- dogs of governments and corporations, spotlighting violations of human rights online, and calling out surveillance and censorship. However, they have found it much easier to identify what they are against than what they are for, especially when it comes to securing cyber- space. Security is traditionally seen as an anathema to civil society, for some the language itself evocative of the very constituencies that need to be resisted. Yet, sidestepping the conversation will ensure only that citizens communicate in environments secured according to the interests and values of others. Civil society is moreover critically dependent on communications, and should see securing cyberspace as a top priority as much as any other stakeholder. To be sure, what is loosely called "global civil society" is hardly unified, and contains many divisions along ethnic, gendered, and regional lines. However, at a baseline, all of civil society depends on both an open

[30]Jensen, Michael &Danziger, J. &Venkatesh, Alladi. (2007). Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics. Inf. Soc.. 23. 39-50. 10.1080/01972240601057528.

and secure Internet, one not subject to disruption and through which ideas can be freely exchanged by citizens around the world. In the following article, the author lays out what he believes some of the core elements of that strategy should be, beginning with a consideration of first principles. Together these strategies are oriented around building a fortress for liberal democratic republics that can be extended as part of a global civil society strategy for cyberspace.[31]

4.3STARTING WITH FIRST PRINCIPLES OF SECURITY

The political nature of security begins with what is defined as the "object" of security, meaning that which is considered worth protecting. While the object of security in international affairs may seem too obvious to state, there is wide variation in objects of security, even in today's nation- state system. For some, the object of security is the entire country: its population, territory, and way of life. For others, it is more narrowly defined around the regime, party, or even an individual in power. It is remarkable how rarely such considerations of first principles around security are examined.[32] Part of the reason is that for so long, one tradition has had a monopoly on security discourse and practice. Once invoked, security tends to privilege Realist-associated institutional responses and elevate certain priorities in an almost instinctual fashion: hierarchy, secrecy, concentration of power, the erection of borders between "inside" and "outside," and the employment of military and intelligence agencies to positions of power and authority.

While these lessons have a long pedigree and were formed out of centuries of hard-fought experiences, they may not always be appropriate to the conditions of a time and place. There is also a lack of clearly articulated alternatives to this tradition, especially in civil society. Not surprisingly, those who consider themselves to be part of a global civil society, such as advocates of human rights, lack their own tradition of security from which to draw. Security tends to be seen by members of this community as some- thing to be resisted at best, or delegated to the men and women in uniform at worst. Those among civil society who are outraged today by revelations of government surveillance may even go further, believing that no government is good government. Yet, civil society is inherently dependent on the rule of law, without which human rights- including privacy, freedom of speech, and access to information-cannot be guaranteed. Without agencies capable of enforcing laws or defending against those whose aims are to destroy the very basis of liberal democracy, civil society networks would quickly find themselves extinguished. It is both undesirable and unrealistic to advocate doing away with government altogether.[33]

The question is not a matter of states versus no -states, but rather which type of state do we want? The work of Johns Hopkins, University Professor Daniel Deudney argues that there is a long- standing security theory at the heart of liberal democratic thought, one which is derived from the republican tradition of politics stretching to

[31]Cauce, A., and Srebnik, D. 1990. Returning to social support systems: A morphological analysis of social networks. American Journal of Community Psychology 18(4):609–616

[32]Davis, R. 1999. The web of politics: The Internet's impact on the American political system. New York: Oxford University Press

[33]Lessa, E. P. 1990. Multidimensional analysis of geographic genetic structure. Systematic Zoology 39(3):242–252.

ancient Greece. While having different elements, that tradition can be boiled down to core practices that mix and disperse authority around a system of checks and balances, in order to tie down and prevent the concentration of political power. Deudney has described these republican security practices as employing the structural principle of “negarchy,” namely, something in between the twin evils of anarchy and hierarchy. Republican security thinking is associated mostly with domestic political orders, but it is inherently an inter- national approach as reflected in the founding of the early United States of America and later the European Union, both of which sought to achieve a confederation of independent units but stopped short of full amalgamation into a consolidated state.

Republican systems of rule are designed to guard against not only internal hierarchy, but also external predation and empire. Reflecting on this theory in the con- text of cyberspace governance, it is noteworthy that the Internet exploded in a short period to become one of the most densely integrated of these transnational networks. However, the gradual encroachment of governments into Internet policy has imposed borders on cyberspace, perversely under- mining one of the pillars of republican security practice in the process. More than forty countries engage in some form of Internet censorship, including liberal democratic countries, with the censorship undertaken in secrecy using technologies developed by Western firms. Countering these tendencies requires a nuanced understanding of the interconnections between these multi-layered processes, and an orientation starting with first principles and working outwards. From this perspective, speaking about “Internet freedom” abroad while taking advantage of locally domiciled companies to subject communications to surveillance seems like self-serving hypocrisy. Instead, it is in the interest of liberal democratic governments to push for ever expanding transnational communications infrastructures that operate with the greatest degree of transparency and independence from specific jurisdictions, while working to strengthen and deepen practices of mixture, division, and restraint starting in the liberal democratic core and working outwards.

4.4OPENING UP THE BLACK BOX

At the heart of republican security practices is what Jeremy Bentham called a “system of distrust,” one in which elites are kept in line, in part, by fear of public exposure. Likewise, John Stuart Mill argued that exposure compels “deliberation and force[s] everyone to deter- mine, before he acts, what he shall say if called to account for his actions.” Government secrecy in a liberal democracy should be practiced infrequently with exceptional justifications, and closely monitored by independent oversight bodies. Over the years, however, and especially in response to the exigencies of 9/11, government secrecy has ballooned. Ironically, at the same time that elected officials have been campaigning on platforms of “open government,” security programs are being quietly buried in layers of classification and shielded from public scrutiny. For example, the deliberations of the U.S. court whose ostensive mission is to provide a check against the operations of the NSA, the Foreign Intelligence Services Court, are themselves shielded from public scrutiny.

At the same time, government agencies that operate with the most secrecy, notably signals intelligence, have mushroomed in scope and scale, their budgets and missions expanding. The influence of these pro- grams has extended into the private

sector, including scores of defence and intelligence contractors that service their programs, like Edward Snowden's former employer Booz Allen Hamilton. These companies are drawn into an orbit of classification and secrecy, some estimates as many as 1.4 million Americans hold Top Secret clearances. While a great deal of attention has focused on the adequacy of the United States system of checks and balances in the wake of the Snowden revelations, arguably its system of oversight is much more rigorous than those of other liberal democratic countries. In Canada, for example, the operations of the Communications Security Establishment of Canada (CSEC) - the Canadian counterpart to the American NSA are overseen by a single independent commissioner, a retired federal judge.[34]
There is no parliamentary oversight of the CSEC. Meanwhile, its budget and staff have grown considerably since 2001. Likewise, recent reports by the Guardian disclosed that officials in the U.K.'s Government Communications Headquarters (GCHQ) held the belief that "We have a light oversight regime compared with the US. Not only have these agencies ballooned in size, but some have also been given expanded responsibilities as lead agencies in cyber security. For example, the NSA and the U.S. Cyber Command share the same chief, General Keith Alexander. According to intelligence historian James Bamford, "never before has anyone in America's intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy." More important than Alexander's personal rule, however, is the gradual positioning of the NSA as the command agency for U.S. cyber security. While it certainly can make an argument for having the most advanced capabilities for the mission, the secrecy that surrounds the organization means that having it do so can further inter- national suspicion, undermine inter- national cooperation, and introduce military solutions to a domain that is primarily owned and operated by the private sector. A corrective to this excess should be an urgent priority, and a good place from which to start are the Tshwane Principles, drafted by 22 organizations and academic centers in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world. The principles recognize that withholding information from the public is often a necessary component to protect the full exercise of human rights.

4.5SHUTTING THE BACK DOOR

The prevailing paradigm of cyber security has brought about pressures on industry not only to provide governments with access to data they control, but also to build directly into their technologies access systems, known as "backdoors." Built-in backdoors for law enforcement and intelligence agencies are not new to the post 9/11 era. In a report published by the Center for Democracy and Technology in the United States in 2013, a group of twenty computer security researchers argued that "mandating wiretap capabilities in endpoints poses serious security risks," and that "building intercept functionality into products is unwise and would be ineffective, with serious consequences for the economic well-being and nation."[35]

[34]Muhlberger, P. 2004. Access, skill and motivation in online political discussion: Testing cyberrealism. Democracy online: The prospects for political renewal through the Internet, ed. P. M. Shane. New York: Routledge

[35]Shutting the Backdoor - Open Canada. https://opencanada.org/shutting-the-backdoor/

A republican cyber security policy will stress the opposite: promoting universal use of state-of-the-art cryptography, the introduction of protocols such as “https by default” and “two factor authentication,” and the implementation of open source applications to create trust across borders, rather than designing in those insecurities by nature. Regulations surrounding data deletion and policies like the “freedom to be lost,” which, although traditionally used in a rights-based context, have security ramifications insofar as they limit the amount of stored data that may be used for malicious purposes, are in accordance with this strategy. In a world of “Big Data,” in which so much of our information is routinely given away as part of our daily life, law enforcement and intelligence agencies need to find ways to work within this universe as it exists, rather than drill holes from the inside out in ways that undermine confidence and create additional risks for all of society.

4.6 LET’S SUM UP

These elements of a republican strategy for cyber security are only starting points. Most of them are hardly novel, and each in their own right have been widely and loudly advocated by many organizations and individuals. However, it is important to remind oneself occasionally that the whole is greater than the sum of its parts; tying each of these elements together (and no doubt others that the author has failed to include here) into a coherent strategy will provide support, coherence, and direction to what otherwise might be seen as isolated arguments. Civil society need not shy away from the cyber security debate. Indeed, there is a rich tradition of republican theorizing about security from which to draw that can help inform a robust alternative to the conventional Realist approaches dominating today. The recent NSA revelations offer an opening to make such an argument, and to push for practical solutions to widespread cyber security issues from a republican security point of view.

4.7FURTHER READING

- Ronald Deibert, “Why NSA spying scares the world,” 12 June 2013, CNN, Internet, http://www.cnn.com/2013/06/12/ opinion/ deibert-nsa-surveillance (date accessed: 30 October.
- Ronald Deibert and RafalRohozinski, Risking security: Policies and paradoxes of cyberspace security,” International Political Sociology 4» no 1 (2010): 15-32. 4 Barry Buzan, Ole Waever and Jaap de Wilde, “Security: A new framework for analysis,” London: Lynne Rienner Publishers, 1998.
- Daniel, Deudney, Bounding power: Republican security theory from the polis to the global village, (Princeton: Princeton University Press, 2008).

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How is existence of global societies relevant in present cyber security era?**

   Those who would consider themselves to be part of global civil society have been among the most persistent watch- dogs of governments and corporations, spotlighting violations of human rights online, and calling out surveillance and censorship.

4.9 ACTIVITY

Explain the reasons with incidents as to why global societies are concerned about cyber security. (1000-1500 words)

Block-2

CASE STUDIES / DATA PROTECTION

1

Unit 1: EQUIFAX DATA BREACH: CASE STUDY

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Background

1.4 Factors that contributed to the breach

1.5 External Responses to the Data Breach

1.6 Analysis of the Case

1.7 Equifax handling of the Incident

1.8 Problems Inherent with Credit Reporting Agencies

1.9 Government Response to the Incident

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible Answers

1.13 Activity

1.1 LEARNING OBJECTIVES

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

- factors contributing to the data breach
- Equifax data breach case
- government's response to the Equifax case

1.2 INTRODUCTION

One of the most notable cyberattacks of 2017 was the Equifax data leak. The attack has far-reaching consequences, involving millions of civilians as well as many corporations and government departments. In reality, the attack was so serious that the US Government Accountability Office was called in to review the incident and provide a report for Congress about how to deal with it. This chapter will investigate the facts and circumstances around this devastating cyberattack, as well as objectively examine the case's causes in order to draw conclusions on how to prevent similar exposures. Finally, a latest cyberattack would be discussed, as well as a measure of customer vulnerability to cybercrime vs. conventional crime.[36]

1.3BACKGROUND

Equifax is one of the top three credit reporting companies in the United States. Equifax announced on September 8, 2017, that it had been the target of a cyberattack that resulted in a major data leak. The world was stunned to find that 148 million US citizens' confidential personal details, including addresses, dates of birth, Social Security numbers, and driver's license numbers, had been hacked in this data breach. A total of 209,000 credit card numbers were also stolen, in addition to personal details. At the moment, the magnitude and extent of the Equifax data breach is unthinkable.[37]The vulnerability and criticality of the personal identification details in the financial information in this breach presented an issue whose size could barely be measured at the moment, despite the fact that prior breaches had been greater. The idea that Equifax's flagship offering is actually extracted from a database holding much of the US population's personal and financial records was one of the problems that compounded the Equifax data breach. Equifax keeps track of each individual's credit history, which includes personal identification details, identified addresses, and account numbers. Furthermore, since the data is collected by companies rather than people in the database, the system is not an opt-in system.[38] Lending institutions record information about payment history, balances, and other main information pieces while an individual borrows money. When anyone

[36]Thomas, Jason. (2019). A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach. 10.13140/RG.2.2.16468.76161.

[37]Marc Rotenberg, Testimony before the House Committee on Financial Services, Hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime"

[38]Atleson, M. (2019, July 2019). Equifax data breach: beware of fake settlement sites. Retrieved from Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-beware-fakesettlement-websites

applies for a loan, the new lender examines this information in order to determine the borrower's credit value, which is then used to make a lending decision.[39]

1.4FACTORS THAT CONTRIBUTED TO THE BREACH

Equifax claimed in their original statement that criminals compromised their databases from May to July of 2017. A vulnerability known as Apache Struts CVE-2017-5638 allowed criminals to gain access to Equifax systems and cause the data breach. As users go to import files, this flaw takes advantage of exception handling problems in the software's Jakarta Multipart parser. This vulnerability allows attackers to execute arbitrary commands from a remote location using a constructed Content-Disposition, Content-Type, or Content-Length HTTP header with a Content-Type header containing the characters #cmd=string (NIST, 2018).[40] Apache Struts is a well-known platform for developing fast Java applications. Since this valuable product is used by many companies, it is an excellent target for numerous cyber criminals because it can provide an access point to a large range of victims and their data. The Apache Software Foundation identified the alleged flaw and released a patch to address it. Then they made an announcement to the rest of the planet to let them know about the problems. On March 7, 2017, the patch was issued. The Department of Homeland Security notified Equifax and other credit reporting agencies of the system's failure on March 8, 2017, and instructed them to apply the patch. The Apache Software Foundation contacted Equifax systems administrators on March 9, 2017, and instructed them to install the patch. Equifax completed a search of the infrastructure on March 15, 2017, eight days after the repair announcement, seven days after warning from the Department of Homeland Security, and six days after notification from the provider. The Apache Struts vulnerability was not found in the scanner study. As a result, until July 29, 2017, the networks were unpatched and vulnerable. Equifax's security department found malicious behavior on the network around this period. Equifax shut down the program for three days before enlisting the help of an outside cyber security specialist to launch a forensic review. Most archives have been compromised, according to the initial investigation. As a result, reports were made that the sensitive records of about 145 million Americans, 8,000 Canadians, and 693,000 British people had been hacked as a result of a data leak.

1.5EXTERNAL RESPONSES TO THE DATA BREACH

Equifax's lackluster reaction to the vulnerability warning and clumsy treatment of the intrusion notification drew widespread condemnation. Equifax wanted to develop a new domain and webpage to handle all of the information that needed to be disseminated as well as engage with impacted customers and stakeholders. This perhaps well-intentioned business maneuver highlights the difficulty of coping with the issue. Other parties quickly set up bogus settlement and information pages,

[39]Marc Rotenberg, Testimony before the Senate Banking Committee, Hearing on Consumer Data Security and the Credit Bureaus

[40]Deahl, D., & Carman, A. (2017, September 20). for weeks, Equifax customer service has been directing victims to a fake phishing site. Retrieved from the verge: https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishingidentity-monitoring

opening up new avenues for bribery and cybercrime, as well as more public confusion. The platform was also flagged as a phishing hazard, which added to the accident injury. Worse, Equifax customer support used their Twitter feed to point possible users to one of the illegal phishing sites. Customers were issued PINs with naming conventions depending on the date the accounts were frozen as they flocked to freeze their credit reports. Unfortunately, this rendered them convenient for cybercriminals to figure out and exploit, allowing for even more potentially destructive assaults.[41]

Equifax was also chastised for providing free credit monitoring when attempting to limit customers' right to sue them in the terms and conditions during the registration period. When the crisis worsened and spiraled out of control, policymakers at all levels began to note and launch investigations and interventions. Equifax eventually reached a $600 million settlement with the 50 state attorneys general in the United States. The federal government took care as well. The Federal Trade Commission investigated Equifax, and Congress held numerous hearings on the matter. Bills were passed in both the House and Senate covering credit reporting agencies' business practices and privacy.

1.6ANALYSIS OF THE CASE

This data breach exposed a number of serious flaws in Equifax's treatment of the incident, as well as concerns with credit reporting agencies and the incident response process. As a result, there are many takeaways from this landmark cybercrime. In the following parts of the chapter, we'll go through some of these lessons.

1.7EQUIFAX HANDLING OF THE INCIDENT

End-users are often cited as a primary target for cyberattacks, and technology professionals frequently advise proactive user training and awareness, as well as adult-oriented training methodologies, to avoid phishing attacks and identity theft. However, it seems that the most important causal factors in this situation were system maintenance procedures. The Equifax IT team, in particular, did not implement the patch when it was released. The IT department refused to apply the fix that would have eliminated the flaw after being prompted by several outlets such as the Department of Homeland Security and the tech provider.It's worth noting that Equifax's protection staff ran a check to determine whether the flaw was present in the framework.[42] The flaw was also not detected by the scan, according to reports. This raises the possibility of other IT machine management problems. One explanation is that the scanning program was not adequately patched or upgraded, and that its list of existing vulnerabilities did not include the necessary information to

[41]Frost, A. (2018, September 6). Equifax data breach: Still haven't frozen your credit since the huge hack? Here's how. Retrieved from USA Today: https://www.usatoday.com/story/money/2018/09/06/equifax-data-breach-how-freezeyour-credit-report/1136955002/

[42]Fruhlinger, J. (2019, October 14). Equifax data breach FAQ: what happened, who was affected, was the impact? Retrieved from CSO: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happenedwho-was-affected-what-was-the-impact.html

diagnose the vulnerability. Given that the flaw was well-known, another explanation is that the scanning program was unreliable or disabled.
However, in the author's view, it's more plausible that the scanning program was out of date and therefore unable to spot the flaw. It also suggests that the Equifax IT and compliance departments may have acted negligently. A search was run to see if the flaw was still there. On several occasions, detailed instructions for applying the patch were given. The fix was clearly not introduced. Why didn't the team just check the repositories for updates to make sure they were installed? In general, this is a simple procedure that would have automatically shown that the patch has not been implemented. Equifax has a fiduciary responsibility at the executive level, both ethically and legally, to warn concerned users that their details had been hacked and to try to rectify the situation. Equifax's treatment of the case, both before and after the incident, can only be defined as poor. As previously mentioned, the attack was primarily caused by Equifax's lack of patch management diligence and cluster reaction to instructions to apply a fix to correct a recognized weakness.[43] Following that, the company seemed to behave in a way that was inconsistent with efficiently disseminating facts about the attack or effectively addressing the issue. The corporation attempted to curb consumers' right to claim civil action and restitution by selling $1.8 million in company securities before the violation was publicly revealed, ostensibly to avoid losing money on these substantial amounts of stock shares. These activities seem to suggest that Equifax and its executive team members' reactions were motivated by possible financial motives. Executive benefits are sometimes cited as motivators for leaders to make decisions in their own best interests, rather than in the best interests of their clients or other stakeholders.[44]

1.8PROBLEMS INHERENT WITH CREDIT REPORTING AGENCIES

There were also threats at the time of the attack due to the intrinsic existence of the credit reporting agency structure in the United States. Consumers are unwitting participants in the systems; they did not and do not have the ability to opt out, and their knowledge is reported by the businesses in whom they do business. For the majority of customers in the United States, this poses an unapproved and often uninformed possibility. Following the attack, there was a lot of talk about how important it was to be able to freeze credit files. Credit records have gone from being able to be frozen for a small fee to being able to be frozen for free since then.

1.9GOVERNMENT RESPONSE TO THE INCIDENT

As previously said, the incident elicited responses from governments at all stages. The responses ranged from chastising Equifax to suing for damages to enacting stricter credit reporting agency and privacy laws, as well as strict penalties against

[43]Gressin, S. (2017, September 8). The Equifax data breach: what to do. Retrieved from The Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

[44]Melin, A. (2017, September seven). Three Equifax Manager Sold Stock before Cyber Hack Revealed. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2017- 09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

Equifax. In addition to increased awareness and surveillance, the federal government spearheaded two concrete initiatives to resolve potential issues: improved credit report freezing and unfreezing capabilities, and a thorough examination of the need for data holders to alert users of data breaches. The passing of the Economic Growth, Regulatory Relief, and Consumer Protection Act is an example of this.[45]

1.10 LET'S SUM UP

The Equifax data breach was unprecedented at the time, and it was the worst and most complex data breach ever. The attack was triggered by a vendor-published identified vulnerability, and Equifax issued several alerts to install the fix that would mitigate the vulnerability. However, corporate systems maintenance and cyber security are extremely nuanced, and despite having a presumably massive IT branch, Equifax was unable to detect and trace the intrusion using traditional digital forensic techniques and systems administration procedures. Forensics investigations were carried out by an outside security firm. A catastrophic cybercrime with far-reaching consequences was enabled by the simple act of forgetting to download a patch and failing to search correctly to see if the patch was installed. New cybercrimes are created or perpetrated on a regular basis as a result of the evolving existence of technology and its growing use in everyday life and industry. When emerging technology is adopted, these crimes vary from the use of completely new tools to the commission of various forms of cybercrime, as well as the application of previous cybercrime methodologies to new goals. Cyber crime has become so common that more people are more concerned with identity fraud than about home burglaries. Cybercrime is becoming increasingly prevalent as a method of committing illegal acts due to its nuanced nature and economies of scale, as well as the lower expense and probability of committing the crimes. People are more vulnerable to cybercrime than conventional criminals because of the wide range of tools and touch points available.

1.11FURTHER READING

- Perez, L. (2017, September 8). 2019 Fed Meeting Predictions — A Fourth Fed Rate Cut Is Unlikely.
- Rajna, G. (2018). Equifax Data Breach. viXra. Retrieved 12 7, 2019
- The Apache Software Foundation. (2018). Apache Struts.
- Thomas, J. E. (2017). Lessons learned in management, marketing, sales, and finance incentive practices a decade after the Subprime Mortgage Crisis. International Journal of Business and Management, 12(3), 19-26.

[45]Oregon Department of Justice. (2019, July 22). 50 State Attorney Secure 600 Million from Equifax in the Largest Data Breach Settlement in History. Retrieved from Oregon Department of Justice: https://www.doj.state.or.us/media-home/news-media-releases/50- state-attorneys-general-secure-600-million-from-equifax-in-largest-data-breachsettlement-in-history/

- Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business and Management, 13(6), 1-24.
- Thomas, J. E., &Hornsey, P. E. (2014). Adding Rigor to classroom assessment techniuqes for non-traditional adult programs: A liifecycle improvement approach. Journal of Instructional Research, 3, 27-37.
- Thomas, J., Galligher, R., Thomas, M., &Galligher, G. (2019). Enterprise Cyber security: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques. Computer and Information Science, 12(3), 72-80.

1.12CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What vulnerability led to the breach at Equifax?**

   A vulnerability known as Apache Struts CVE-2017-5638 allowed criminals to gain access to Equifax systems and cause the data breach. As users go to import files, this flaw takes advantage of exception handling problems in the software's Jakarta Multipart parser. This vulnerability allows attackers to execute arbitrary commands from a remote location using a constructed Content-Disposition, Content-Type, or Content-Length HTTP header with a Content-Type header containing the characters #cmd=string (NIST, 2018).

1.13 ACTIVITY

Critically analyse the case study of Equifax substantiating your views with examples. (1000-1500 words)

Unit 2: WHAT'S UP WITH WHATSAPP? A TRANSATLANTIC VIEW ON PRIVACY AND MERGER ENFORCEMENT IN DIGITAL MARKETS

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Privacy Law in the United States

2.4 Privacy Law in the European Union

2.5 Privacy and Digital Market Mergers

2.6 Facebook/Whatsapp Merger

2.7 Let's sum up

2.8 Further reading

2.9 Check your progress: Possible Answers

2.10 Activity

2.1 LEARNING OBJECTIVES

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

- Privacy laws of US and EU
- Privacy and digital market mergers
- Facebook/Whatsapp merger

2.2 INTRODUCTION

Data can be thought of as the knowledge economy's raw material, and companies in markets with customer-facing digital products and services have developed business models on the processing and use of consumer data. As companies in this industry combine, it will result in a significant increase in the reach and significance of customer data under a single company's jurisdiction. Some regulators and privacy activists are concerned that the merged entity's aggregated data, when exposed to more sophisticated "big data" analytic software, would produce particularly exposing portraits of customers, making data breaches more serious and raising the risk that data will be exploited in ways that will harm customers. The first line of protection in shielding users from the threats involved with combining vast amounts of data is privacy legislation.[46] Both the United States and the European Union have strong privacy laws that aim to increase transparency and customer protection of personal information. At the same time, as the storage and use of customer data becomes more common and predictive analytic software become more strong, some privacy regulators and activists on both sides of the Atlantic have called for antitrust oversight of the privacy implications of digital market mergers, a claim first heard nearly a decade ago in conjunction with Google's purchase of Double Click.
Recently, Facebook's decision to buy WhatsApp, a social messaging app, has reignited demands for antitrust solutions to address the privacy threats that may arise as a result of digital industry mergers. In this part, we'll look at how privacy and antitrust law work together to protect consumers from privacy threats posed by digital market mergers. Despite their different legal systems, the privacy regimes in the United States and the European Union share shared goals of fostering openness and market control, according to the report.In terms of antitrust, both jurisdictions have scrutinized mergers that could affect customer privacy solely on the basis of competitive consequences. Although this lens is broad enough to catch privacy threats associated with digital industry mergers that could build or boost market dominance, it isn't intended to capture risks that aren't related to a possible reduction in competition. Privacy threats that aren't linked to reduced competitiveness are better handled by enforcing privacy laws aggressively and incorporating the new safeguards needed to protect users into those regimes.

[46]1 See, e.g., Art. 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things (Sept. 16, 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/ opinion-recommendation/files/2014/wp223_en.pdf; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter FTC PRIVACY REPORT], available at http://www.ftc.gov/sites/default/files/documents/ reports/federal-trade-commission-report-protecting-consumer-privacy-erarapid-change-recommendations/120326privacyreport.pd

2.3PRIVACY LAW IN THE UNITED STATES

Despite varying regulatory mechanisms to defend privacy in the commercial sphere, privacy authorities in the United States and the European Union articulate common goals of open data policies, real customer preference, and "privacy by nature."The United States has a "sectoral" privacy regime, which requires businesses to follow a set of focused privacy laws covering categories of information that Congress has determined warrant special protection, such as children's online data under the Children's Online Privacy Protection Act, and health information held by medical providers, hospitals, pharmacies, and insurance companies under Non-public publicly identifiable information kept by financial institutions under the Gramm-Leach-Bliley Act, some information for decisions about a consumer's eligibility for credit, jobs, insurance, and other services under the Health Insurance Portability and Accountability Act (HIPAA), non-public personally identifying information retained by financial institutions under the Gramm-Leach-Bliley Act, certain information for decisions about a consumer's eligibility for credit, jobs, and insurance under the Gramm-Leach-BliUnder the Fair Credit Reporting Act (FCRA), or homes, and under the Video Privacy Protection Act, video rental documents.[47] The Fair Information Practice Principles, a series of privacy standards that has served as the framework for privacy regimes around the world, are the basis for these targeted regulations. As a result, any or more of the fair information practice rules, such as warning and an ability to respond to the storage and use of personal data, appropriate data access, and limitations on the reasons for which data can be collected, such as those contained in the FCRA, are usually mandated by U.S. privacy legislation. The key federal protections for the vast body of data that lies outside of these discrete areas are contained in the FTC Act's broad bans on "deceptive" or "unfair" commercial activities and practices. 8 After the 1990s, as the Internet became widely used, the FTC has used its power to regulate both online and offline commercial data activities. Data protection is a significant component of this regulatory operation.

The FTC has brought a relentless stream of lawsuits against corporations accused of failure to take appropriate action to protect customer data, enforcing the bans of both misleading and unfair practices. For example, in 2008, the FTC charged The TJX Companies with engaging in unreasonable and thereby discriminatory activities by storing and distributing personal information in its network in unencrypted code, failing to require network administrators to use strong passwords, and failing to use firewalls to restrict access among its customers, after what was at the time the largest breach of payment card details. Outside of data protection, the FTC has used the fraud ban to accuse businesses of making false or misleading statements about what customer data they would gather or how the data would be used or exchanged. For example, the FTC claimed in Snapchat that a smartphone app deceptively promised users that their videos and photo messages would be permanently deleted after a brief time period set by the user, while receivers had readily accessible means to save the videos and images. The FTC has challenged retroactive modifications to data procedures made without affirmative express approval, citing the ban on discriminatory actions or practices. The FTC, for example, said that when

[47]See, e.g., ASIA-PACIFIC ECONOMIC COOPERATION, PRIVACY FRAMEWORK (2005); ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (rev. ed. 2013)

Facebook revamped its website in December 2009, it unjustly overrode users' privacy settings, which had limited access to such information such as a profile picture and Friends List, without their informed consent. In addition, the FTC said that the misleading storage of extremely private data by the covert installation of spyware and key loggers on laptop computers was an unfair practice in lawsuits lodged against Aaron's rent-to-own franchisor, a number of its franchisees, and a software designer. In FTC v. Frostwire, LLC, the lawsuit claimed that a tech company's inability to warn consumers that many pre-existing files on computers and mobile devices would be reserved for public sharing was an illegal practice.[48]
Growing gaps in the United States' user protection legal system have arisen from changes in technology and corporate practices. Health data is now often in the possession of companies that are not protected by HIPAA, thanks to emerging technology and business models including smart workout bands and mobile health applications. Similarly, outside standard credit ratings, new products that claim to forecast or "rate" anything from the likelihood of a purchase resulting in theft to the feasibility of sending customers catalogs and the best rates to give consumers are typically exempt from the FCRA. To close these gaps, the FTC has backed "baseline" privacy regulations as well as data broker legislation. Similarly, the Obama administration has asked Congress to pass laws establishing a Consumer Protection Bill of Rights, which it hopes to enforce by multi-stakeholder meetings to develop cooperative codes of ethics in areas such as smartphone privacy disclosures and facial recognition.[49]

2.4PRIVACY LAW IN THE EUROPEAN UNION

Unlike the United States, where the Constitution only safeguards individual privacy from government action, the European Union has had a "protection of personal data" enshrined in the EU Charter of Fundamental Rights since 2000.[50] In addition, unlike the U.S. privacy regime, which is characterized by a complex mix of federal sectoral laws, the FTC Act, state laws, and private rights of action, a general EU data protection directive adopted in 1995 (General Directive) establishes comprehensive principles to limit the "processing"—a broadly defined term—of all "personal data," which includes "any information relating to an identifiable individual."Each member state enacts its own legislation to incorporate the General Directive, which is administered by one or more autonomous data protection agencies in each state. Personal data must only be processed for defined, explicit, and valid reasons under the General Directive, and must not be processed for an incompatible cause later. The approval of the user - the "data subject" in EU jargon - at the time of data

[48]See generally PAM DIXON & ROBERT GELLMAN, THE SCORING OF AMERICA: HOW SECRET CONSUMER SCORES THREATEN YOUR PRIVACY AND YOUR FUTURE 9–11 (2014), available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf; Press Release, Fed. Trade Comm'n, FTC Announces Agenda, Panelists for Alternative Scoring Seminar (Mar. 14, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/03/ftc-announces-agenda-panelistsalternative-scoring-seminar

[49]FTC PRIVACY REPORT, supra note 1, at 12–13; FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 49–54 (2014) [hereinafter FTC DATA BROKER REPORT]

[50]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (L 281) 31.

collection is one legal justification for collecting personal data. Furthermore, the storage and use of personal data must be equal to the reason for which it was collected in the first place. The General Directive also stipulates that data collection must be clear, which means that individuals must be informed of the intent of the processing as well as the recipients or groups of recipients to whom data is disclosed.[51] Similarly, data controllers must take reasonable steps to ensure the data's protection. Individuals have the freedom to view data gathered on them, according to the General Directive. In implementing the General Directive, the European Court of Justice recently held in Google Spain, SL v. González that search engines are "data controllers" and must delete connections to personal records that are incomplete, insufficient, unnecessary, or disproportionate in relation to the original reason for which the data is stored, upon request. The court clarified that the extent of this so-called "right to be overlooked" would be determined on a case-by-case basis and would have to be weighed against Internet users' rights to access content.

The EU is replacing the General Directive and member state implementation legislation with a single, statutory data protection policy across the EU in order to modernize its data protection regime. On March 12, 2014, the European Parliament adopted a draft of the new legislation. The establishment of a "one-stop shop" in which each data protection authority will manage all EU compliance activities for entities with EU headquarters in its jurisdiction is one of the main features of the Parliament-approved legislation. The law, which was passed by Parliament, would also provide a right to data portability, allowing individuals to move their data from one digital network to another. If a company is deemed to have breached the new law, it will face penalties of up to 5% of its annual revenue or 100 million euros, whichever is greater—a significant improvement from the actual fines already imposed on most individual data protection authorities. The final text of the legislation must be negotiated and approved unanimously by the EU Parliament and the EU Council of Ministers before it can become law.

2.5PRIVACY AND DIGITAL MARKET MERGERS

Despite increased attempts on both sides of the Atlantic to defend data privacy, privacy authorities and activists have turned to antitrust legislation to protect customers from the privacy threats associated with digital industry mergers. The combination of massive data sets that can result from mergers in this market, according to advocates and regulators, poses two key privacy threats. First, as businesses amass more detailed and revealing profiles of their customers, a single data breach will result in a broader trove of information falling into the hands of hackers, ultimately placing customers at greater risk of malicious behavior. Second, as richer data sets are subjected to predictive analytic tools, firms will be able to draw more revealing inferences about customers and make finer-grained distinctions between them, potentially increasing the likelihood of differential treatment in terms of what products and services are marketed to them, the prices they are charged, and the level of customer service they get, potentially outside of the

[51]See THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 35–39 (2012), available at http://www.white house.gov/sites/default/files/privacy-final.pdf.

telecommunications industry. In competition investigations, the European Data Protection Supervisor (EDPS), an EU privacy regulator, has emphasized the competitive ramifications of data, especially the relationship between data, entry barriers, and market influence.[52] The European Data Protection Supervisory Authority (EDPS) suggested in a preliminary opinion on the interplay between data protection and competition law that merger enforcement in digital markets should be based on a broader definition of consumer harm that goes beyond looking solely at competitive effects and accounts for risks to consumer privacy from the combination of large datasets that aren't always linked to a reduction in competition.

In the areas of data security, customer protection, and competition at the intersection of these areas, the EDPS called for further consultation among regulators. Many of these topics were revisited in a follow-up workshop and study. 37 In her opposition from the FTC's decision to close its inquiry into Google's purchase of DoubleClick in 2007, then-FTC Commissioner Pamela Jones Harbour raised some of the questions that the EDPS raised. Harbour has pressed enforcers to create a more sophisticated methodological system for assessing the antitrust ramifications of privacy and big data since leaving the department. Howard Shelanski, then-FTC Bureau of Economics Director, has also recommended that antitrust enforcers focus on the potential exclusionary effects of acquiring customer data, which "can reveal horizontal dimensions of facially vertical conduct and transactions," and recognize privacy protection as a significant non-price dimension of competition in digital markets, in a letter written in his personal capacity, Revisiting Google/DoubleClick. In 2007, after investigating Google's acquisition of DoubleClick, the FTC for the first time publicly grappled with the intersection of privacy and antitrust. In both the United States and Europe, Google was the leading source of search advertisements, and both firms were major players in the market for online display advertising, which consists of graphic advertisements that appear on websites that use icons such as corporate logos to create brand identity. Websites also offer premium advertising space, which is typically found in the top half of a website, to in-house personnel and rely entirely on third-party "ad servers" to handle the scheduling and location of those advertisements.

Websites typically use "ad intermediaries" to monetize their less lucrative real estate, which buy, aggregate, and market the property to marketers. Google was a major online advertisement intermediary for its AdSense product, and DoubleClick was a leading online ad server. The proposed consolidation of data held by Google and DoubleClick on user web search and browsing behavior sparked concerns among privacy advocates. The Electronic Privacy Information Center (EPIC), the Center for Digital Democracy (CDD), and the United States Public Interest Research Group (US PIRG) filed a lawsuit with the Federal Trade Commission (FTC) opposing the merger on the basis of privacy concerns. They also believed that combining the data would give Google a strategic edge over competitors in both search and display ads, enabling it to "monitor the process of monetizing web content." The FTC and the EC also published a thorough review of the transaction's strategic consequences as part of their unconditional approval of the merger.

[52]Robert McMillan, You May Not Use WhatsApp But the Rest of the World Sure Does, WIRED (Feb. 20, 2014, 8:17 PM), http://www.wired.com/ 2014/02/whatsapp-rules-rest-world/; Mike Isaac, Zuckerberg: More Than 200 Million People Use Facebook Messenger, RE/CODE (Apr. 23, 2014, 3:04 PM), http://recode.net/2014/04/23/zuckerberg-more-than-200-millionpeople-use-facebook-messenger.

In the competition for web advertisements or utilities, both companies determined that Google and DoubleClick were not near real or future rivals.[53] They also discovered that, due to its lack of market control, DoubleClick could not remove content intermediation competitors by bundling AdSense with DoubleClick's publisher ad server. Since DoubleClick's contracts did not allow Google to use the details to target advertising, and Google committed that it would not combine the data post-merger, no jurisdiction was convinced that the combining of data would offer AdSense an anticompetitive advantage over rivals.More specifically, both jurisdictions determined that, even though Google amended or broke these arrangements, DoubleClick's data were not exclusive, and that rival ad intermediaries could obtain comparable data of similar quality and quantity from other outlets. The FTC determined that the antitrust laws did not include a reason to attempt to prohibit or enforce restrictions on a merger solely to protect privacy, despite voicing a firm commitment to privacy and acknowledging that FTC workers have recently proposed a package of privacy standards for online behavioral advertisements. The FTC has stated that privacy is a non-price dimension of competition, and that it has the right to intervene where a deal is likely to minimize competition on that basis. However, it concluded that harm to competition on the basis of privacy was no more possible in this deal than harm to competition on the basis of price or other non-price dimensions. As a result, it came to the conclusion that "privacy interests, as such, do not provide a basis for challenging this transaction."The EC also assessed the agreement purely on the basis of its competitive consequences, while stressing that its decision did not affect the parties' different obligations under European data protection legislation.

2.6FACEBOOK/WHATSAPP MERGER

Related allegations were made to the FTC during its latest investigation of Facebook's planned purchase of WhatsApp.[54] Facebook, a social network with over a billion active monthly users worldwide, now provides networking platforms that enable users to send and receive text messages, images, and other digital content through its "Messenger" mobile app and its social network's messaging feature. Facebook revealed on February 19, 2014 that it had decided to pay $16 billion for WhatsApp, an instant messaging service. WhatsApp, like Facebook Messenger, has a smartphone app that helps members to deliver text messages and other multimedia content to other WhatsApp users over the Internet without having to pay for short message service. WhatsApp had 450 million subscribers globally when the acquisition was completed, with the bulk of them based outside of the United States. Messenger has 200 million daily users, according to Facebook. WhatsApp has marketed itself, at least in part, on the fact that it would not mine users' personal data to sell ads. "Your data isn't even in the picture," WhatsApp claims. We simply don't care for all of it." 50 WhatsApp advised users on the day of the takeover that the deal would change "nothing" for them in this respect. A few days later, Facebook CEO

[53]See Ellen Nakashima, Privacy Group Objects to DoubleClick Deal, WASH. POST (Apr. 20, 2007), http://www.washingtonpost.com/wp-dyn/content/ article/2007/04/19/AR2007041902647_pf.html.
[54]Complaint at 7–9, Facebook, Inc., FTC Docket No. C-4635 (July 27, 2012), available at http://www.ftc.gov/sites/default/files/documents/cases/ 2012/08/120810facebookcmpt.pdf

Mark Zuckerberg was quoted as saying that the company would not "change its plans about WhatsApp and how it uses user data."
Despite these promises, privacy activists expressed reservations about the deal. EPIC and CDD filed FTC lawsuits opposing the planned purchase, repeating many of the claims leveled against Google/DoubleClick. They argued, in particular, that Facebook's business model contradicted WhatsApp's assurances to subscribers regarding how their mobile data would be gathered and used, and that WhatsApp failed to properly reveal that its privacy obligations could be rescinded or that customer data could be moved in the case of an acquisition.They asked the FTC to look at WhatsApp's actions and use its "authority to review mergers" to put a stop to Facebook's planned takeover of WhatsApp before the questions raised in the lawsuit is addressed. The groups asked the FTC to "order Facebook to insulate WhatsApp users' details from links to Facebook's data collection practices" if the transaction was approved. The FTC cleared the transaction on April 10, 2014, according to Facebook. The FTC does not usually release a statement outlining the specifics of its analysis when it concludes a merger investigation without taking action, and it did not do so here. However, on the same day as Facebook received approval, Jessica Rich, Director of the Federal Trade Commission's Bureau of Consumer Protection, wrote to Facebook and WhatsApp, stating that Facebook's acquisition of WhatsApp would not invalidate the commitments provided by both companies in WhatsApp's privacy policy, as well as public comments made by both companies regarding privacy when the deal was revealed.
As a result, Rich clarified, businesses can not make any material changes about how they employ data already gathered from WhatsApp users without affirmative express permission, nor can they misinterpret how they keep WhatsApp consumer data. Failure to take these measures, she warned, may be considered misleading or discriminatory actions and activities, in breach of the FTC Act and a 2012 FTC consent order against Facebook. Rich's note, although released at the conclusion of the inquiry, did not place restrictions on the merger, as the FTC does when it has cause to suspect an agreement would damage competition in the consent decree process.[55] Instead, the letter spells out the responsibilities that all businesses must meet when it comes to the acquisition, handling, and utilization of customer data, both before and after a merger. On August 29, 2014, the EC launched an investigation into the Facebook/WhatsApp merger. On October 3, 2014, the European Commission announced that the deal had been approved without conditions, stating that the merger was unlikely to affect competition in three areas of concern: consumer information services, social networking services, and online advertisement services. In terms of networking services, the EC determined that, while Facebook Messenger and WhatsApp serve identical roles, the companies are not direct competitors, owing to the fact that Messenger links users via their Facebook accounts, while WhatsApp relies on cell phone numbers.
Consumers use the services in a variety of ways, according to the EC, with those using both apps on the same computer. Furthermore, the European Commission determined that the demand for digital connectivity platforms was quickly expanding and that the obstacles to introducing new applications were limited. Although the EC acknowledged that network effects can often limit entry in telecom markets, it

[55]U.S. Horizontal Merger Guidelines, supra note 64, at 2; Guidelines on the Assessment of Horizontal Mergers Under the Council Regulation on the Control of Concentrations Between Undertakings 2004 O.J. (C 31) 5, ¶ 8, available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX: 52004XC0205(02).

determined that the merger would not lift hurdles because “consumers can and do use multiple applications at the same time and can quickly migrate from one to another.”Similarly, the European Commission concluded that in the field of social networking, the companies are at most “distant rivals” in a competitive industry with no clear borders and a large number of potential participants. Finally, the European Commission dismissed the possibility of competitive damage in online advertisements. The EC determined that even if Facebook used WhatsApp to extend the store of data it uses to target ads, it would also face significant rivalry in this area, in part because data on users’ online activity is open to competitors from alternative outlets, as it did in Google/ DoubleClick. The EC did not analyze privacy concerns associated with the “potential data concentration” that were not applicable to evaluating competitive results when it approved the merger. Instead, it argued, as it had in the case of Google/DoubleClick, that “any privacy-related issues arising from the enhanced accumulation of data under Facebook’s jurisdiction as a result of the purchase do not come within the limits of EU Competition law.”

2.7 LET’S SUM UP

Despite the possible connection between privacy issues and big data mergers, guidelines from both the US and the EU clearly signals that no jurisdiction can use antitrust regulation to oppose a deal that poses privacy concerns without causing a reduction in competition. In both Google/DoubleClick and Facebook/WhatsApp, the FTC and the EC rejected the opportunity, and a different conclusion would be inconsistent with both jurisdictions’ takeover compliance rules, which examine transactions exclusively on the basis of competitive results.As a result, merger enforcement has the power to supplement privacy legislation only in such situations where protecting competition still protects consumer privacy. Antitrust authorities in the United States and the European Union have yet to respond in a situation where the link was obvious. However, as emerging technology and business models make data collection and processing a virtually universal part of daily life, we should anticipate concerns about antitrust enforcement’s position in shielding customers from privacy threats associated with digital sector mergers to begin to appear in transaction reviews on both sides of the Atlantic.

2.8FURTHER READING

- The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 35–39 (2012).
- Joseph E. Stiglitz, Imperfect Information in the Product Market, in 1 Handbook of Industrial Organization.

2.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What privacy policy and principles are followed by United States?**

The United States has a "sectoral" privacy regime, which requires businesses to follow a set of focused privacy laws covering categories of information that Congress has determined warrant special protection, such as children's online data under the Children's Online Privacy Protection Act, and health information held by medical providers, hospitals, pharmacies, and insurance companies or Non-public publicly identifiable information kept by financial institutions under the Gramm-Leach-Bliley Act, some information for decisions about a consumer's eligibility for credit, jobs, insurance, and other services under the Health Insurance Portability and Accountability Act (HIPAA), non-public personally identifying information retained by financial institutions under the Gramm-Leach-Bliley Act, certain information for decisions about a consumer's eligibility for credit, jobs, and insurance under the Gramm-Leach-Bli or Under the Fair Credit Reporting Act (FCRA), or homes, and under the Video Privacy Protection Act, video rental documents. The Fair Information Practice Principles, a series of privacy standards that has served as the framework for privacy regimes around the world, are the basis for these targeted regulations.

2.10 ACTIVITY

Critically analyse the privacy laws of United States and European Union. (1000-1500 words)

3

Unit 3: FACEBOOK DATA THEFT IN INDONESIA

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Problems and Methods

3.4 Data Breaker Facebook in Indonesia: Case Analysis

3.5 Expert Opinion Regarding Facebook data breaker case

3.6 NGO Comments on the Hack top of Privacy

3.7 The Government Measures

3.8 Let's sum up

3.9 Further reading

3.10 Check your progress: Possible Answers

3.11 Activity

3.1 LEARNING OBJECTIVE

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

- Overview of crimes affecting economy
- Different kinds of cybercrimes using the computer and Internet
- Legal provisions pertaining to it

3.2 INTRODUCTION

The use of information technology in Indonesia has increased positively from year after year. Progress has been mentioned since the entry of the internet theology to the homeland since in 1988. The harmony between the development of information technology with the media and telecommunications today has resulted in a growing variety of services and existing products. The convergence of these technologies is called telematics (telecommunications, media, and informatics). The use of the Internet in various fields in our lives not only makes things easier but also causes some problems, one of which is the legal problem. One of the legal issues which may occur are issues related to the protection of privacy rights. The right to privacy is the privacy rights possessed by a person of his or her privacy. This right becomes private because it involves information that cannot be owned or submitted to all party without the permission of the owner of that identity. Some experts express this basic understanding of the right to privacy.[56]

Professor of public administration law from the University of Colombia, Alan Westin, defines the right to privacy as claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. The extent of privacy coverage usually makes the number of privacy settings in a country, both in type and level.[57] The notion and scope of other privacy concepts often referred to be the formulations developed by William Posser, referring to at least four things: (a) Disturbance of a person's act of alienation or aloofness, or interference with his relationships (b) Disclosure of personal facts publicly embarrassing (c) The publicity that puts a person wrong in public opinion (d) Unauthorized control of a person's likeness for the benefit of others.3 In international legal instruments, freedom of privacy is recognized as inherent basic rights to every human being. This provision is contained in the Universal Declaration of Human Rights. The Declaration has provided the legal basis for its member states in respect of the state's obligation to protect and respect the right of the individual's private citizens.

This provision is explicitly stated in Article 3 and Article 17 of the Universal Declaration of Human Rights. Article 3 set the right of the person as follows: "Everyone has the right to life, freedom, and liberty as an individual. "While Article 17 to protect the freedom in two paragraphs, namely: (1) Everyone has the right to own property alone or jointly with others; (2) No one shall be deprived of his property arbitrarily. Both the terms of the Universal Declaration of Human Rights above

[56]AF Westin, Privacy and Freedom, New York: Atheneum, (1967), pp. 7-8

[57]Natamiharja, Rudi. (2018). A Case Study on Facebook Data Theft in Indonesia.FIAT JUSTISIA. 12. 206. 10.25041/fiatjustisia.v12no3.1312.

provide for the broad protection of the right to privacy. But this is the embryo of the emergence of more specific protection classified into two classes of protection, first against civil rights and political rights, the second is the protection of economic, social and cultural rights or known as "ECOSOC" originating from International Covenant on Economic, Social and Culture Rights. Furthermore, the International Covenant on Civil and Political Rights (ICCPR), which was born on December 16, 1966, through Resolution 2200A and entered into force on 23 March 1976 provides more protection for the rights of the human person. Indonesia has ratified the ICCPR on 28 October 2005 through the Law of the Republic of Indonesia Number 12 the Year 2005 on the Ratification of the International Covenant on Civil and Political Rights.

The State of Indonesia state based on the rule of law and it's obliged to embody this international provision in a positive, applicable and positive contribution to its citizens. The importance of this rule must be felt in everyday life.[58] So that the people of Indonesia do not feel anxious personal data will be used or known to other parties that he does not desire. One example of cases of personal data protection in Indonesia is about the theft of users of social media data Facebook. Facebook reveals the number of users whose data is utilized by Cambridge Analytica to reach 87 million users of Facebook, about 1 million of whom belong to users of Facebook in Indonesia. Indonesia is the third biggest country after the United States and the Philippines whose data are used. This data theft incident stems from the cooperation of Facebook and the application "thisisyourdigitallife." According to data compiled by Facebook Indonesia, 748 people have installed the application "thisisyourdigitallife" from November 2013 until December 2015. There are additional more than 1 million users who are affected by the friends of the user application. Then there are a total of 1,095,918 users whose data are stolen or 1.26 % of the total affected users globally. The meeting between the Commission 1 of the House of Representatives and Facebook been held. House of Representatives worried about Facebook data will affect the Indonesian political year of elections and elections simultaneously 2019 because Cambridge Analytica reportedly ever used a Facebook user information related to US presidential elections in 2017 and where the underdog Trump has managed to win his fight with Hillary Clinton. The disappointment of the House against Facebook is the absence of law enforcement from Facebook to third parties (Cambridge Analytica). The government's irresponsiveness in taking action has sparked the question of whether the provision in Indonesia is sufficient to cover its citizens or whether it is the House of Representatives' reluctance to resolve the issue. After the amendment of the The 1945 Constitution of the Republic of Indonesia (Undang-UndangRepublik Indonesia 1945), Law Number 11 on 2008 of Information and Electronic Transactions or abbreviated as the ITE Law was established. Then some articles of the law have improved in 2016 which became known as the Law Number 19 Year 2016 on the Amendment of Law Number 11 on 2008 of ITE. The establishment of the ITE Law is a mandate of the 1945 Constitution of the Republic of Indonesia, including articles relating to personal data, rights to privacy. In the elucidation of Article 26 paragraph 1 of Law Number 19 Year 2016 it is stated that the definition of personal rights is, the right to enjoy private and free life,

[58]Oik Yusuf, "Data 1 JutaPengguna Facebook Indonesia Dicuri", Kompas, April 05, 2018, https://tekno.kompas.com/read/2018/04/05/10133697/data-1-juta-user-facebook-indonesiadicuri, (accessed June 12, 2018).

the right to be able to communicate with others without spying action, the right to monitor access to information about personal life and data someone.
In Article 17 paragraph 3 of Regulation of the Minister of Communication and Informatics Number 12 of 2016, it is clearly stated that the Telecommunication Service Provider must keep the data and the identity of the customer confidential. The rules of personal data protection are outlined in the Ministerial Regulation No. 20 of 2016 on Personal Data Protection (PDP) set on November 7, 2016, enacted and effective from 1 December 2016. In the rule, it is stated that Personal Data is certain personal data stored, cared for, and safeguarded by the truth and protected by its secrecy. In this rule, an electronic system that can be used in the process of protecting personal data is an electronic system that has been certified and has internal rules on the protection of personal data which must pay attention to aspects of the application of technology, human resources, methods, and costs. The owner of the personal data, is entitled to the confidentiality of his data; have the right to lodge a complaint in order to settle a private data clause; entitled to access to obtain historical personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system. Through the existing personal data rules in Indonesia, it can be concluded that the protection of personal data in Indonesia is insufficient because it has no comprehensive laws or rules regarding the protection of personal data protecting its citizens from data misuse. It is, therefore, necessary to create a Personal Data Protection Law that has clarity of rules on the recovery of victims. Citizens also need to be educated about digital privacy to understand the potential risks that exist and the right to protect privacy and personal data.[59]

3.3PROBLEMS AND METHODS

Based on the background described above, the first issue to be described in this chapter is the extent to which regulations in Indonesia have covered the protection of personal data. The second issue, what the Government of Indonesia should take policies and steps in providing privacy data protection?

3.4DATA BREAKER FACEBOOK IN INDONESIA: CASE ANALYSIS

In 2013, Cambridge University researchers named AleksandrKogan created a personality quiz app, “thisisyourdigitallife.” Mark Zuckerberg revealed that the Kogan app is in use by around 300,000 people all of whom are willing to share their data as well as some data from their friends. Then Facebook changed the platform policy to limit the data accessible to the app a year later.[60] Such changes make developers like Kogan unable to request friend data from users unless their friends also access the app. In 2015, Facebook got information from the media that Kogan has shared

[59]A sample case can be found at https://tekno.tempo.co/read/1080112/dpr-bert -facebookbesok-bahas-skandal-data.
[60]KustinAyuwuragil, “KronologiPembobolan Facebook oleh Cambridge Analytica”, CNN Indonesia, March 03, 2018, https://www.cnnindonesia.com/teknologi/20180322194919-185- 285163/kronologi-pembobol-facebook-oleh-cambridge-analytica.

its data on Cambridge Analytica. Kogan has violated Facebook's policies for illegally obtaining data so that the platform removes the Kogan app. Cambridge Analytica does not delete all data as they promised before. Facebook took action to block Cambridge Analytica from its services. Cambridge Analytica argues that they have deleted all the data. They even agreed to be audited forensically by the Facebook-appointed company, Stroz Friedberg, to confirm the incident. The misuse of data by Kogan is widely cited as the largest data theft in history. Facebook reveals the number of users whose data is utilized by Cambridge Analytica to reach 87 million Facebook users, about 1 million of whom are owned by Facebook users in Indonesia. Indonesia is the third largest country after the United States and the Philippines whose data is utilized without seizing Facebook users.[61]

3.5EXPERT OPINION REGARDING FACEBOOK DATA BREAKER CASE

Cyber security expert, PradamaPersadha expertise from Indonesian Security Research Institute of Cyber and Communications assesses that Indonesia is difficult to act firmly against Facebook in case of data leakage involving data of more than one million users of social media applications owned by Indonesian citizens. This is because Indonesia does not have high bargaining power. Facebook Indonesia is currently still searching for data related to the leak and promised to conduct an internal audit as soon as the data is obtained even without detailing when the investigation was completed.[62] This promise has previously been conveyed by representatives of Facebook Indonesia in a Public Hearing Meeting (RDPU) with the Commission 1 House of Representatives, in April. Commission 1 of the House gives a one-month deadline for Facebook to submit its internal audit results. The results will be used to measure potential hazards that could result from data leak incidents. Meanwhile, he said that the call to Facebook manager in Indonesia would not have a significant impact on the settlement and follow up of the case. Because currently, Indonesia does not have "bargaining power" to force Facebook to follow government rules. On the contrary, according to Pratama, this case should be momentum for Indonesia to start its independence in the field of social media application services, while exemplifying China that prohibits Google to operate in the country and has its microblogging site called Weibo. But he admitted it is still far to materialize considering Indonesia has no resources either Human Resources (HR) and infrastructure. For now, the least that the government can do is to urge the FB to minimize the impact of data leakage for example if it is used for political purposes such as in the United States.

3.6NGO COMMENTS ON THE HACK TOP OF PRIVACY

SintaDewi, Chairman of Cyber Law Center in Faculty of Law Padjadjaran University, stated that the interests of personal data protection regulations are increasing. This will be related to information technology business on security and data protection. It

[61]Fatimah KartiniBohang, "DPR BeriWaktu Facebook 1 Bulan", Kompas, April 17, 2018, https://tekno.kompas.com/read/2018/04/17/16240047/dpr-beri-waktu-facebook-1-month

[62]Antara, "Data Bocor, Elsam: Menutup Facebook BukanSolusi" Tempo, April 11, 2018, https://bisnis.tempo.co/read/1078332/data-bocor-elsam-closing-facebook-not-solution.

also becomes one of the necessities in ensuring the sustainability of the digital economy in the future. Deputy Director of Research ElsamWahyudiDjafar, strengthen SintaDewi's opinion citing the resolution of the board of Human Rights in 2012 and 2013 adopted by the UN General Assembly which refers to Article 19 of the Covenant on Civil Rights and Political, states that: "the protection of all people when they are offline it will also apply when they are online "and" privacy protection on someone when they are offline it is also attached if they are online ".[63] Under both resolutions, the UN encourages member states to revise its privacy-related national laws. Facebook's case according to WahyudiDjafar, is an analytic data engineering that is not in line with the protection of the privacy of its citizens. If it persists, this practice will be perpetuated by affecting the preferences of the social choice of the social user with the consequences of excluding the rights of individual citizens. Hearing the explanation of experts from the civil society Vice Chairman of Commission I of the House of Representatives, Satya WidyaYudha acknowledges the urgency of this PDP Act. Even He also urged the Parliament to make laws for the PDP as a law a priority in the 2018-2019 national legislation. According to him, at this hearing, there was not a single fraction against the establishment of the PDP Law, so there is no reason for the House to postpone it. The Institute for Policy Research and Advocacy (Elsam) believes that closing Facebook access in Indonesia due to the misuse of user data by third parties is not the right solution.

Deputy Director of Research ElsamWahyudiDjafar encourages the implementation of audits with the government and Facebook to find out where the violations, what data is leaked, and what data is transferred. The issue of blocking or closing is according to him, usually depart from content issues, but for Facebook started from the issue of personal data of Facebook users. So do not have the right reasons if there is a Facebook shut down. When Facebook is closed, he fears it will limit the right of public information that has been able to communicate through Facebook and retrieve information from social media. In addition to a joint audit, it proposes a recovery mechanism against Facebook users who violated their privacy, then the obligations that must be charged to Facebook, such as updating terms of service or privacy policy to comply with privacy provisions. This is done so that the practices of alienation or misuse of data do not happen again. Also, in the future, Facebook needs to be encouraged to educate its service users, not only do recording of data or content uploaded on Facebook for large-scale data collection. In response to this Facebook case, Elsam sees the importance of placing human rights as the direction of its development. Human rights must be formulated in the form of a legal instrument as a guarantee of public protection. Normative forms are important for placing state responsibility and affirming the role of corporations in protecting people's privacy rights. This assurance of protection will ensure that technology and machinery work including artificial intelligence, for the benefit of data collection, will be in line with the principles of privacy protection. It can be concluded that the government has done various actions to solve the case of personal data protection data theft Protection of this Facebook, but the action is not sufficient because until now there has been no settlement from the Government and Facebook. The law in Indonesia implicitly provides for the guarantee of the right to privacy. Unfortunately, the legal regulation has not been properly outlined in the level of legislation.

[63]Quoted from http://elsam.or.id/2018/05/elsam-menghadiri-rapat-dengar-pendapat-umumdari-panja-pengamanan-data-ponsel-komisi-i-dpr-ri/.

Countries with low data protection laws such as Indonesia may be subjected to irresponsible companies for theft of personal data for their benefit.

3.7THE GOVERNMENT MEASURES

Minister of Communications and Informatics, Rudiantara, said his side keeps escorting the effort to hold Facebook accountable. Because of the possibility of account data in Indonesia abused that is to affect the results of elections next year (2019). The government has sent a letter to Facebook related to the theft of Facebook data in Indonesia to request confirmation and explanation of the case.[64] The government can also press Facebook to immediately close access to applications that allow the theft of personal data users. The company should not submit to the account owner to actively disable the leak-prone application. Facebook needs to be responsible for the privacy of its users. The Ministry of Communication and Informatics does not stand alone but also cooperates with the police. The Ministry of Communication and Informatics only takes care of administrative sanctions, while for criminal sanctions the process is carried out by the police. Relate leaked data social media platform Facebook, Rudiantara rate the process is not easy because Facebook is pursued quibble pending audit results from the authority in the UK, namely Information Commissioner Office (ICO).

3.8 LET'S SUM UP

Protection of the security of private data must have a place as a basic right that needs to be protected and attached to each. Such protection should not appear when data theft has occurred. The basic thing that needs to be considered and more effective is to build public awareness. The Ministry of Information and the Government of Indonesia must be able to provide and enrich people's knowledge of the importance of privacy data.

3.9FURTHER READING

- David, Robert. (2004). A dictionary of Human Rights. Europa, London, New York.
- Freeman, Marc and Gibran Van Ert. (2004). International Human Rights Law. Canada: Irwin Law Inc.
- The Institute for Policy Research and Advocacy (Elsam). (2015). Privasi 101 PanduanMemahamiPrivasi, Perlindungan Data danSurveilansKomunikasi. Norman E. Bowie, Karim Jamal. (2006).

[64]Quoted from https://www.kominfo.go.id/content/detail/13163/rudiantara-bakal-insiasiregulasi-soal-konten-medsos/0/sorotan_media.

- Privacy Rights on the Internet: Self-Regulation or Government Regulation. Business Ethics Quarterly. https://doi.org/10.5840/beq200616340
- Raymond, Wacks. (2013) Privacy and Media Freedom. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199668656.001.0001
- Westin, A.F. (1967). Privacy and Freedom. New York: Atheneum

3.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What do Articles 3 and 17 of UDHR state?**

   Article 3 and Article 17 of the Universal Declaration of Human Rights. Article 3 set the right of the person as follows: “Everyone has the right to life, freedom, and liberty as an individual. “While Article 17 to protect the freedom in two paragraphs, namely: (1) Everyone has the right to own property alone or jointly with others; (2) No one shall be deprived of his property arbitrarily. Both the terms of the Universal Declaration of Human Rights provide for the broad protection of the right to privacy.

3.11 ACTIVITY

Based on the case study provide with your opinion and solutions on how to curb such data thefts.(700-1000words)

4

Unit 4: YAHOO DATA BREACH

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Breach of 2013

4.4 Breach of 2014

4.5 Business Impact

4.6 Financial Implications

4.7 Regulatory Violations

4.8 Recommendations against hacking

4.9 Let's sum up

4.10 Further reading

4.11 Check your progress: Possible Answers

4.12 Activity

4.1 LEARNING OBJECTIVE

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

- Yahoo data breach during different times
- The impact on data breach on business
- Recommendations against hacking

4.2 INTRODUCTION

What a relief! At the end of 2016, an online service provider had announced two large data breaches involving over 1.5 billion users. Following further investigation, Yahoo announced that the cyber security breach had infected its 3 billion accounts. This is regarded as one of the most serious data leaks in the history of online service providers.[65]

Yahoo CEO Marissa Mayer's attempts to restore the company's previous success failed. Verizon announced in 2016 that it would buy Yahoo for $4.83 billion, but the sale fell apart due to Yahoo's disclosure of the data breaches. Yahoo's universe was turned upside down after it was revealed in 2014 that it had experienced data breaches. User names, email addresses, phone numbers, dates of birth, hashed keys, and certain encrypted and unencrypted security questions were stolen in the cyber-attack, which affected 500 million users. They made the public aware of the breach in 2016 and suspected it was the work of state-sponsored hackers. In an unexpected turn of events, Yahoo lodged an SEC report in early September claiming ignorance of the data breach. When a new investigation was filed in November following the official disclosure of the data leak, Yahoo admitted to learning about the hack into their scheme. Yahoo also stated in this filing that the whole attack was focused on cookies.

As Yahoo and its investigators were attempting to determine the origin and effect of the 2014 cyber-attack, they discovered a previous major attack that occurred prior to 2014. This assault occurred in the year 2013 and was attributed to an unidentified third party. The size of the attack was massive; this time, the hackers stole information from 1 billion users, including backup email addresses. The police were directed to a dark web broker who was selling the data for $300,000 in August 2015 when hunting down details of the hack.[66]

4.3BREACH OF 2013

While it is still unclear how hackers were able to steal all 3 billion Yahoo account records in 2013, an Eastern European hacking group provided the data for sale in 2016. Three organizations have acquired the data after it was put up for sale; two of

[65]See Nicole Perlroth, Yahoo Says Hackers Stole Data on 500 Million Users in 2014, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoohackers.html

[66]See Robert McMillan, Ryan Knutson & Deepa Seetharaman, Yahoo Discloses New Breach of 1 Billion User Accounts, WALL ST. J. (Dec. 15, 2016, 5:19 PM), https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts1481753131.

the identified entities are “spammers,” and the other claims to be involved in spying. Yahoo was able to track the selling of 1 billion accounts for a quarter million dollars with the help of law enforcement and an independent security agency.[67] Authorities suspect the 2013 hack was a state-sponsored attack due to the severity of the intrusion.

4.4BREACH OF 2014

Soon after Yahoo announced that 1 billion of their accounts had been hacked, another leak affecting 500 million accounts occurred. Via a spear-phishing program that directly targeted Yahoo staff, the hacker, Aleksey Belan (a Latvian hacker recruited by Russian agents), was able to obtain access to Yahoo’s User Database and account management tool. Belan mounted a workaround on a Yahoo server after gaining access to the user account, and then stole a duplicate copy of the database onto his personal computer.

Hackers used stolen cryptographic values, known as “nonces,” to create access cookies via a script built on a Yahoo server after identifying accounts of interest. The Department of Justice arrested four people for the hack in March of 2017. Russian intelligence officers made up two of the indictees. The compromised material, according to authorities, was used to spy on a variety of targets in the United States.

These major security breaches had a significant financial, corporate, and public-reputation effect on Yahoo, as well as numerous regulatory violations.

4.5BUSINESS IMPACT

The Yahoo hack revealed a variety of risks raised by the attack, not just to users and the business, but also to the entire IT world. Yahoo has effectively placed millions of consumers at risk of personal information leakage as a result of its incompetence. Yahoo took two years to notify customers, the SEC, and the general public of the security breach. Mayer, Yahoo’s CEO, was opposed to the proposal to require all affected users to update their passwords because she believed the company would lose business. As a result of this incident, Yahoo’s customers and users lost interest in the brand.

Yahoo is also accused of misleading Verizon with fake facts, leading to the signing of a stock deal with no mention of the significant security breach.[68] It gave consumers yet another excuse to think twice about doing business with Yahoo. Due to a shortage of cyber security liability insurance, it is the only company that could not be trusted with confidential data privacy and defense.

4.6FINANCIAL IMPLICATIONS

[67]See Lawrence J. Trautman, Managing Cyberthreat, 33 SANTA CLARA HIGH TECH. L.J. 230, 240 (2016) (discussing the risk assumed by companies that acquired malware-tainted Nortel software from bankruptcy proceeding); see also Lawrence J. Trautman& George P. Michaely, Jr., The SEC & the Internet: Regulating the Web of Deceit, 68 CONSUMER FIN. L.Q. REP. 262 (2014) (discussing electronic commerce operations and websites).

[68]See Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors 4–6 (Oct. 8, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323; see also SMEDINGHOFF, supra note 8, at 30–31.

During talks with Verizon, the two security events allowed Verizon to pay $350 million less for Yahoo in 2017 and sparked a slew of inquiries and litigation that tarnished Yahoo's image. Yahoo's unprecedented data theft, which exposed 3 billion users, resulted in a massive financial loss. The Securities and Exchange Commission fined them $35 million for making misleading statements about the evidence and failure to warn investors about the violation. Yahoo was ordered to pay $85 million in fines to offer free credit management services to over 200 million consumers as part of a mediation agreement. When Verizon learned of the breach, it referred to it as a "material adverse case," which cost Yahoo $350 million in merger costs. Aside from the fines, Yahoo had to pay $35 million in legal costs and another $16 million for its cyber attacks, of which $5 million was devoted exclusively to technical analysis and remediation efforts. They admitted to spending $11 million in legal fees, as well as five state and federal prosecutions and class-action cases.

4.7REGULATORY VIOLATIONS

Yahoo is accused of violating Sections 17(a) (2) and (3) of the Securities Act of 1933, as well as Section 13(a) of the Securities Exchange Act of 1934, according to the SEC's administrative order. The SEC was surprised that the violation was not disclosed quickly enough, and that investors were left in the dark for almost two years. By December 2014, Yahoo's CISO had received warnings that hundreds of millions of Yahoo users' personal information had been compromised, and they were already aware that the same group of hackers had continued to attack their database in 2015 and 2016.[69] Yahoo refused to recognize and minimize cyber security threats, which might have avoided this major data leak if it had been able to do so.[70]

4.8RECOMMENDATIONS AGAINST HACKING

A large-scale data theft is a big problem for an enterprise, and it has ramifications for both its company and its customers.[71] The following suggestions should be used to strengthen the situation and discourage companies from being hacked:
Preventive:

1. Increase data access limits by encouraging workers to only access data that they are allowed to see. Via a phishing campaign, the hacker in the 2014 breach was able to gain access to Yahoo's customer account. If multiple access authorizations are issued to different workers, one compromised employee account can do less harm based on their level of access to the

[69]Bruce H. Nearon et al., Life After Sarbanes-Oxley: The Merger of Information Security and Accountability, 45 JURIMETRICS 379, 391, 394 (2005).

[70]"Consequences of Yahoo Data Breaches Continue." *Audit Analytics*, www.auditanalytics.com/blog/consequences-of-yahoo-data-breaches-continue/.

[71]Garum, Natt. Yahoo Says All 3 Billion User Accounts Were Impacted by 2013 Security Breach. The Verge, 3 Oct. 2017, 5:07 pm EDT, www.theverge.com/2017/10/3/16414306/yahoo-security-data-breach-3-billion-verizon

company's confidential data. In the case of Yahoo, access to the consumer website can be restricted to a limited number of high-level workers who need it.

2. Be certain that all staff and users adhere to a uniform login policy. Recommend that they update their passwords on a regular basis to keep the network and confidential data safe and to deter hackers from using the same keys to enter the device again. Yahoo's bcrypt password program can help to deter brute force attacks, but it can't prevent front door attacks. We suggest informing employees about the dangers of phishing emails and the many ways that hacks or data breaches can occur.
3. Using firewalls and encryption tools such as anti-spyware and antivirus applications, malicious code may be prevented and removed from software. Through advising consumers and staff to upgrade their systems and services on a daily basis in order to stay protected from suspected glitches and vulnerabilities. Particularly for Yahoo workers, because the vulnerabilities in their work computers could compromise the entire network.
4. Keep an eye on suspected activity or cookies: The executive branch should collaborate with the private sector to reduce or prohibit the use of cookies, as hackers have been known to use "forged cookies," which are pieces of code stored in the user's web cache that don't really need a user authentication. Utilize the tools to detect login behavior using cookies and limit access for these users in the future.
5. By supplying the security department with the necessary financial services. In the case of Yahoo, Ms. Mayer, the company's CEO, refused to provide sufficient funding for the company's technology facilities and delayed effective security protections, such as intrusion detection mechanisms for Yahoo's manufacturing systems.
6. Using specialist service services to handle IT security. Improve monitoring infrastructure by enlisting the help of trained security service providers and adhering to best practices. The IT protection department, which is located in the corporate hierarchy, is still overconfident in their own structure. The advice of a reputable IT security company will ensure the security of any sensitive corporate records.

Detective Measures:

1. Intrusion Detection System Review: Hiring an independent team or a security firm to keep an eye on the machines for suspicious activities. Reviewing any protocol violations or other prohibited behavior will aid in the prevention and diagnosis of potential risks and dangers. This will help deter intruders from obtaining access to information through viruses or malware.

Technologies for detecting security breach:

CAPTCHA stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart." It is a device that verifies that the behavior is being requested by a person. When you attempt to log into your account, the CAPTCHA will most likely appear. Words, queries, and graphics recognition are the most popular types of CAPTCHA.

reCAPTCHA: Also known as reversed CAPTCHA, this technology is used to prevent spam as well as digitize books and publications. reCAPCHA, on the other hand, uses digitized words to classify individual actions, while CAPTCHA uses random words to validate.

Since these extra measures cannot be done by computers, they can help deter robots and machines from obtaining access to secure information.

Response Measures:

1. Update account and employee credentials: When a hack is discovered, it is strongly advised that all employees change their passwords. Since the hackers have the passwords, changing the data will prevent the breach from continuing and restrict the hacker's scope. Be sure to beef up your security by enabling two-factor or multi-factor authentication, among other things.
2. The company's breach management team must use tools such as Business Impact Analysis (BIA) and Disaster Recovery to determine the scope of the breach (DR). This will assist them in identifying confidential data and taking the appropriate precautions to secure it. This team can also look at organizations that have leaked data to ensure that no one else has a copy of it.
3. Discuss a fair time to restart activities with the forensics staff and law enforcement. The forensics team will aim to carefully track the actions of users and staff because it aids in determining when the attack happened and, if activities are logged and tracked, it might be possible to detect further intrusions.

Yahoo's data theft was one to recall and respond on, but other big and small businesses are constantly at risk of being hacked. The conventional approach of focusing on vital components and defending against larger threats would not be

beneficial as the prevalent risks evolve. In today's climate, becoming pragmatic and adaptable in approaching and minimizing various threats is essential. Any employee of a company must recognize the importance of data and work to protect it from cyberattacks.It is possible if each person is informed about past attacks by someone who knows and tries to mitigate the risks. Understanding the truth is critical, and ensuring that preventive procedures are revised and in effect will guard against further threats.

4.9 LET'S SUM UP

By developing and implementing a cyber security strategy, businesses will defend themselves from future data attacks. By putting in place pre-emptive steps, certain traditional cyber security methods can be understood and put to use. Also, ensuring that all necessary updates are completed on time.Getting rid of any outdated software that are no longer in service and may be vulnerable to hacking. Keeping cyber security applications up to date and checking them to ensure they function. The most popular and reliable method is to teach staff how to create complicated codes, prevent opening attachments from phishing emails, and properly dispose of sensitive data. In the systems that are used, two-factor authentication is used. Industries should establish a bring-your-own-device policy that specifies what types of company data can be exchanged and processed on these devices. Web filtering technology, which monitors URLs in real time and blocks unwanted entry, can be used by businesses. Businesses should have a solid business continuity strategy in place to assist them through a time of turmoil. A disruption may have a negative effect on the company and revenue; providing a data backup reduces the risk.

4.10FURTHER READING

- Britannica, The Editors of Encyclopaedia. "Yahoo!" Encyclopedia Britannica.
- Al-Heeti, Abrar. "Yahoo Must Pay $50M in Damages for Security Breach." CNET, CNET, 23 Oct. 2018.
- "The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far)." The National Law Review, National Law Review.
- Asher-Dotan, Lital. "Yahoo's Potential Financial Fallout Shows the Unexpected Impacts of a Data Breach." Cybereason.
- "Consequences of Yahoo Data Breaches Continue." Audit Analytics.
- Insureon. "How to Prevent a Data Breach at Your Business." Insureon.
- Williams, Martyn. "Inside the Russian Hack of Yahoo: How They Did It." CSO Online, CSO, 4 Oct. 2017.

4.11CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What kind of responsive measures can be taken into consideration?**

   This chapter discusses three solution steps, one of which is upgrading account and employee passwords. When a hack is discovered, it is strongly advised that both users update their passwords. Since the hackers have the passwords, changing the data will prevent the breach from continuing and restrict the hacker's scope. Take the requisite steps to improve your defense, such as enabling two-factor or multi-factor authentication.

4.12 ACTIVITY

Explain how the Yahoo data breach could have been avoided with proper strategies and infrastructure. (1000-1500 words)

Block-3

INDIAN LAWS AND CYBER SECURITY

1

Unit 1: PRIVACY AND CYBER LAW

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Information Privacy

1.4 Concept of Privacy

1.5 Concept of Data Protection

1.6 Privacy and Data Protection

1.7 Specific Regulatory Areas

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible Answers

1.11 Activity

1.1 LEARNING OBJECTIVES

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

- What is meant by privacy
- The concept of data protection
- Specific statutory regulatory areas

1.2 INTRODUCTION

The right to privacy encompasses a wide range of issues. The right to privacy has been recognised in western culture, both legally and in everyday speech. Article 21 safeguards the right to privacy and supports human dignity. In recent years, there has been an increasing concern about the vast volume of personal information stored in electronic archives. The right to privacy applies to an individual's ability to monitor how sensitive information is collected, used, and disclosed.[72]Data information may include, but is not limited to, personal desires, behaviors, and events, family and educational records, correspondence (including mail and telephone records), medical records, and financial records. An person may be easily affected by the presence of false or deceptive computerized data about him or her that could be transmitted to an unauthorised third party at high speed and for a low cost. This increase in the use of personal data has a lot of advantages, but it also has a lot of drawbacks. Furthermore, the integration of technology has spawned a new generation of privacy and data security concerns. Personal data is readily available and communicable thanks to innovative technology. The right to privacy and data security are inherently at odds. The primary goal of data security should be to balance these competing informational desires. Individuals and organizations' data, on the other hand, should be protected in such a way that their privacy rights are not jeopardized.

1.3INFORMATION PRIVACY

The relationship between data storage and distribution technologies, the public presumption of privacy, and the legal and political concerns affecting them is known as information privacy or data privacy.[73] A few examples should be used to understand the degree to which secrecy must be preserved. The Supreme Court ruled on the issue in Union of India v. Assn. of Democratic Reforms. In a democracy, the freedom to obtain facts is recognised throughout and is a fundamental right that flows from the principle of democracy. Article 21 gives everybody the right to know, including the right to obtain information. Article 21 has a much broader reach and

[72]Sharma, Indu&Afshar, M..(2016). Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law.International Journal of Computer Applications. 145. 11-18. 10.5120/ijca2016910185.

[73]Chun Cheng Niu , Kuan Cheng Zou , Yuan Ling Ou Yang, Guan Jie Tang, Yi Zou "Security and Privacy Issues of the Internet of Things", September 2013

ambit than article 19(1). (a). The Supreme Court stated in People's Union for Civil Liberties v. Union of India that this promotes a voter's or citizen's right to know. When an individual's right to privacy and citizens' right to know compete, the former must yield to the latter because it represents the greater public good. The concern emerges as to how much information about a candidate's privacy a voter has a right to see.By eliminating the disadvantages of legislation pertaining to voters' access to information, the voter's right to hear about a candidate's privacy can be preserved and flourished. The right to monitor the exchange of publicly identifiable information about any individual is known as privacy. It necessitates a balancing mindset, as well as a balancing interest. As a result, a balanced and agreeable inter-relationship between the common good and individual liberty is needed in the end. As a result, it is concluded that a balance must be struck between a citizen's right to know and a candidate's right to privacy while seeking office.[74]

1.4CONCEPT OF PRIVACY

The concepts protection and right to privacy are difficult to grasp. It's been seen in a variety of contexts in various scenarios. 'The right to privacy is bound to include the inviolability and modesty of the body, as well as the intimacy of personal identity, including marital privacy,' according to Tom Gaiety. Jude Cooley has defined privacy as "the right to be left alone," according to the law. Edward Shils defines privacy as a "nil relationship between two or more individuals in the sense that there is no contact or connection between them, whether they want."'Once a society has made a distinction between the "outer" and "inner" man, between the life of the soul and the life of the body...the notion of a private sphere is in which man may become and remain himself,' Warren and Brandeis have eloquently explained. Privacy has been recognised in western culture, both legally and in everyday speech. However, various legal codes prioritize different facets, so it differs. Privacy is a neutral relationship that exists between individuals or entities, or between individuals and groups. Privacy is a value, a cultural state, or a situation aimed at individual and social self-realization that varies by society.

The right to freedom of speech and expression is guaranteed by the Indian Constitution, which means that an individual is free to express his or her opinion on any subject. A individual has the right to life and personal liberty, which can only be taken by legal means. Individuals and/or classes of people have an improbable right to privacy within these regulations. A person's identity is further protected against unjustified arrests, and he or she has the right to share his or her interests on the practice and propagation of either faith. Property protection is still protected because the statute allows it, i.e. a person's property cannot be taken from him without his consent.[75] Personal liberty, as defined in Article 21, has the broadest scope and

[74]AsouAminnezhad, Ali Dehghantanha, MohdTaufik Abdullah "A Survey on Privacy Issues in Digital Forensics", International Journal of cyber security and digital forensics, The society of Digital Information and wireless communication, 2012(ISSN: 2305-0012)

[75]A. A. Sattikar ,Dr. R. V. Kulkarni "A Review of Security and Privacy Issues in Social Networking", International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2784-2787.

encompasses a wide range of rights, including secrecy, sovereignty, human dignity, human property, self-evaluation, restricted and safe contact, restricting man's visibility, and so on. Any of them, such as life and personal liberty, freedom of movement, freedom of speech and expression, human and societal rights, have been elevated to the level of constitutional rights and are protected under Article 19. As such, Article 21 guarantees the right to privacy and promotes human dignity. The right to monitor the distribution and use of one's personal knowledge is referred to as privacy.[76]

1.5CONCEPT OF DATA PROTECTION

The Information Technology Act, which took effect in 2000, is the only law to date that addresses the most important aspects of data security, but not all of them. In reality, the Indian Parliament passed the Information Technology (Amendment) Act, 2008, which is the first law to have data privacy provisions. According to section 2(1)(o) of the Act, "data" refers to a formalized representation of information, knowledge, facts, concepts, or instructions that is intended to be processed, is being processed, or has been processed in a computer system or computer network, and can take any form (including computer printouts, magnetic or optical storage).[77] Personal data is not specified in the IT Act, and the concept of "data" will be more applicable in the area of cybercrime. In addition, the IT Act defines terms such as connection, computer, computer network, computer resource, computer system, computer database, records, electronic medium, electronic record, information, intermediary, secure system, and security procedure in relation to data protection. The aim of the above section is to ensure that someone who has obtained access to such information does not take undue advantage of it by releasing it to a third party without the permission of the individual concerned. The word "third-party information" is described as "any information handled by an intermediary in his capacity as an intermediary," and it's possible that this restriction even extends to "information" and "contact." Section 79 states that an intermediary is not responsible for any third-party material, data, or contact connection that he makes accessible or hastened, except under the conditions set forth in sub-sections (2) and (3).[78]

There is no concept of personal data in the IT Act. Furthermore, in the area of cybercrime, the concept of "information" will be more applicable. Data protection is a technological system of security mechanisms meant to ensure that data is treated in

[76]Mahantesh B Madiwalar, Prof(Dr.) B S Reddy "Privacy Rights and Data Protection In Cyber Space with Special Reference to E-Commerce", Global Journal for Research Analysis, Volume-4, Issue-12, Dec-2015 • ISSN No 2277 – 8160.

[77]Sanaz Taheri Boshrooyeh, AlptekinKupcu, OznurOzkasap"Security and Privacy ofDistributed Online Social Networks", Conference: IEEE ICDCS (International Conference on Distributed Computing Systems) Workshop ESP-DGC, At Columbus, Ohio

[78]Privacy and Human Rights, An International Survey of Privacy Laws and Practise, Global Internet Liberty Campaign at www.gilc.org/ privacy/survey/intro.htmlaccessedon23rd August,2013

such a way that it is protected from unauthorized, accidental, unwanted, or malicious use.

1.6PRIVACY AND DATA PROTECTION

Data regarding people should not be immediately made accessible to other individuals or organisations, according to privacy and data security laws. Each person must have a significant amount of control over the data and how it is used. Data security is a regulatory precaution that prevents the abuse of personal information on any means, even computers. That is the use of administrative, electronic, or physical barriers to protect sensitive information. Data security and privacy are inextricably linked. Data about a person, such as his name, location, phone numbers, occupation, relatives, choices, and so on, can be found in a variety of locations, including schools, universities, banks, directories, polls, and numerous web pages. Passing such information on to third parties will result in invasions of privacy, such as constant marketing calls. The Information Technology (Amendment) Act, 2008 enumerates the main rules on privacy and data security, including identifying data, civil and criminal responsibility for data breaches, and confidentiality and privacy violations.

1.7SPECIFIC REGULATORY AREAS

1.7.1 Financial privacy

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983[79]

Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except in accordance with laws of practice and usage.

The Prevention of Money Laundering Act 2002[80]

The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offence under the PMLA.

Credit Information Companies (Regulation) Act 2005 and The Credit Information Companies Regulations 2006[81]

[79] http://legislative.gov.in/sites/default/files/A1983-48_0.pdf.
[80] https://dea.gov.in/sites/default/files/moneylaunderingact.pdf
[81] http://legislative.gov.in/sites/default/files/A2005-30.pdf.

This legislation is essentially aimed at regulation of sharing and exchanging credit information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offences is maintained permanently while information relating to civil offences is retained for seven years from the first reporting of the offence. In fact, the regulations also prescribe that personal information that has become irrelevant may be destroyed, erased or made anonymous.

Credit information companies are required to obtain informed consent from individuals and entities before collecting their information. For the purpose of redressal, a complaint can be written to the Reserve Bank of India.

Payment and Settlement Systems Act 2007[82]

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

Foreign Contribution Regulation Act 2010[83]

This Act is aimed at regulating and prohibiting the acceptance and utilisation of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

Workplace privacy

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, in relation to the workplace, the effect of the Supreme Court judgment on privacy as a fundamental right remains to be seen.

Children's privacy

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child's best interest. The Personal Data

[82] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf
[83] https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf

Protection Bill 2019 provides for the protection of personal and sensitive data of children by requiring consent of a parent or guardian and imposing various restrictions on data fiduciaries processing such data.

Health and medical privacy

Under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)[84] regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

Medical Termination of Pregnancy Act 1971

This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

Ethical Guidelines for Biomedical Research on Human Subjects

These Guidelines require investigators to maintain confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person's life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is risk to public health.

1.7.2 Technological innovation and privacy law

There are no marketing restrictions on the internet or through email. Because India has no comprehensive data protection regime, issues such as cookie consent have not yet been addressed by Indian legislation. The Personal Data Protection Bill 2019 does prohibit data fiduciaries from profiling, tracking or behaviourally monitoring, or generating targeted advertising at children.

The IT Rules provide reasonable security practices to follow as statutory security procedures for corporate entities that collect, handle and process data, and these also apply to the use of big data. Unfortunately, no specific guidelines exist for the use of big data and big-data analytics in India.[85]

1.8 LET'S SUM UP

Privacy is a fundamental human right, and computing networks store vast quantities of potentially sensitive data. Unauthorized access to a device, computer system, computer network, or services, unauthorized alteration, elimination, extension, change, degradation, replication, or transfer of records, computer database, and so on are all covered by Chapters IX and XI of the Information Technology Act. Financial records, health information, company plans, intellectual property, and personal data could all be protected. However, today's technology allows anybody to

[84] http://niti.gov.in/writereaddata/files/1.pdf

[85] The sources upto this level are available at https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india

access all information about anyone from anywhere at any moment, posing a new vulnerability to private and sensitive data. Technology has gained worldwide recognition as a result of globalization. Different nations have adopted different regulatory frameworks from time to time, such as the DPA (Data Protection Act) 1998 in the United Kingdom, the ECPA (Electronic Communications Privacy Act of 1986) in the United States, and so on. Unique privacy regulations apply in the United States to preserve student school data, children's online privacy, medical records, and private financial documents. Self-regulatory initiatives in both countries are assisting in the definition of better privacy environments. The right to privacy is protected by the Constitution, but its expansion and extension is solely at the discretion of the courts. It is exceedingly impossible to avoid information from leaking into the public domain in today's wired society if anyone is willing to do so without resorting to extremely repressive tactics. The Information Technology (Amendment) Act, 2008 dealt with data security and privacy, but not in a comprehensive way. The Information Technology Act would define strict guidelines for the processes and purposes of assimilation of the right to privacy and personal data. To sum up, the IT Act has an issue with data security, and separate regulation is desperately needed to strike an acceptable balance between personal liberty and privacy.

1.9FURTHER READING

- Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233.
- Edward Shils, "Privacy: Its Constitution and Vicissitudes" 31 Law & Contemporary Problems 281 (1966).
- Samuel Warren & Louis D. Brandeis, "The Right to Privacy" Harvard Law Review 193 (1980).

1.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How can data protection be effectively ensured in India?**

   The right to privacy is protected by the Constitution, but its expansion and extension is solely at the discretion of the courts. It is exceedingly impossible to avoid information from leaking into the public domain in today's wired society if anyone is willing to do so without resorting to extremely repressive tactics. The Information Technology (Amendment) Act, 2008 dealt with data security and privacy, but not in a comprehensive way. The Information Technology Act would define strict guidelines for the processes and purposes of assimilation of the right to privacy and personal data.

1.11 ACTIVITY

Explain the concept of data protection with respect to the Information Technology Act, 2000. (1000-1500 words

Unit 2: DATA PROTECTION BILL 2

Unit Structure

2.1 Learning Objectives
2.2 Introduction
2.3 Anonymised Data
2.4 Consent
2.5 Right to be Forgotten and Right of Erasure
2.6 Rights of Data Principal: Reporting of Personal Data Breach
2.7 Data Protection Bill: Brief Analysis
2.8 Let's sum up
2.9 Further reading
2.10 Check your progress: Possible Answers
2.11 Activity

2.1 LEARNING OBJECTIVE

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

- The provisions relating to the Data Protection Bill
- Protection of personal data and the effects of breach of personal data
- About anonymised data

2.2 INTRODUCTION

"Data is the new oil…."—Clive Humby

The above statement was made in the year 2006 and almost a decade later, it rings true in the present day information technology context. "Data" has become one of the most important, if not the most important resources every individual holds in 2019. In light of its importance, data has also become subject to theft and misuse. Countries, having realised its value, have started formulating laws and regulations to protect from any form of misuse and developed countries have already formed stringent enforcement mechanisms to protect data at the same level as its citizens. Data has come across more than just a container of information. In an article published in 2017 aptly puts, "internet companies' control of data gives them enormous power. Old ways of thinking about competition, devised in the era of oil, look outdated in what has come to be called the 'data economy'."[86]

Apart from the Information Technology Act, 2000, dealing with issues of cybercrime and e-contracts, India does not have any legislation governing data protection. The Supreme Court's recommendation for much-needed legislation on data protection in India in K.S. Puttaswamy v. Union of India or the "right to privacy" became the foundation for formulating a new law on the subject. Justice B.N. Srikrishna led Committee of Experts submitted a report on the same and the Draft Personal Data Protection Bill, 2018 (2018 Data Protection Bill). The Draft Personal Data Protection Bill made the rounds with regard to its formulation being hugely inspired by the European Union's General Data Protection Regulation (GDPR) in terms of data localisation, expansion of the definition of "sensitive personal data", among other things. Upon receiving various reviews and recommendations from the stakeholders of various levels, the Ministry of Electronics and Information Technology prepared the 2019 Bill (the Personal Data Protection Bill, 2019) which was introduced to the Lok Sabha on 11-12-2019. The 2019 Bill is primarily based upon its predecessor with certain significant changes. As much as it has done away with certain flaws of the 2018 Data Protection Bill, the 2019 Bill is also inclusive of red flags raising questions regarding the personal rights of the individuals or "data principles". This article focuses on discussing some changes in the newly proposed Bill and the grey areas

[86]Sable, Vivek.(2020). Constitutional Validity of Data Protection Bill 2019.

in the provisions. The article shall also briefly provide a comparative analysis of the said Indian provisions with GDPR.[87]

2.3ANONYMISED DATA

The term "anonymised records" is one of the first provisions of the 2019 Data Protection Bill that seems to be contradictory. Clause 3 defines the term "anonymisation" in a very specific way. "Anonymisation in relation to personal data" means "any permanent method of transferring or translating personal data to a manner in which a data principal cannot be traced, and which satisfies the authority's requirements of irreversibility."The Act prohibits the processing of anonymised data, but Clause 91 of the proposed Bill makes an exception, allowing the Central Government to collect anonymised data or other non-personal data for "targeting or delivery of services, or the formulation of evidence-based policies." This provision needs further more robust enforcement mechanism along with necessary regulations regarding the usage of such anonymised data.[88]
A privacy bill brings all sectors to abide by the tenets of data security. Except, under the new Bill, that does not quite happen. This is because provisions are very strong when it comes to how private companies and the other entities collect and process data but it lacks when it comes to how the Government can access personal data.

2.4CONSENT

A provision on the requirement of explicit consent before processing of personal data has been provided in Clause 11 of the 2019 Data Protection Bill. However, the grounds for the processing of personal data without consent in certain cases as provided under the later clauses eventually ends up limiting the power of Clause 11 due to the vast number of exceptions.

2.5RIGHT TO BE FORGOTTEN AND RIGHT OF ERASURE

As mentioned above earlier, even despite new additions to the 2019 Data Protection Bill, it falls short to provide complete justice to the rights of the data principal, among other things. It is very interesting to note one such addition in the new Bill is providing the data principal for the "right of erasure" of personal data which is no longer necessary.[89] Clause 18 of the 2019 Data Protection Bill reads: The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such

[87]The Economic Times. (2019). Personal Data Protection Bill: India's digital safety kit. [online] Available at: https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-indias-digital-safetykit/articleshow/72429680.cms?from=mdr
[88]Harvard Business Review. (2019). How India Plans to Protect Consumer Data. [online] Available at: https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data
[89]India Today. (2019). Personal Data Protection Bill seeks access to user data without consent in select cases: Report. [online] Available at: https://www.indiatoday.in/india/story/personal-data-protection-bill-seeks-accessto-user-data-without-consent-in-select-cases-report-1627265-2019-12-11

conditions and in such manner as may be specified by regulations, have the right to—
(a) the correction of inaccurate or misleading personal data;
(b) the completion of incomplete personal data;
(c) the updating of personal data that is out of date; and
(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.
The 2019 Data Protection Bill has simply expanded the provision by including rights for completion, updating and erasure of personal data which the 2018 Draft Bill, in comparison, only provided for the right to correct personal data. Although in the sub-clauses to Clause 18 it lays down the procedure on how the data principal will be able to perform the necessary tasks, it will still require a detailed regulation. It will also be interesting to note that Clause 9 of the 2019 Data Protection Bill provides for the deletion of such data by the data fiduciary which is no longer necessary, but it does not provide any system for notifying the data principal regarding the same.
When it comes to the aspect of "right to be forgotten", the Indian regime has provided it separately under two different clauses unlike the GDPR, where the "right to be forgotten" and "right to erasure" is provided under one article. Despite a new addition of "right of erasure", the 2019 Data Protection Bill still retains one of the major flaws of the 2018 Draft Bill with certain minimum modifications. The 2018 Draft Bill camouflaged the full exercise of the right by stating that the data principal shall have the "right to restrict or prevent continuing disclosure of personal data", which was clearly ambiguous in nature. Clause 20 of the proposed Bill does not shift much from the abovementioned words, thereby retaining the earlier criticised provision. The proviso to the clause states that "no order shall be made under this sub-clause unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen." This is one of the most prominent examples to show why Indian courts have a plethora of cases pending. Especially in the 21st century, where data is considered more valuable than any other asset, and by the time the matter will be heard by the judiciary the data principal would not be in a position to proceed with his case. To add to the above, the enforcement of the data principal's right to "restrict or prevent continuing disclosure of personal data" vests upon the discretion of the adjudicating officer. In this context, not only does the GDPR provide clarity regarding erasure of personal data, it provides for a wider set of provisions to obligate the data controller in the erasure of the data. Therefore, this proves to be another provision which lacks clarity as to the rights of the data principal.

2.6RIGHTS OF DATA PRINCIPAL: REPORTING OF PERSONAL DATA BREACH

The highly criticised, Draft Bill, presented a bizarre provision wherein it provided that in case of breach of personal data, neither the data fiduciary nor the data protection authority shall have any obligation or any requirement to inform the data principal about the breach. Hoping this will be dealt more strategically in lines with the GDPR, the 2019 Data Protection Bill fails to come up with any change. The provision presents itself in the exact format in the new Bill and there is a very limited requirement for the data fiduciary or the data protection authority to notify

the data principal regarding the breach. The provision also provides for the data protection authority the right to publish such breach on their website but retains the right to inform the data principal on its own accords, thereby exposing the data principal to a large number of leaks of his personal data and thereby its misuse. It is one of the provisions which needs significant attention in light of the recent data breaches occurring within the nation. The 2019 Data Protection Bill also fails to provide for a system capable of countering such breach of data in a well-equipped manner. The mechanism is merely a notification of such breach to the necessary websites and other platforms. The GDPR, under Article 34 provides for a more stricter regime wherein it has explicitly provided for notification to the data subjects ("data principal" in Indian context) regarding any such breach of personal data and in case where it has not been communicated in due time by the data controller ("data fiduciary" in Indian context), the authority, upon considering the likelihood of such breach shall notify to the data subject. Since the Indian Data Protection Bill is largely based upon the GDPR, it is indeed surprising to note such important criteria have been left out of the regime.

2.7DATA PROTECTION BILL: BRIEF ANALYSIS

The IT Rules state that all data handlers must create a privacy policy to govern the way they handle personal information. Further, the policy must be made available to the data subject who is providing this information under a lawful contract.

A body corporate (or any person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the data subject to use it for that specific purpose. Consent must be obtained before collection of the data. The IT Rules also mandate that sensitive personal information may not be collected unless it is connected to the function of the corporate entity collecting it, and then only if the collection is necessary for that function. It is the responsibility of the body corporate to ensure that the sensitive personal information thus collected is used for no other purpose than the one specified. The Personal Data Protection Bill 2019 defines 'consent' and 'explicit consent' and provides grounds, including the functions of the state, or compliance with a court order, for the lawful processing of personal data as well as sensitive personal data.

Purpose limitation

The IT Rules state that any information collected by a body corporate or a person on its behalf shall be used for the purpose for which it has been collected. The Personal Data Protection Bill 2019 prescribes that personal data be processed only for specific, clear and lawful purposes. It states that data shall be processed in a fair and reasonable manner that ensures the privacy of the data principal (the person to whom the data relates) and for the purpose consented to by the data principal. Alternatively, the purpose may be incidental to or connected with such purpose, and for which the data principal would reasonably expect that such personal data shall be used. It also limits the collection of personal data to such data that is necessary for the purposes of processing.

Data retention

Section 67C of the IT Act requires that an intermediary preserve and retain information in a manner and format and for such period of time as prescribed by the central government. The Personal Data Protection Bill 2019 states that a data fiduciary may not retain personal data beyond the period necessary to satisfy the purpose for which it is processed. It also states that such data must be deleted at the end of this period. However, the Bill also allows for longer periods of retention if required by compliance with legal obligations, or if the consent of the data principal has been obtained, and prescribes periodic reviews by data fiduciaries for an ongoing assessment of the continued necessity of the retention of personal data.

Registration formalities

India currently does not have any legislative requirements with respect to registration or notification procedures for data controllers or processors. The Personal Data Protection Bill 2019 requires that based on certain criteria, the data protection authority envisaged by the bill shall notify certain data fiduciaries as being 'significant'. Significant data fiduciaries will be required to register with the authority in a manner specified by it, and will also be subject to data protection impact assessments, data audits, etc. The Bill also states that the data protection authority may require registration by other data fiduciaries at its discretion, even if such entities are not 'significant'.

Rights of individuals

Access to data

Rule 5, Subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided. The Personal Data Protection Bill 2019 teases out this right in more detail, providing the option for the data principal to obtain from the data fiduciary in a clear and concise manner, confirmation of whether its personal data is being (or has been) processed and a brief summary of processing activities. The Bill states that the data principal shall also have the right to access in one place the identities of the data fiduciaries with whom their personal data has been shared, along with the categories of such personal data.

Correction and deletion

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and to ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, Subsection 1 that corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

The Personal Data Protection Bill 2019 provides data principals with the right to correction and erasure of personal data. However, such correction or erasure is subject to the agreement of the data fiduciary. If there is a dispute between the two entities in this regard, the data principal may require the data fiduciary to indicate alongside the relevant personal data that it has been disputed by the data principal.

Objection to processing and marketing

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent that may have been given to the corporate entity previously, and the withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the corporate body is prohibited from processing the personal information in question. In the case of the data subject not providing consent, or later withdrawing consent, the corporate body shall have the option not to provide the goods or services for which the information was sought.

The Personal Data Protection Bill 2019 also envisages the right to be forgotten, in that it provides for the data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary. However, this right may only be enforced by order of an Adjudicating Officer.

The Supreme Court of India has also identified and clarified that citizens have the right to be forgotten, which exists in physical and virtual spaces such as the internet, under the umbrella of informational privacy.

Right to restrict processing

As mentioned above, the Personal Data protection Bill 2019 provides for a data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary, but only if the data protection authority, through an adjudicating officer, determines that any of the listed grounds for restriction or prevention of disclosure have been found.

Right to data portability

The IT Act and Rules do not contain provisions relevant to data portability. However, the Personal Data protection Bill 2019 provides data principals with this right where processing has been performed through automated means. Subject to certain restrictions, the data principal shall have the right to receive in a structured, commonly used and machine-readable format, any personal data provided to the data fiduciary, the data that has been generated in the course of provision of services or use of goods by such fiduciary, or the data that forms part of the profile on the data principal, or that the data fiduciary has otherwise obtained.

Right to withdraw consent

The Personal Data Protection Bill 2019 envisages the right to withdraw consent, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

Disclosure of data

Data subjects also possess rights with respect to disclosure of the information they provide. Disclosure of sensitive personal information requires the provider's prior permission unless either disclosure has already been agreed to in the contract between the data subject and the data controller; or disclosure is necessary for compliance with a legal obligation.

The exceptions to this rule are if an order under law has been made, or if a disclosure must be made to government agencies mandated under the law to obtain information for the purposes of verification of identity; prevention, detection and investigation of crime; or prosecution or punishment of offences.

Recipients of this sensitive personal information are prohibited from further disclosing the information.

Right to complain to the relevant data protection authority

Rule 5, subsection 9 of the IT Rules mandates that all discrepancies or grievances reported to data controllers must be addressed in a timely manner. Corporate entities must designate grievance officers for this purpose, and the names and details of said officers must be published on the website of the body corporate. The grievance officer must redress respective grievances within a month from the date of receipt of said grievances.

The Personal Data Protection Bill 2019 states that the data fiduciary must provide all data principals with clear information on the procedure for grievance redressal under the Bill. Under the Bill, a data principal may make a complaint of contravention of any provision of the Bill to the data protection officer (in the case of a significant data fiduciary) or any other officer designated for this purpose (in the case of any other data fiduciary). Should such officer fail to resolve the complaint expeditiously and within 30 day of receipt of the complaint, the data principal may file a complaint with the data protection authority.[90]

2.8 LET'S SUM UP

The 2019 Data Protection Bill has brought about certain important additions. Namely, the "social media intermediaries", "sandbox for encouraging innovation", etc. However, it is safe to say most of the important red-flagged provisions of the 2018 Draft Bill still remain, thereby the new proposed Bill simply can be called an "old wine in a new bottle". Most of the provisions lack clarity and proper enforcement mechanism, which if passed as an Act, would end up increasing volumes of petitions and most certainly be raising questions regarding the security of an individual's personal data. Upon comparing the Indian regime with the GDPR, it can be safe to say that where the latter seeks to focus on the protection of the data principal's rights, the former puts more emphasis on authority and fiduciary's rights. It will be interesting to see what the joint selective committee responds upon reviewing the new Bill. As mentioned above, data is the most valuable asset in today's time, and misuse of the same will lead to doomsday for the individuals, and eventually the country.

2.9FURTHER READING

- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna the Personal Data Protection Bill, 2018<http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report comp.pdf>, the Personal Data Protection Bill, 2018

[90]https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india

<http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf>;.

- European Union's General Data Protection Regulation [Regulation (EU) 2016/679] <https://gdpr-info.eu/>.
- <https://www.indiatoday.in/india-today-insight/story/data-protection-bill-govt-breaks-silence-but-secrecy-remains-1627717-2019-12-12>.

2.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Does the new Data Protection Bill favour the right to be forgotten?**

   When it comes to the aspect of "right to be forgotten", the Indian regime has provided it separately under two different clauses unlike the GDPR, where the "right to be forgotten" and "right to erasure" is provided under one article. Despite a new addition of "right of erasure", the 2019 Data Protection Bill still retains one of the major flaws of the 2018 Draft Bill with certain minimum modifications.

2.11 ACTIVITY

Explain the provisions of Data Protection Bill which talk about the anonymised data. (1000-1500 words)

Unit 3: CYBER CRIMES AND THE LAW: EVALUATION OF THE INFORMATION TECHNOLOGY ACT, 2000

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Concept of Cyber Terrorism

3.4 Cyber Criminals

3.5 Positive Aspects of IT Act, 2000

3.6 Negative Aspects of IT Act, 2000

3.7 Let's sum up

3.8 Further reading

3.9 Check your progress: Possible Answers

3.10 Activity

3.1 LEARNING OBJECTIVE

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

- The concept of cyber terrorism
- About who are the cyber criminals
- About the evolution of the Information Technology Act, 2000

3.2 INTRODUCTION

Knowledge is a resource that is worthless until it is retrieved, stored, and put to good use. Information technology is concerned with data collection, access, processing, interpretation, and intelligent decision-making. Information technology encompasses the processes and devices that allow the production, collection, processing, storage, display, and distribution of information. Individually and as a culture, information technology has an impact.[91]

The hardware and software of a computer and telecommunication system are the foundations of information technology. This, though, is just one aspect of information technology. The other facets are today's global threats, such as cybercrime and, most importantly, cyberterrorism. When the internet was first created, the founders had no idea that it would grow into an all-encompassing revolution that could be used for illegal purposes and necessitate regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level the examples of it are:

(i) Cyber stalking
(ii) Cyber harassment
(iii) Cyber fraud
(iv) Cyber defamation
(v) Spam
(vi) Hacking
(vii) Trafficking
(viii) Distribution
(ix) Posting and dissemination of obscene material including pornography
(x) Indecent exposure and child pornography, etc.

The misapplication of technology has necessitated the enactment and enforcement of cyber rules.[92] The machine has grown in importance in every part of our lives since the new millennium has begun. This involves the use of computers by those engaged in criminal activity. Computers now play a significant part in nearly any crime committed. While not all crime committed is a computer crime, it does mean that law enforcement must become even more computer literate in order to keep up with the criminal aspect."For the first time in human history, algorithms and digital systems make it possible to own, not just execute, a crime," writes Donn Parker. Today, a total fraud in software can be passed from one perpetrator to the next, with

[91]Basu, Subhajit& Jones, Richard. (2005). Indian Information and Technology Act 2000: review of the Regulatory Powers under the Act. International Review of Law Computers & Technology. 19. 209-230. 10.1080/13600860500133495.

[92]S Basu and R Jones 'Legal issues affecting e-commerce: a review of the Indian Information Technology Act 2000', Contemporary South Asia Vol 12(1), 2003.

each refining or modifying it to his or her own needs." However, the issue of whether these cyber regulations are capable of controlling cyber crime operations demands the most consideration.[93]

Many information technology (IT) experts were unaware of and uninterested in the cybercrime epidemic until recently. In certain ways, law enforcement agents lacked the resources they needed to deal with the problem; outdated rules didn't quite suit the offenses being committed, recent laws hadn't quite caught up to reality, and there were few judicial precedents to look to for direction. Furthermore, privacy debates hindered law enforcement's efforts to collect the facts required to investigate these new cases. Finally, there was some animosity—or at the very least, mistrust—between the two most important actors in any fruitful battle against cyber crime: law enforcement agents and tech experts. However, if we want to monitor the cyber crime issue and make the internet a secure "place" for its users, strong coordination between the two is necessary.

Law enforcement officers are familiar with the criminal culture as well as the fundamentals of collecting evidence and getting criminals to justice. IT professionals are familiar with computers and networks, as well as how they operate and how to locate information about them. Each of them has half of the solution to the cyber criminal's problem. IT experts need clear definitions of cybercrime in order to determine who (and what) to refer to the police, but law enforcement officers need formal definitions of particular offences in order to prosecute a suspect. The first step in identifying individual cyber criminals is to organize all of the activities that may be classified as cyber crimes into groups.[94]

3.3CONCEPT OF CYBER TERRORISM

Both cyber fraud and cyber terrorism are offences committed online. However, there is a distinction between the two in terms of the perpetrator's motivation and purpose. While a cyber crime may be loosely described as an illegal act in which a device is used as a weapon, a target, or both, cyber terrorism requires a more comprehensive description. Cyber terrorism may be described as the premeditated use of disruptive activities, or the threat of disruptive activities, in cyberspace with the intent to further social, ideological, moral, political, or related goals, or to threaten someone in the process.[95]

3.4CYBER CRIMINALS

An convict or a suspect is someone who does something wrong with the intent of committing a felony. Any one who commits a cyber crime is referred to as a cyber criminal in this case. Children and teenagers aged 6 to 18 years may be cyber

[93]Y Benkler 'A free information ecology in digital environment', New York University Conference, Session 12, The Information Law Institute at New York University School of Law, 2001, at p 29

[94]S Wilske and T Schiller 'International jurisdiction in cyberspace: which states may regulate the Internet?', Federal Comm. Vol 50, LJ 117, 1223 –3, 2001.

[95]'Cyber crime and punishment? Archaic laws threaten global information', Mcconnell International December, 2000. Available at: http://www.mcconnellinternational.com/services/ cybercrime.htm

criminals; they may be organized terrorists, skilled hackers or crackers, disgruntled workers, cheaters, or even psychics.

(a) Kids and teenagers (Age group 9-16)

While it is impossible to imagine, it is accurate. Teenagers make up the majority of inexperienced hackers and cyber criminals. Hacking through a computer machine or a website is a source of pride for them, who have just recently started to learn what seems to be a great deal about technology. There's also the issue of looking extremely intelligent among peers. This teenage insurgents can even engage in cybercrime without being aware that they are doing so.

Teen hackers, according to the BBC, have progressed from just seeking to make a name for themselves to potentially finding their way through a life of crime through the use of computers. One of the most significant developments in 2004 was the waning power of the boy hackers eager to make a name for themselves by writing a fast-spreading virus, according to Kevin Hogan. While teen virus authors will continue to experiment with malicious programming, illegal use of malicious programs increased significantly in 2004. The use of technologies by criminals was fueled by financial rewards.[96]

Another cause for the rise of juvenile criminals in cybercrime is that many offenders, often young college students, are ignorant of the severity of the crime. An engineering college student from Tamil Nadu was recently arrested by the Chennai City Police for sending an unsolicited message to a chartered accountant. The young man has been released on bond. As a result, counseling sessions for college students must be established in order to inform them about the seriousness of such offences and the repercussions that can result.

(b) Organised hacktivists

Hacktivists are hackers who have a specific (usually political) goal in mind. In other instances, the cause may be civic justice, religious activism, or something else else. Attacks by a group of hackers known as the Pakistani Cyber Warriors on roughly 200 popular Indian websites are a fine example of political hacktivists at work.

(c) Disgruntled employees

It's hard to imagine how vengeful disgruntled workers can be. They had the choice of going on strike against their employers up to now. Disgruntled workers can now cause more damage to their bosses by committing tech-related offences, and can tear whole networks down, thanks to increased computer freedom and process automation.

(d) Professional hackers (Corporate espionage)

Company organizations now store much of their records in electronic form as a result of extensive computerization. Hackers are used by rival organizations to capture industrial secrets and other intelligence that may be useful to them. The temptation to employ sophisticated hackers for industrial espionage stems from the fact that physical presence is no longer needed to obtain access to critical documents if hacking can procure them.[97]

---

[96] L Lessig Code and Other Laws of Cyberspace, Basic Books, 1999, at p 6; for the contrary view see D Post 'What Larry doesn't get: code, law and liberty in cyberspace', Stanford Law Review Vol 52, 2000, at p 1439.

[97] U Sieber 'Legal aspects of computer-related crime in the information society', Comcrime study prepared for the European Commission 19 January, 1998. Available at: http://europa.eu.int/ ISPO/legal/en/comcrime/sieber.doc

3.5POSITIVE ASPECTS OF THE IT ACT, 2000

Even an email was not recognised as an accepted civil means of correspondence or as testimony in a court of law prior to the passage of the Information Technology Act of 2000. However, the IT Act of 2000 modified this situation by recognizing the electronic version as a legal format. The Information Technology Act of 2000 is, without a doubt, a move forward.

Companies will be required to conduct electronic trading using the regulatory infrastructure established by the IT Act of 2000, from the viewpoint of the private sector. The development of electronic commerce in India was hampered before the Indian cyber law took force because there was no legal infrastructure in place to control commercial transactions conducted online. Corporate transfers will soon be able to be completed electronically using digital signatures. The IT Act of 2000 has granted these digital signatures legal status and sanction.

In today's world, businesses archive records on their own operating systems and keep a backup. Companies will also have a contractual solution if anyone hacks into their operating systems or networks and causes disruption or copies records, thanks to the IT Act of 2000. The IT Act of 2000 provides a relief in the form of punitive damages in the amount of Rs 1,000,000 in compensation.

The Information Technology Act of 2000 defines a variety of cyber crimes, including hacking and computer code damage. Prior to the implementation of the Indian cyber rule, businesses were powerless because there was no legal recourse for such problems. The IT Act of 2000, on the other hand, completely transformed the landscape.

3.6NEGATIVE ASPECTS OF THE IT ACT, 2000

The IT Act, 2000 is likely to cause a conflict of jurisdiction.

Domain names are the foundation of electronic commerce. The Information Technology Act of 2000 makes no mention of domain names. Also domain names have not been specified, and domain name owners' rights and liability are not included in the legislation.

The Information Technology Act of 2000 does not address any questions relating to the enforcement of intellectual property rights in the online world. The statute has left many gaps by leaving contentious but crucial problems such as internet copyrights, trade marks, and patents unaddressed.

When the legislation governing cybercrime evolves, so do the new modes and types of cybercrime. The list of offenses identified in the IT Act of 2000 is far from exhaustive. However, the applicable provisions of the IT Act, 2000 are written in such a way that they seem to be the only cyber offenses that are conceivable and occur. The Information Technology Act of 2000 does not contain a variety of cyber and internet-related offences. These include:

(a) Theft of internet hours
(b) Cyber theft
(c) Cyber stalking
(d) Cyber harassment
(e) Cyber defamation
(f) Cyber fraud
(g) Misuse of credit card numbers

(h) Chat room abuse
Several critical concerns relating to the e-commerce domain, such as anonymity and content control, were not addressed by the IT Act of 2000. The topic of privacy has been completely ignored. Another ambiguity of the IT Act is that it makes no mention of antitrust concerns.
The enforcement of the Indian cyber law is the most serious problem. The IT Act of 2000 does not have any guidelines for enforcement. Furthermore, given India's low internet penetration and the fact that most government and police officials are not tech savvy, the latest Indian cyber law poses more questions than it addresses. To eliminate the above-mentioned grey areas, it appears that Parliament will need to update the IT Act of 2000.

3.7 LET'S SUM UP

It is necessary to pass new laws that cover all facets of cybercrime in order to eliminate legal ambiguities. The recent blasts in Ahmedabad, Bangalore, and Delhi highlight the danger that cyberspace practices pose to humanity, and we agree that only technology and its widespread use can effectively combat these issues. The government should take reasonable measures to limit the content that is readily available for download. The IT Act of 2000 should be updated to make it more accessible and effective in combating crime. Training and public awareness activities can be implemented in the private and public sectors. In India, the number of cyber cops should be increased. The jurisdiction issue is present in the enforcement phase, which can be resolved because cyber criminals have no jurisdiction limit, so why do the laws exist? After all, the laws are in place to punish the criminals, but the current situation allows them to flee.
In today's world, there is a need to develop a "cyber-jurisprudence" that can be used to test and criticize "cyber ethics." There is also a pressing need to develop a cyberspace code of ethics and discipline. The Information Technology Act of 2000 was enacted in response to the country's growing cybercrime crisis. Since the internet is a conduit for vast amounts of data and a vast network of communications around the globe, it is important to exercise vigilance when using it. As a result, it is important to teach everybody and practice secure coding in order to avoid cybercrime.
Many other programmers, including Frank William Abagnale and Robert Morris, want to put their hacking expertise to greater use. This practice is still going on today, with businesses hiring genius hackers as intelligence researchers. There is also a pressing need to develop a cyberspace and discipline code of ethics. It is impossible to determine fault in cyberspace using conventional criminal law standards. Since the majority of cyber offenders are under the age of majority, a new legislative system to deal with them must be developed. Since the cyber universe has no borders, enacting rules to protect all aspects is a Herculean task. However, a balance must be achieved, and legislation must be developed to combat cybercrime.

3.8FURTHER READING

- Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233.

- Edward Shils, “Privacy: Its Constitution and Vicissitudes” 31 Law & Contemporary Problems 281 (1966).
- Samuel Warren & Louis D. Brandeis, “The Right to Privacy” Harvard Law Review 193 (1980).

3.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the negative aspects of IT Act?

The Information Technology Act of 2000 does not address any questions relating to the enforcement of intellectual property rights in the online world. The statute has left many gaps by leaving contentious but crucial problems such as internet copyrights, trademarks, and patents unaddressed.

3.10 ACTIVITY

Elaborate the types of Cyber Criminals. (1000-1500 words)

Unit 4: CYBER STALKING AND THE PLIGHT OF WOMEN IN INDIA — A LEGAL PERSPECTIVE

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Understanding Cyber Stalking & Its Impact

4.4 Cyber Stalking: Legal Remedies

4.5 Let's sum up

4.6 Further reading

4.7 Check your progress: Possible Answers

4.8 Activity

4.1 LEARNING OBJECTIVE

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

- What is known as cyber stalking
- Legal remedies for cyber stalking
- How women can be victimised for cyber stalking

4.2 INTRODUCTION

In June 2016, in Salem district of Tamil Nadu, a 21-year-old woman saw a picture of her face, digitally superimposed on the body of another woman, posted on a social networking site. She informed her parents, and also identified the man responsible for it. He allegedly warped her image using a cell phone app, posted it to the site, and tagged her in the post after she allegedly refused his marriage proposal.[98] A report was filed with the Cyber Crime Cell by the woman's parent. She discovered another blurred picture tagged to her social networking site a few days later, this time with her name and her father's phone number. The woman committed suicide on the same day. In her suicide note, she expressed her complete ignorance about the distorted images and her failure to convince anybody.

With a significant increase in the usage of computer in our daily life and advancement of information technology, the vulnerability for users of computer and internet has remarkably gone up in the cyberspace today. If technology progresses, the vast technological potential of modern computers/computing machines creates possibilities for exploitation as well as criminal activity. Unfortunately, many people are unaware of the bugs they are vulnerable to when surfing the internet, posting on social networking sites, or saving data on their computers. At the same time, perpetrators use the cyberspace as a platform for indulging in various criminal activities against the users. In fact, traditional offences such as rape, molestation and different forms of sexual abuse have gained new significance due to the development of information and communication technology.

There are incidences of rape scenes in the mobile phone devices, extraction of money by threatening to publish images/videos relating to the same. The Information Technology Act, 2000 (hereinafter known as IT Act, 2000) has recognized various offences relating to cyberspace. Among many offensive acts on cyberspace, online abuse is a common phenomenon all over the world, which has directly or indirectly affected online users of different age groups leading to different forms of harassment such as gender bullying, trolling, stalking etc. A person's repetitive, unsolicited, malicious behavior across cyberspace with the intent to terrify, bully, humiliate, insult, taunt, or stalk someone else is known as cyber harassment. Apart from the physical act of harassment being considered as an offence under the Indian laws, any harassment caused through electronic media such as social networking sites, chat rooms, e-mail etc. is also considered to have similar impact as far as traditional

[98] Abhiraj Thakur, Cyberstalking: A Crime or A Tort, Jun. 21, 2016

offences of harassment are concerned.[99] According to popular perceptions, women in India make most vulnerable targets on the internet and digital communication technology due to their gender and consumability of images of Indian women as subject matter of pornography. On many occasions, women become the target of such abnormal activities to destroy the image of the immediate family members. However, it is unfortunate that multiple cases go unreported either due to lack of awareness or absence of stringent laws to deal with them. It is also interesting to note that there are a very few cases of this nature which are actually registered and prosecuted.[100] Besides, with the striking down of Section 66A of the Information Technology Act, 2000 in the decision of the Supreme Court in Shreya Singhal v. Union of India, there has been a void in law to respond to such offences. Highlighting on the fundamental right to freedom of speech and expression, the judgment held that liberty of thought and expression is not merely an inspirational ideal. It is also "a cardinal value that is of paramount significance under our constitutional scheme." Under such a paradoxical situation, where the legal fraternity insists on upholding right to freedom of speech and expression on the one hand and use of cyberspace for publishing offensive messages/images about women (which also includes stalking) on the other hand, it becomes pertinent to understand the phenomenon of cyber stalking, its impact on women and the various challenges involved in effectively addressing this menace.[101]

4.3UNDERSTANDING CYBER STALKING & ITS IMPACT

A. Concept of Cyber Stalking

Stalking has emerged as a socio-legal problem of the recent time, which has resulted in its incorporation as criminal offence in the Indian laws. According to the Oxford Dictionary, stalking means "pursuing stealthily". In other words, stalking refers to trailing someone with the intent of harassing or inconveniencing them. Stalking is characterized as repetitive and unwelcome harassing behavior that is aggressive and intentionally aimed at a single individual (the victim), and that would lead a rational person to fear physical harm or death for themselves or family members.[102] Stalking may be characterized by the following:

- A repeated and unwanted harassing behaviour by a person against another.
- Such behaviour may be reflected by a physical act or may be done through electronic means usually the internet and other communication devices.
- The act may cause mental trauma and fear to the victim, sometimes leading to more serious offences.
- The act is a direct intrusion into the privacy of an individual, where the stalker attempts to establish relationship with the victim without his/her consent.[103]

[99]B. Spitzberg and G. Hoobler, Cyberstalking and the Technologies of Interpersonal Terrorism, 4(1) NEW MEDIA & SOCIETY 71 (2002).

[100]BH Spitzberg and WR Cupach, The State of the Art of Stalking: Taking Stock of the Emerging Literature, 12 AGGRESSION AND VIOLENT BEHAVIOUR 64 (2007).

[101]D. Halder and K. Jaishankar, Cyber Crimes against Women in India: Problems, Perspectives and Solutions, 3(1) TMC ACAD. J. 48, 55 (2008).

[102]D. Lamplugh& P. Infield, Harmonising Anti-Stalking Laws, 34 Geo. Wash. Int'l L. Rev. 853 2002-2003.

[103]Dr.DebratiHalder, Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives, SSRN 103, 103-130 (2015)

Cyber Stalking is a serious form of harassment posing threat to life of an individual if it is not addressed appropriately. It constitutes harassment of individuals on cyber space through use of information and communications technology (especially the Internet). Such harassment may include actions such as the transmission of offensive and derogatory e-mail messages, identity theft and damage to data or equipment. As a result, cyber stalking is a set of behaviors in which a person, a group of individuals, or an organization uses information and communication technologies to threaten one or more people. Transmission of threats and false claims, identity fraud, data theft, data or equipment damage, computer surveillance, solicitation of minors for sexual purposes, and altercation are examples of such behaviors.

B. Cyber Stalking and Victimization of Women

It has often come to be seen that women and young children become victims of such acts leading to threat, harassment, assault and trauma. Privacy in virtual world as well as real life is gradually shrinking and women are the most affected community in this regard. Cyber Stalking is a serious example of infringement of privacy of women in cyberspace. In addition to this, because of the nature of the offence and the target aimed, such abnormal activities leave a serious impression on every aspect of their life.[104] Cyber victimisation of women can be categorised into two main groups: textual victimisation and graphical victimisation. Graphical victimisation may include producing, creating or publishing obscene, derogatory, and pornographic, including revenge pornographic materials on the web to put the victim in shame.[105]

There is no doubt about the fact that traditionally women are considered to be marginalized and disadvantaged section of the society. Even though the Constitution of India guarantees equal rights to men and women, women have been made second grade citizens due to dominantly patriarchal set up of the society. On many occasions, stalking becomes a vindictive instrument for man as an immediate reaction to refusal by the woman to get into any relationship with him. Today, the scenario is far more alarming where internet trolls take to social media website and instant messaging services like WhatsApp to target women activists, journalists, celebrities, academicians and so on to create hatred among the larger community against such women just to gain a sadist pleasure out of it.[106]

According to a comparative data of Working to Halt Online Abuse (WHOA) for the period 2000-2013, it was revealed that women victims generally outnumber male victims when it comes to cyber stalking victimisation and that out of 4043 victims who contacted WHOA in the said period, 70% were women. Women are targeted by trolls, bullies, stalkers with insulting, defamatory, derogatory statements/pictorial depiction on the internet. Even when women are not connected to the worldwide web, they may be harassed and stalked by unnecessary phone calls and SMSs. This may sometimes result in barring women completely from using any such medium of communication. This shows a blatant violation of rights of women through improper exercise of right to speech and expression on the internet. They are violation of basic human rights including right to equality as guaranteed under Article 14 of the Constitution of India as the right to live with dignity as enumerated in Article 21 of the

[104] John M. Deirmenjian, Stalking in Cyber Space, (1998)

[105] Dr.DebratiHalder, Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives, SSRN 103, 103-130 (2015)

[106] K. Y. A. McKenna, A. S. Green and M. E. J. Gleason, Relationship formation on the Internet: What's the big attraction?, 58 (1) J.OF SOCIAL ISSUES 9 (2002).

Constitution. Unfortunately, while deciding in the landmark case of Shreya Singhal v. Union of India, constitutionality of Section 66A of the IT Act, 2000, the Supreme Court emphasized on right to freedom of speech and expression, but overlooked the victimization of women in cyber space by misuse of this right. Such victimization would be dangerous for women because of the nature of electronic media which is different from print media.

4.4CYBER STALKING: LEGAL REMEDIES

Cyber stalking is a common phenomenon in cyberspace, which go unaddressed many a time due to lack of specific laws and enforcement mechanism. This is a glaring example of serious consequences of stalking in cyberspace. There could be end number of cases of similar nature which go unreported. Social norms and orthodox values play a major role here. Women victims and their family members feel reluctant to report such crime, especially due to fear of damage to their social reputation. Apart from this, there are various factual reasons for less number of prosecutions of cases of cyber stalking. This may include lack of focused laws, challenges in establishing identity of the perpetrator, lack of proper infrastructure in the criminal justice machinery in India and above all, the absence of servers within the jurisdiction of India, and conflict of laws between Indian laws and laws of countries which host the internet companies/service providers.[107]

The first initiative to formulate a legal framework for the cyber space was perceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India emerged in the form of the Information Technology Act, 2000 which was significantly amended in the year 2008. The IT Act also amended some of the provisions of the Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing offences like cyber stalking, the problem still remains unaddressed as the law is more on papers than on execution because lawyers, police officers, prosecutors and Judges are in a helpless state in apprehending its highly technical terminology.

The offence of cyber stalking was not incorporated in the IT Act when it came into force in 2000 unless the act involved publication or transmission of obscene material within the meaning of Section 67 of the IT Act. Besides, Section 509 of the Penal Code, 1860 (IPC) partially deals with the offence according to which uttering of any word, making of any sound or gesture or object to be heard or seen by a woman, or intrusion upon the privacy of such woman shall be punishable with imprisonment up to three years and fine. Since Section 509 of IPC defines this act as one of privacy, Section 72 of IT Act was used to deal with cases of cyber stalking to an extent. With the amendment of IT Act in 2008, Section 66A was inserted in the IT Act under which all the cases of cyber stalking were dealt with.

4.5 LET'S SUM UP

[107]Leroy McFarlane & Paul Bocij, Online Harassment: Towards a Definition of Cyber Stalking, 139 PRISON SERVICE .l 31, 31-38 (2002).

Cyber Stalking is a serious form of harassment on the internet. Besides, deciding on the jurisdiction for dealing with such offence is a challenge before the courts. Hence, there is a need for revisiting the IT Act for prosecution of cases of cyber stalking as well as law enforcement mechanism needs to be better equipped to address such problems in an effective manner. At the same time, the challenges involving law and technology in dealing with such offences must be addressed effectively to reduce the vulnerability of the users of cyberspace. The article puts forward the following suggestions and observations for a better redressal system for Cyber Stalking:

1. Global Crime: Need for International Cooperation The nature of most of the cyber-crimes is global in nature due to which the jurisdiction to investigate becomes a major issue. Whenever a stalking takes place in cyber space, the server of the electronic device used for such acts might be located beyond the territorial jurisdiction of India. Hence, it may be feasible to conduct investigation of such cases if it is made mandatory for the service providers such as Facebook, twitter or WhatsApp to install a local server in India. Such arrangement may, to some extent, be able to address the problem of jurisdiction in such cases.

2. Stringent laws at National Level In the absence of a specific provision to address cases of Cyber Stalking, it is highly essential to make necessary amendments in the existing laws or to bring Section 66A of the IT Act back with necessary regulations.

3. Need for Inter-State cooperation Due to serious lack of cooperation and coordination from another state involved in a crime, the investigating agency fails to complete investigation. In this regard, a Cyber-Crime Inter-State Cooperation Cell may be set up and attached with every cyber cell so that it provides exclusive information relating to such crimes.

4. Initiative at the Individual Level As a measure for protection from such exploitation in cyber space, it is necessary to take precautionary steps such as adequate security measures to ensure not to disclose personal information on the internet in inappropriate fora. Passwords should not be made too easy to be cracked by perpetrators. The privacy settings in social media facilitate blocking of accounts causing annoyance. The same must be taken recourse to avoid unnecessary harassment.

5. Revisiting the Right to Freedom of Speech and Expression: It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. There is a need for striking a balance between freedom of speech and expression on the one hand, and right to privacy on the other.

Cyber stalking has become a recent threat for the cyber community in India, especially women irrespective of age or any other social strata they belong to. It has even gone to the extent of ruining the lives of many young women. Therefore, it is the need of the hour to formulate a technically sound legal framework as well as an impartial mechanism for better redressal of cases of Cyber Stalking in India.

4.6FURTHER READING

- See Salem woman, 21, kills herself after obscene pictures morphed to look like her were posted on Facebook, Daily Mail, Jun. 29, 2016, available

at http://www.dailymail.co.uk/indiahome/article-3664841/Salem- woman-21-kills-obscene-pictures-morphed-look-like-posted-Facebook.html.

- DebaratiHalder& h. Jaishankar, Cyber Crimes Against Women in India 8 (2017).
- Ursula Smartt, The Stalking Phenomenon: Trends in European and International Stalking and Harassment Legislation, European Journal Of Crime, Criminal Law And Criminal Justice, Vol. 9/3, 209-232 (2001).

4.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the suggestions and observations for a better redressal system for Cyber Stalking?**

   Need for International Cooperation; Stringent laws at National Level; Need for Inter-State cooperation; Initiative at the Individual Level and Revisiting the Right to Freedom of Speech and Expression.

4.8 ACTIVITY

Elaborate the legal remedies available against cyber stalking. (1000-1500 words)

Block-4

CYBER TERRORISM

Unit 1: CYBER TERRORISM: AN ANALYSIS WITH AN INDIAN PERSPECTIVE

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Conventional vs. Cyber age terrorism

1.4 Forms of Cyber Terrorism

1.5 Judicial Response

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible Answers

1.9 Activity

1.1 LEARNING OBJECTIVES

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

- Meaning of cyber terrorism in India
- Difference between terrorism and cyber terrorism
- Forms of cyber terrorism
- How judiciary has interpreted the cases of cyber terrorism

1.2 INTRODUCTION

Terrorism, as a part of the 21st Century, grew as a cult with an end in itself. Terrorism instils a fear in the minds of the people against their state's inability to protect them from damage in person and property; it also creates a psychological and social havoc in the lives of people. Conventional terrorism was aimed at eroding the tranquillity and tolerance among a group of people, or more precisely to disrupt the harmonious well-being of a nation.[108] With emerging trends in generations, terrorism has changed its shape and form, keeping pace with modern era. With the advent of the culture of the world being online, cyber-terrorism developed its roots to tackle the ever advanced techno-geek reality, forcing into the personal space of people without any visible damage. But is there any remarkable difference between conventional and contemporary forms of terrorism? What makes it different from cyber-attacks and renders it a form of terrorism? How does it affect the government and its policies? How does the law deal with it? While most of these are lethal, the question regarding their legality with respect to ethical hacking and security also arises.[109]

Cyber-terrorism has been defined by various organisations, adding various dimensions to its scope, but retaining the crux of the problem. NATO defines cyber-terrorism as "a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal." The National Infrastructure Protection Centre defines cyber-terrorism as, "a criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction, and/or disruption of services to create fear by causing confusion and certainty within a given population conform to a political, social, or ideological agent." The most accepted notion of cyber-terrorism is defined by FBI which defines it as, "a premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." A close analysis of these definitions reveals some common aspects of cyber-terrorism which are inherently present in it - fear, political association and/or ideological influence. What can be gathered is a simple line-up for this term, i.e., Cyber-terrorism is a technologically transmitted

[108]S. Best, Defining Terrorism: http://www.drstevebest.org/Essays/Defi ning%20Terrorism.htm www.symantec.com/avcenter/reference/cyberterrorism.pdf

[109]M. Cereijo Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006: http://www.lanuevacuba. com/archivo/manuel-cereijo-110.htm

crime with intent to destroy or affect a set of information which is politically, morally or ideologically undesired by a group or race of people and to create a sense of fear so as to stop its future perpetuation. While cyber-terrorism is more or less assumed to be a form of hacking, the latter is subsumed by the former and thus encompasses a much wider centre-stage.[110]

1.3CONVENTIONAL VS. CYBER AGE TERRORISM

While most of the scholars believe that terrorism is a term which brings with it destruction, deaths, and devastation, the cyber-world of terror attacks is incapable of such level of desolation. The conventional mode uses more of physical warfare and weapons, including both men and matter, in order to gather more fear and pressure, and sometimes to give effect to their own macabre ideology. Scuttling of peace attains topmost ground in a terror instance. On the other hand, the 'cyber enabled terrorism' uses virtual mode to delve into the lives of people and disturb them psychologically and financially. It uses a more formal approach of maliciously transmitted viruses and ransom wares. The motive behind cyber-terrorism is usually not personal, and this is what differentiates it from cyber-crime. The end result of cyber-terrorism may include shut down of networks, money extortion for terrorism purposes, stealing of information, and hacking of government systems. Just like the recent instance of 'Wannacry' ransom ware that hit more than 150 countries and demanded payment of 'Bitcoins', another cyber-related terrorism.[111] The 'Flame' malware that hit the Middle-Eastern countries in 2012 is also an example of cyber-terrorism. Although, this form of terrorism is not as much devastating as its other counterpart, it is gaining more ground due to its other attributes, that is to say that it is comparatively easier to spread with no costs and no limits. Also, the identity of the perpetrator can be concealed along with his/her location. Cyber-terrorism has thus created a niche for itself with it being the 'new' normal.

1.4FORMS OF CYBER-TERRORISM

With the advancement in the technological world, the cyber related crimes are on an increase with every coming day and it is humanly impossible to attempt a categorisation of the same. Cyber-terrorism can acquire new dimensions, with an edge in almost every sphere and thus, the types of crimes are endless. While we await newer forms to dig up, the following forms are not hard to compile:

- **PRIVACY VIOLATION**

Every individual has a right to live in privacy and the right to be let alone. The Right to privacy gained recognition under Articles 21 and 19(1) (d) of the Indian Constitution in post-Maneka era. Also, privacy is an independent and distinguished concept recognised by the tort law, although it is not exercised much in

[110]R. L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation, Before the House Energy and Commerce Committee, Oversight and Investigation Subcomittee Washington, DC, 05 April 2001, http://www.fbi.gov/news/testimony/issue-of-intrusions-intogovernment-computer-networks
[111]R. Lemos, Cyberterrorism: The real risk, 2002: http://www.crime-research.org/library/Robert1.htm

India in that context. As 'Privacy' has now gained status of fundamental right, it is well protected by both civil and criminal consequences. With the dawn of solidarity-oriented culture, people have become more and more sensitive to the invasion of their personal space, not only physical but also mental. To cope up with this intrusion done by information technology, the legal society has evolved a fresh new outlook, although not so advanced. Privacy violation may include information access without the consent of the person or the organisation involved, or passing off of information by an agent to a person not authorised to do so. Cyber-terrorism invades the right to privacy of an individual. The acts of cyber-crime are a threat to personal information and activities of a person and can be treated as a form of cyber-terrorism. It may include phishing, hacking of accounts, transmission of viruses etc.[112]

- **DATA THEFT AND MISAPPROPRIATION**

Cyber-terrorism also aims at leaking out confidential information not only of private individuals but also of the government and other agencies. Such information may be of national importance and of vital nature with respect to the security and defence of a country. It can be used by terrorist outfits to facilitate their objectives and to further facilitate their infiltrations by finding the probable lacunae in the system. The same may be used to destroy property which is public or private, movable or immovable, and tangible or intangible. Data misappropriation is another tool of cyber-terrorism to tackle the odds. Data on a source can be manipulated to gain access to a particular object, while denying the same to the owner. This renders the security systems useless and puts information under seize.

- **DEMOLITION OF E-GOVERNANCE BASE**

The e-governance is the main source of interaction between state and its citizens. The right to information is also an outcome of the e-governance. While it facilitates transfer of information on one hand, it also helps in raising voices and opinions on particular policies and actions. The government acts as a custodian of public information, ranging from personal information of its citizens to data related to their public activities. The public has a right to information; however, it is not an absolute privilege to them. The Hon'ble Supreme Court of India in People's Union for Civil Liberties v. Union of India held that the government can withhold information related to various matters on certain grounds. While most of this information is in hard-copy form, the digital version is susceptible to a probable cyber-attack. Such an attack could cause a complete demolition of this established e-governance base.

- **DISTRIBUTED DENIAL OF SERVICE ATTACK**

Distributed Denial of Service (hereinafter DDoS) is a kind of attack where-in multiple 'infected' computer systems or servers attack another system or server, which causes the affected computer to 'deny' service to the user. The affected computer is actually flooded with endless data and information which causes the server to slow down or crash, which further causes it to stop working and denies the service requested or required by the legitimate user of the server. This works as an interlinked web of infections spreading from one system to another vulnerable

[112] A. Jahangiri, Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion: http://www.alijahangiri.org/publication/Cyberspace-Cyberterrorism-andInformation-Warfare-A-Perfect-Recipe-for-Confusion.htm

system and finally attacking a single targeted system. The purpose of using multiple systems to attack a single system is manifold; first, it becomes impossible to block all the infecting systems, and second that multiple systems transmit large amount of traffic, so the collapse of infected system is ensured. Such an attack causes a communication break between various heads and also leads to monetary losses. On a national level, a DDoS can cause system slowdown and hinder efficient administration by the government, while at the same time hovering as a constant threat to national security and integrity.[113]

1.5JUDICIAL RESPONSE

The Judiciary has a very important role to play when it comes to controlling the menace of cyber-terrorism. With the advent of judicial activism, or rather judicial adventurism, the Indian Judiciary has got a new dimension to venture into. The first issue which the Judiciary may face is of jurisdiction as before going into the merits, it should be satisfied that it has the requisite jurisdiction to do so. Since internet is not a 'single-entity owned or government operated', it cannot be regularised as an ordinary crime by invoking the jurisdiction. Again, the cross-border terrorism may also give rise to the problem of jurisdiction. The Indian Judiciary may have the jurisdiction to deal with these cases if the victim is in India, and/or the perpetrator is present in India, or the cause of action lies in India, or if the primary effect of the attack is on India. Another situation may arise when none of the given situations are present, but extraordinary circumstances are present and the country's sovereignty or security is at stake. In that case too, the Judiciary may have the jurisdiction to take up the matter. Otherwise also, section 1(2) read with section 75 of the Information Technology Act, 2000 gives courts the jurisdiction to deal with matters outside India. Apart from the jurisdictional matters, the Judiciary should also be well equipped with appropriate and adequate laws to decide the matters with utmost strictness and provide harsh and deterring punishments to the originators of these attacks. An active Judiciary must be backed with laws that are generic and living in nature, further watered by way of precedents. Lack of precedents causes hindrances in development of the law as without judicial interpretation, the law remains confined to its literal meaning and there is little scope to fill up the lacunae therein. The role of Judiciary must be supported by the whole lot of citizens and netizens who reap the benefits of internet but are targeted as victims. But at the same time, it is the duty of the court to ensure anonymity and security to them.

1.6 LET'S SUM UP

Efforts should be made to make a comprehensive law with both national and international approach to stop cross-border cyber-attacks with a smooth mechanism for redressal. Adopting a mutual code of cyber legislation can go a long way as cyber-terrorism knows no borders and thus, a well incorporated mechanism must be evolved. If internet can be used to spread terrorism, the same can be used to

[113]E. Waak, The Global Reach of Privacy Invasion, Humanist, November/December 2002: http://www.thehumanist.org/humanist/articles/waakND02.htm

tackle it also. The Ministry of Electronics and Information Technology, Government of India's 'e-security' scheme is a well applauded step in this direction. While there can be various approaches to deal with this issue, the one provided in the United Nations' Counter Terrorism Implementation Task Force seems to be the most rational and practical one. According to Counter-Terrorism Implementation Task Force (CTITF), working group of UN, this proposition should be approached by a multi-disciplinary approach, involving experts in counter-terrorism, technology, law, public policy, law enforcement and human rights. As a single agency cannot deal with this issue, in the same way, a single legislation may not serve the purpose. Cyber-terrorism control can be put onto other Acts as well. For instance, online frauds because of online transactions and contracts can also come under the ambit of the Indian Contract Act, 1872 and the Sale of Goods Act, 1930. Protection of intellectual property is also one of the major problems in this era, be it inventions, formulae, movies, books, ideas or recipes and so on and so forth. The Indian Copyright Act and the Indian Trademarks Act may be altered to invoke special attention to this issue with respect to cyber-terrorism. As far as other illegal activities on the internet are concerned, while the Information Technology Act penalises them, other legislations may govern them. A specific legislation for this purpose may solve the problem to an extent, but as the gamut of cyber-terrorism is expanding, a holistic legal development is required to tackle this issue effectively. This may demand amendments in the existing statutes, a lot more oriented research and development, combined with the ability of secure technology, an active government agency and an open-eyed Judiciary.

1.7FURTHER READING

- NIPC, 'Cyberterrorism : An Evolving Concept. National Infrastructure Protection Centre' (National Infrastructure Protection Centre, June 2015) <www.nipc.gov/%20NIPC>
- M Gercke, 'Understanding Cybercrime : A Guide for Developing Countries' (International Telecommunication Union, March 2011) <www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf>
- Urgent measures for combating international terrorism' (Decree-Law, 27 July 2005) <www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026>

1.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How does cyber terrorism affect government agencies?**

   Cyber-terrorism also aims at leaking out confidential information not only of private individuals but also of the government and other agencies. Such information may be of national importance and of vital nature with respect to

the security and defence of a country. It can be used by terrorist outfits to facilitate their objectives and to further facilitate their infiltrations by finding the probable lacunae in the system. The same may be used to destroy property which is public or private, movable or immovable, and tangible or intangible.

1.9 ACTIVITY

Explain the judicial response towards the menace of cyber terrorism. (1000-1500 words)

Unit 2: THE CYBER TERRORISM CONUNDRUMAND 'PROTECTED' SYSTEMS

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Sections 70 & 66F of the IT Act: An Insight into the Concerns

2.4 Addressing The Concerns Regarding Section 70

2.5 Let's sum up

2.6 Further reading

2.7 Check your progress: Possible Answers

2.8 Activity

2.1 LEARNING OBJECTIVES

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

- Mens rea under the Information Technology Act, 2000
- The implications of sections 70 and 66 F of the IT Act, 2000
- The doctrine of mens rea under sections 70 and 66 F of IT Act, 2000

2.2 INTRODUCTION

"Crime is crime because it consists of misconduct that explicitly and seriously violates society's welfare or well-being, and that it is not safe to leave it redressable only by restitution of the person injured." After reading these lines, one can see how serious an act that constitutes fraud is: "wrongdoing that specifically threatens society." Equally important is the observation that it is something that cannot be remedied only by monetary rewards. However, there is something more important than the act (of wrongdoing) itself that this meaning ignores, including the accused's mens rea.[114] International criminal law recognizes that no offence, major or minor, may occur without an immoral mind, since the nature of a crime is its unlawful purpose, without which it cannot exist. As a result, punishing behavior without considering the actor's state of mind is both ineffective and unfair.

2.3SECTIONS 70 & 66F OF THE IT ACT: AN INSIGHT INTO THE CONCERNS

To begin, what exactly is a guilty mind? Since each offense consists of a prohibited act or omission together with whatever state of mind is required by the law that bans it, the answer to this question will vary. In this respect, the Penal Code of 1860 has numerous components relating to mens rea in phrases like "intentionally," "knowingly," "dishonestly," and so on. The Information Technology Act of 2000 (hereinafter "IT Act") also allows for such words.

However, the language of Section 70(3), which punishes simply gaining access to a protected system: "Any individual who secures or attempts to secure access to a protected system in contravention of the provisions...", contains no such requirement. Second, this issue leads to another, seemingly pointless question: should the legislature's purpose be to acquit an individual even though he has perpetrated the act with the intention "ordered" by the legislative provisions? This question would be resolved affirmatively under two circumstances: first, when the legal clause is not worded according to the legislature's purpose; and second, when the provision is not implemented according to the legislature's meaning. Both of these scenarios are crucial in the context of Section 66F of the IT Act. The statute is

[114]See: Gabriel Weimann, 'Cyberterrorism – How real is the threat', United States Institute of Peace, Special Report 119, December 2004; ZahriYunos and SharifuddinSulaman, 'Understanding Cyber Terrorism from Motivational Perspectives', *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), pp. 1-13; Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet', *First Monday*, Vol. 7, No. 11-4, November 2002.

divided into two parts: Section 66F (1) A and Section 66F (1) B of the IT Act, which specify the spectrum of cyber terrorism.

About the fact that it governs a serious crime like cyber bullying, the provision is too vague. The requirement of mens rea under the clause broadens the scope of the provision and causes concern in two respects. First, when we assume that an insecure system like the Aadhaar scheme falls beyond the scope of the provision, "knowingly" accessing a computer system without authorization becomes pretty straightforward to prove.[115] This is because the Aadhaar scheme is a framework that can only be lawfully obtained by a limited number of people. Furthermore, any leak of information from the Aadhaar database will be extremely harmful to the nation due to the current importance of such data. It would be easier to prove that the unauthorized access was followed by reasonable grounds to assume that the information was "likely to inflict harm to the sovereignty and dignity of India, the protection of the State,... public order."[116] As a result, the Aadhaar scheme can be inferred to be a device that is "limited for purposes of state protection" and hence comes under the purview of Section 66F (1) B of the IT Act. Second, someone who "knowingly" accesses any prohibited material or archive in regards to "contempt of court" or "defamation" falls under its purview. It should be remembered that slander or even contempt of court have little effect on state protection, making their presence impossible to explain. However, this Chapter is limited to the convenience of demonstrating entry to a computer device and does not address the inclusion of slander. The following section addresses the topic with the aid of an analogy.

A. AN ILLUSTRATION

The Unique Identification Authority of India (hereinafter "UIDAI" Aadhaar)'s scheme entails the gathering of biometric and demographic data from 1.3 billion individuals. It has created the world's largest biometric identity project, which must be carefully scrutinized to ensure that it complies with human rights. In reality, the database's wasteful management is not made available. Notably, the UIDAI has declared the Aadhaar database to be a "secure device" under Section 70 (1) of the IT Act, as well as stating that the biometric data stored is "important personal data" under Section 43A of the IT Act. The above section imposes on the UIDAI, which is a legal entity, an obligation of responsibility to enforce and uphold fair security standards and procedures. The Information Technology (Information Security Policies and Procedures for Protected Systems) Rules, 2018 (hereinafter "2018 Rules") outline the practices and procedures that must be followed in the case of protected systems (such as the Aadhaar database).According to the source, the UIDAI's compliance with most of the 2018 Rules' responsibilities is in doubt. This is as a result of the confirmed non-compliance. The 2018 Rules, for example, mandate that the UIDAI appoint a Chief Information Security Officer (hereinafter "CISO"). However, it has been stated with proof that the UIDAI currently lacks a CISO. As a result, the authority has been unable to keep the details intact, despite its best efforts. The author wants to emphasize that the Aadhaar database is only secured for its own sake, and that the UIDAI is not following fair protection procedures in order to fulfill its obligations under Section 43A of the IT Act. Let's take a look at a data leak scenario against this backdrop. After being able to enter the Aadhaar database, say

[115]Defense Intelligence Agency, 'Cyberterror.Prospects and Implications', pp. 10 and 9, respectively.

[116]JonalanBrickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', *CTC Sentinel*, August 2012, Vol. 5, No. 8, p. 6.

"A," an information technology student, circulated a connection on WhatsApp, reporting the "mismanagement" in the Aadhaar database.[117]
According to the WhatsApp links exchanged, he quickly hacked the personal information of 1.3 billion Indian people and made it available there. The connection has now reached thousands of people as a result of the subsequent sharing. Legally, gaining access to a computer device may or may not be considered a crime. To be held criminally liable, the individuals involved must be able to form the necessary criminal motive to commit the offense. Ethical hackers who break into a computer system for the sole purpose of seeing how it works do so with no intention of committing a crime. As a result, someone who wants to reveal the Aadhaar system's fallacy in order to raise public awareness about such a serious issue is not committing a crime just by accessing the database. As a result, "A," the hacker who gained access to the database, should preferably be exempt from all cyber-crime provisions. Surprisingly, a literal reading of the clause would place "A" as well as those who opened the shared connection under the purview of Section 66F of the IT Act. These people not only lacked authorization, but also knowingly accessed the device. This translates to them doing something that meets the requirements of the provision. To bolster his case, the author now adds a twist in the above-mentioned example (hereinafter referred to as "the modification"). Let's pretend that the connection posted by "A" does not currently have access to the database and has just come to the public's attention as a result of "A's" publicity stunt.
In this case, simply opening the connection would be considered a "attempt" to gain access to the device, which is punishable under Section 70 of the IT Act. In certain situations, one must consider the legislature's intent: was it the legislature's intention to prosecute those who accessed the connection exchanged on WhatsApp for crimes as serious as cyber terrorism under Section 70 of the IT Act? That certainly wasn't the case. These people, on the other hand, "knowingly" accessed information that was shielded for the sake of the state's protection and sought to enter a protected structure. As a result, they will be responsible under Sections 66F and 70 of the IT Act, according to current regulatory interpretation.[118]
At the same time, the UIDAI will exclude prosecution under Section 43A of the IT Act because it has never given clarification on the security mechanism in place to protect citizens' "sensitive personal data." Since the UIDAI's compliance with the 2018 Rules is unknown due to a lack of required details on the UIDAI's website, this is the case. This is significant because, in the case of covered structures like the Aadhaar database, the 2018 Rules are the applicable norm. Furthermore, there is a growing fear that the UIDAI has not implemented appropriate security procedures as a result of reports of non-compliance with the duty to nominate a CISO. To answer the author's questions about mens rea, consider the maxim of proportionality, which states that sentences should be proportionate in magnitude to the seriousness of a defendant's criminal behavior.[119] Applying this theory to the example, thousands of people who opened the connection out of respect for their personal information will be criminally liable and fall into the category of crimes punishable by incarceration for up to ten years or even a lifetime. The UIDAI, on the other hand, which has violated

[117]Daniel Cohen, 'Cyber terrorism: Case studies', in *Cyber Terrorism Investigator's Handbook*, Chapter 13.
[118]Department of Justice, 'ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison', *Justice News*, September 26, 2016.
[119]Ellen Nakashima, 'U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election', *The Washington Post*, December 25, 2019

a severe duty to keep information confidential, is only liable for a civil wrong under Section 43A of the Act, which it avoids in any situation due to the provision of “fair” action.As a result, the statute’s wording ignores the concept of proportionality, which, like mens rea, is a foundational principle of criminal law. The same thing should be taken into account when drafting criminal laws. After determining the location of the problem, it’s a good idea to include some concepts and provisions that will help you come up with a solution.

2.4ADDRESSING THE CONCERNS REGARDING SECTION 70

Examining Section 66 of the IT Act’s general clause on “computer based crimes,” whereas Section 70 of the IT Act to further reflects the legislature’s purpose. Acts coming under Section 43 of the IT Act that are performed “fraudulently or dishonestly” are punishable under Section 66 of the IT Act, which is a penal clause. To put an act into the scope of Section 66 of the IT Act, two broad requirements must be met. First, the act must fall under the scope of Section 43, and second, the act must be performed with the intent to defraud or deceive. The act of accessing a computer, storing, copying, or removing any data or material from such a computer is covered by Section 43 of the IT Act in its particular portion. The investigation, on the other hand, has nothing to do with the first ingredient. It is important to emphasize the requisite intention for our purposes. In a nutshell, the two degrees of purpose listed in the provision are as follows:
When anything is done fraudulently, it is done with the intent to defraud. When the deceiver receives a reward or profit, or even the possibility of receiving a gain as a result of the deception, he is said to have an intention to “defraud.”
Dishonestly - A deceptive motive is that that seeks to achieve unfairly by obtaining something one does not have. Wrongfully gaining clearly refers to gaining illegally.
Let us use this legal matrix to see if the conduct of those who tried to enter the Aadhaar database by clicking on the connection met the legal requirements. Their conduct does not trick anybody, nor does it entail an advantage, or even the possibility of one. As a result, it does not qualify as a deceptive act. Similarly, their conduct is not unethical as they do not want to reap unfairly. As a result, while the acts of the citizens do not meet the requirements of the less serious crime punishable under Section 66 of the IT Act, they specifically meet the requirements of the more serious offence punishable under Section 70 of the IT Act. As a result, adding one of the two degrees of purpose included in the former section as an additional condition to the latter would limit the scope of the provision. As a result, situations like the one described above would fall beyond the scope of the clause, resolving the issue to a large degree.

2.5 LET’S SUM UP

This demonstrates how many criminal aspects of the IT Act, which were written in a broad sense, require more specific language to preclude ethical hackers. This necessity necessitates the inclusion of other degrees of mens rea in the provisions of Sections 66F and 70 of the IT Act. Alternatively, if an amendment requiring the use of mens rea as a component of the offence is deemed unsuitable, there is a remedy.

The issue of ethical hackers could be addressed by establishing a system of officially authorizing ethical hacking by legislation or subordinate legislation. This will, to a large degree, suffice in answering the author's questions. While the government, and in the event of its failure, the judiciary, must ensure that the UIDAI complies with the 2018 Rules, the suggested solutions for Sections 66F(1)(B) and 70 of the IT Act require legislative or executive action in the manner recommended in the preceding paragraphs. These provisions must be written in a way that represents the legislature's purpose while also facilitating their proper execution. The author acknowledges that the IT Act is a comparatively recent statute that is currently experiencing drastic revisions, but he addresses these topics that need to be addressed immediately.

2.6FURTHER READING

- Aadhaar in numbers: key figures from UIDAI CEO's presentation to the Supreme Court, THE HINDU, March 22, 2018.
- Editors' Guild, Others Condemn FIR Against Journo For Exposing Aadhaar Data Leak, Demand Centre's Intervention, LIVELAW.IN, January 7, 2018.

2.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What constitutes a guilty mind?**

   Various components related to mens rea are used in words such as "intentionally," "knowingly," "dishonestly," and so on, according to the Penal Code of 1860. The Information Technology Act of 2000 (hereinafter "IT Act") also allows for such words.

2.8 ACTIVITY

Explain the concerns associated with sections 77 and 66F of the IT Act. (1000-1500 words)

3

Unit 3: COUNTERING CYBER TERRORISM EFFECTIVELY

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Motivations for Cyber Terrorism

3.4 Types of Cyber Terrorism Attack

3.5 Psychological Effects of Cyber Terrorism to Humans

3.6 Let's sum up

3.7 Further reading

3.8 Check your progress: Possible Answers

3.9 Activity

3.1 LEARNING OBJECTIVES

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

- How to counter cyber terrorism effectively
- Reasons for cyber terrorism
- Types of cyber terrorism attacks
- Mental effects of cyber terrorism

3.2 INTRODUCTION

The Federal Bureau of Investigation (FBI) and the System Administration, Networking, and Security Institute (SANS) released a list of the top 20 flaws in Internet-connected networks in 2001, according to a survey reported by PCWorld.com online magazine. The study advised companies to close the dangerous gaps in order to prevent potential cyber terrorist attacks. “The Internet is clearly not ready because of these vulnerabilities; we’re not ready to survive a massive attack,” says SANS Institute Director Allan Paller in the post.[120]

We can’t help but concur with Allan’s viewpoint on the subject. We will find it incredibly difficult to protect ourselves from cyber terrorist threats due to the massive and free existence of cyberspace. As a result, it is critical that we delve deeply into the problems of cyber terrorism and gain a thorough understanding of them in order to defend our nation’s, industries’, and personal interests from cyber attacks. Cyber terrorism is characterized as electronic attacks from cyberspace, originating from both internal and external networks, especially the Internet, that are directed at a specific target and originate from a variety of terrorist sources with varying motives.

Cyber terrorists typically see high-profile elements of a country’s sensitive infrastructures or company activities as their targets. The primary goal of these terrorists is to do significant physical and psychological harm to targets by doing damage that compromises or destroys them. “The ultimate threat to information security is the insider,” says Clifford A. Wilke. It is a well-known phenomenon that the majority of data breaches occur inside organisations. As a result, cyber terrorism may also take the form of computer assaults carried out by sanctioned insiders, through which the terrorists have gained internal access to networks and databases by different means, such as jobs with the organisation. Internal threats are much more risky than external attacks, owing to the obvious difficulty of identifying them. In addition to overt insider threats, unsafe relationships with contracting firms who recruit or have been compromised by attackers may be hazardous. As a result, it is critical that efforts to combat cyber terrorism begin at the source, which means that organisations must prioritize internal and external security equally, if not more than external security.[121]

[120]Thibodeau, Patrick. “Internet Vulnerabilities to Cyberterrorism Exposed. “ 1 October 2001. URL: http://www.pcworld.com/news/article/0,aid,64224,00.asp

[121]A. Wilke, Clifford. “Infrastructure Threats from Cyber-Terrorists.” 5 March 1999. URL: http://www.occ.treas.gov/ftp/bulletin/99-9.txt

3.3MOTIVATIONS FOR CYBER TERRORISM

Terrorists use cyber warfare as a means of inflicting harm or destruction to their targets for a variety of reasons.[122] Terrorism attacks have four key goals: disrupt enemy organizational capability, destroy or distort the prestige of an organisation, country, or alliance; force those targeted to change affiliation; and show to their own supporters that they are capable of causing serious harm on their objectives.[123]

- **To destroy enemy's operational capabilities**

  This is the primary justification for the use of cyber terrorism. Terrorists believe that using cyber capabilities provides them with a low-cost and reliable way to seriously harm or kill their targets, preventing them from continuing their regular operations. The results of such attacks, if effective, can be devastating in a variety of ways, including significant economic and social collapses. If vital infrastructure and company activities are disrupted, an entire country or business may be brought to a halt.

- **To destroy or misrepresent the reputation of an organization, nation or alliance**

  One of the key aims of cyber terrorism is to do this. Because of their unmistakable and solid prestige, many organisations, states, and associations are able to act successfully and are well valued and esteemed. If this critical component is tainted, it could have a significant effect on the targeted entity's daily operations. Web site defacements and circulating fake news about the target through electronic means such as e-mail, web pages, and others are the most common methods of undermining or misrepresenting the target's credibility.

- **To persuade those attacked to change affiliation**

  Cyber bullying is often used to compel attacked organisations to alter their relationship or association with specific groups. Despite the fact that achieving this objective is even more difficult, it has been accomplished in the past. To defend against such motivated threats, the attacked entity must form close relationships with its partner organizations in order to properly manage the situation or prevent it from occurring in the first place.[124]

- **To demonstrate to their own followers that they are capable of inflicting significant harm on their targets**

  Cyber militants are now eager to carry out cyber attacks in order to demonstrate to their fans and the rest of the world that they are capable of

[122]Sproles, Jimmy; Byars, Will. "Statistics on Cyber-terrorism." 1998. URL: http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm

[123]Axelrod, C. Warren. "Security Against Cyber Terrorism." 27 February 2002. URL: http://www.sia.com/iuc2002/pdf/axelrod.pdf.

[124]Erbschloe, Michael; Vacca, John. Information Warfare: How to Survive Cyber Attacks. Reading: McGraw-Hill Osborne Media, 2001.

wreaking havoc on their targets. There are so many people who are sceptical of the realities of cyber terrorism and its capability. As a result, if cyber criminals feel compelled to demonstrate their ability to carry out electronic-based attacks on their targets, they will do so to demonstrate their "prowess" to the rest of the world.[125]

3.4TYPES OF CYBER TERRORISM ATTACK

Cyber threats use a number of different forms of cyber warfare attacks. Cyber terrorism capabilities can be classified into three groups, according to the Naval Postgraduate School in Monterey, California's Center for the Study of Terrorism and Irregular Warfare: "simple-unstructured," "advanced-structured," and "complex-coordinated."

- **Simple-Unstructured**

  The ability to use software developed by others to perform simple hacks on specific systems. This style of enterprise has restricted target analysis, command, and control skills, as well as learning capabilities.
- **Advanced-Structured**

  The ability to launch more complex attacks against different devices or networks, as well as the ability to change or build simple hacking techniques. The company has basic goal analysis and command and control abilities, as well as a limited learning capacity.
- **Complex-Coordinated**

  The ability to launch concerted assaults against interconnected and heterogeneous defenses in order to cause widespread destruction. Terrorists are capable of using advanced hacking techniques. They may also perform target analysis and command and control operations. They still have a high level of organizational learning capabilities.

Incursion, disruption, misinformation, denial of service, and defacement of websites are the five major forms of cyber crime attacks. Some of these attacks are more serious than most, and they both have different goals. It is important that we consider the multiple attack tactics in order to achieve a greater understanding of how they can be successfully countered.[126]

- **Incursion**

  These attacks are carried out with the aim of obtaining access to or breaching computer systems and networks in order to obtain or alter data. This is a common and commonly used approach with a high success rate. Terrorists can exploit several loopholes in vulnerable operating systems and networks to

[125]Glaessner, Thomas; Kellermann Tom; McNevin, Valerie."Electronic Security: Risk Mitigation In Financial Transactions". June 2002. URL: http://www1.worldbank.org/finance/assets/images/E-securityRisk_Mitigation_In_Financial_Transactions-3.0.pdf

[126]Bryen, Stephen. ITU Workshop on Creating Trust in Critical Networks Infrastructure."A Global Security Approach to Protecting the Global Critical Infrastructure." 2002. URL: http://www.itu.int/osg/spu/ni/security/workshop/ presentations/cni.20.pdf

access and/or change sensitive information that can be used to do more harm to the organisation or for personal benefit.

- **Destruction**

  This kind of intrusion is used to break into computer systems and networks with the purpose of causing significant harm or damaging them. Depending on the nature of the attacks, the effects of such an incident can be devastating, with organisations being forced to shut down for an indefinite period of time. It will be very expensive for impacted companies to have their activities back up and running, which would have a significant financial effect as well as a negative impact on their image.

- **Disinformation**

  This approach is used to disseminate rumors or facts that may have a significant effect on a specific goal. Whether or not the rumours are real, the use of such threats carelessly will cause uncontrollable confusion in a country or organisation. This method of attack is difficult to stop since it can be carried out in a matter of seconds without requiring access to the victim's computer or network systems.

- **Denial of Service**

  Denial of Service (or DOS) attacks, as they are more commonly called, are another popular attack type. E-commerce powered businesses that offer goods or services online are the hardest hit by such attacks. Cyber hackers have also been known to threaten public websites with this form of attack. DOS attacks are designed to bypass or interrupt online operations by overwhelming targeted servers with a large number of packets (requests), causing the servers to become incapable of handling regular service requests from legitimate users.The consequences of such attacks can be devastating from both an economic and social standpoint, resulting in significant casualties for organizations.

- **Defacement of web sites**

  This method of assault is designed to deface the victims' websites. The websites may be completely redesigned to include messages from cyber criminals for marketing or advertising reasons, which may result in their removal, or they can be redirected to other websites that may include identical messages. Since more people are aware of the issue, the frequency of such attacks has decreased in recent years. However, a limited number of such incidents continue to occur, necessitating the implementation of appropriate monitoring protocols in order to prevent such humiliating and financially disastrous circumstances from occurring again.[127]

3.5PSYCHOLOGICAL EFFECTS OF CYBER TERRORISM TO HUMANS

[127]Shahar, Yael. "Information Warfare: The Perfect Terrorist Weapon." 31 October 2001. URL: http://www.ict.org.il/articles/infowar.htm

It goes without saying that if cyber terrorists destroy or threaten the nation's vital infrastructures or business processes, the people who are personally impacted will experience immense psychological trauma. We must not underestimate the psychological effect of cyber terrorist threats, when various individuals respond differently to certain circumstances. Any individuals that are personally impacted by cyber attacks, such as those that lose sensitive business information that can be used to endanger the organization's or the targeted person's well-being, can become fearful and live under extreme stress.
The person(s) affected may be physically harmed, which can have an effect on his or her mental health. In other situations, where misinformation attacks are carried out using blogs, e-mail, and other electronic means to refute rumors about a specific circumstance, organisation, or individual, the general public can experience chaos. People would panic, causing daily company practices and lifestyles to be affected. As a result, it is critical that the general public is well-informed about cyber terrorism and is able to recognise the actions that can be done to help address the issue. Psychological topics relating to the impact of cyber warfare on individuals, as well as appropriate approaches to treat related disorders, can be addressed more often in order to offer a reliable and better avenue for people who are concerned about those issues.

3.6 LET'S SUM UP

And if most of us are new to the world of cyber crime, it has proven to be a difficult one. In several nations, substantial progress has been made in protecting against cyber attacks thanks to business and government programs. It is universally acknowledged and understood by all that defense is not a one-stop shop. Instead, it's a never-ending path that everyone involved must be dedicated to. Understanding the various motivations and forms of threats, as well as considering the impact of cyber crime on sensitive infrastructures, enterprises, and individuals, as well as taking the often complex measures to reduce the chances of such attacks occurring, makes the challenge of defending against it such an enviable one. However, strategic security initiatives and strengthened working relationships among different bodies, including industry, government, and the general public, give us all a good chance of winning this war. The truth is that cyber bullying is here to remain, and we still have a long way to go in successfully defending the nation's, corporations', and our interests. The good news is that, thanks to the numerous strategic strategies in progress, we are moving closer to our key goal of having a highly stable and efficient working climate.

3.7FURTHER READING

- Thibodeau, Patrick. "Internet Vulnerabilities to Cyberterrorism Exposed."
- A. Wilke, Clifford. "Infrastructure Threats from Cyber-Terrorists."
- E. Denning, Dorothy. Testimony before the Special Oversight Panel on Committee on Armed Services US House of Representatives "Cyber terrorism."

3.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the main factors of motivation for cyber terrorism?**

   Terrorism attacks have four key goals: disrupt enemy organizational capability, destroy or distort the prestige of an organisation, country, or alliance; force those targeted to change affiliation; and show to their own supporters that they are capable of causing serious harm on their objectives.

3.9 ACTIVITY

Explain the psychological effects of cyber terrorism on Humans. (1000-1500 words)

Unit 4:ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR AND OTHER CYBER THREATS

4

4.1 Learning Objectives

4.2 Introduction

4.3 “Routine” Failure v. Cyber Attack

4.4 Hacking and Terror

4.5 Cyber Crime and Economy

4.6 Let’s sum up

4.7 Further reading

4.8 Check your progress: Possible Answers

4.9 Activity

4.1 LEARNING OBJECTIVES

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

- The differences between the intelligence failure and cyber attacks
- The concepts of hacking and terror
- Impact of cyber crime on economy

4.2 INTRODUCTION

Cyber-terrorism is not the first time a new technology has been seized upon as creating a strategic vulnerability. While the match between theories of cyber-warfare and air power is not precise, a comparison of the two is useful. In reaction to the First World War, European strategists like Douhet and Trenchard argued that aerial bombing attacks against critical infrastructure well behind the front lines would disrupt and cripple an enemies' capacity to wage war.[128] Their theories were put to the test by the U.S. Army and Royal Air Forces during World War II in strategic bombing campaigns aimed at destroying electrical power, transportation and manufacturing facilities. Much of the first tranche of literature on cyber attacks resembles in many ways (and owes an unspoken debt to) the early literature on strategic bombing.

A key document for understanding how attacks on infrastructure affect societies is the Strategic Bombing Survey conducted by the United State during and after World War II. During the war, Britain and America launched thousands of heavy bombers that dropped millions of tons of high explosives on Germany, seeking to cripple its infrastructure, destroy its industrial base and break the will of the population to continue the war. Early theorists of air warfare had predicted that such an onslaught would paralyze or cripple the target.[129] What the survey found, however, is that industrial societies are impressively resilient. Industrial production actually increased for two years under the bombing and it was not until ground forces occupied Germany that resistance ceased: As the air offensive gained in tempo, the Germans were unable to prevent the decline and eventual collapse of their economy. Nevertheless, the recuperative and defensive powers of Germany were immense; the speed and ingenuity with which they rebuilt and maintained essential war industries in operation clearly surpassed Allied expectations. Germany resorted to almost every means an ingenious people could devise to avoid the attacks upon her economy and to minimize their effect. The mental reaction of the German people to air attack is significant. Under ruthless Nazi control, they showed surprising resistance to the terror andhardships of repeated air attack, to the destruction of their homes and belongings, and to the conditions under which they were reduced to live. Their morale, their belief in ultimate victory or satisfactory compromise, and their

[128]Barton Gellman, " Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002

[129]DeNileon, Guy, "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2001, Volume 93, No. 5, pp. 78–85,http://www.awwa.org/Communications/journal/Archives/J501es3.htm, see also Scott Berinato, "Debunking the Threat to Water Utilities," CIO Magazine, March 15, 2002,

confidence in their leaders declined, but they continued to work efficiently as long as the physical means of production remained. The U.S. found similar results from aerial bombardment during the Vietnam War.
Counter-intuitively, the effect of aerial attack was often to harden and increase popular support for continued resistance. The advent of nuclear weapons (and perhaps large precision-guided munitions) gave air power the ability to disrupt civil infrastructures needed to achieve the visions of Douhet, Trenchard or Mitchell, but cyber attacks do not pose the same level of lethality. One of the Strategic Bombing Survey's conclusions was that "The German experience showed that, whatever the target system, no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary." However, cyber attacks are likely to be single attacks. Once a hacker has gained access and the damage done, the target usually responds quickly to close off the vulnerability that allowed that line of attack and to bring systems back on line. Cyber attackers would continually need to exploit new vulnerabilities and new tactics to ensure sustained disruption. Cyber attacks also seldom if ever produce physical damage that requires time-consuming repairs.[130]

4.3"Routine" Failure v. Cyber Attack

Critical infrastructure protection creates a new set of problems for national security. Different actors are involved. The focus is on civilian and commercial systems and services. Military force is less important. The scope of these new problems depends on how we define national security and how we set thresholds for acceptable damage. From a legal or public safety perspective, no country will accept even a single attack on infrastructure or interruption of services.[131] If the goal is to prevent cyber-attacks from costing a single day of electric power or water service, we have set a very high standard for security. However, from a strategic military perspective, attacks that do not degrade national capabilities are not significant. From this perspective, if a cyber-attack does not cause damage that rises above the threshold of the routine disruptions that every economy experiences, it does not pose an immediate or significant risk to national security.
It is particularly important to consider that in the larger context of economic activity, water system failures, power outages, air traffic disruptions and other cyber-terror scenarios are routine events that do not affect national security. On a national level, where dozens or even hundreds of different systems provide critical infrastructure services, failure is a routine occurrence at the system or regional level, with service denied to customers for hours or days. Cyber-terrorists would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect. For most of the critical infrastructure, multiple sustained attacks are not a feasible scenario for hackers, terrorist groups or nation states (particularly for nation states, where the risk of discovery of what would be universally seen as an act of war far outweigh the limited advantages gained from cyber-attacks on infrastructure).

[130]Larissa Paul, "When Cyber Hacktivism Meets Cyber terrorism," SANS Institute, February 19, 2001 "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding…"
[131]Riptech Internet Security Threat Report, July 2002

4.4HACKING AND TERROR

Much of the early work on the 'cyber threat' depicted hackers, terrorists, foreign spies and criminal gangs who, by typing a few commands into a computer, can take over or disrupt the critical infrastructure of entire nations. This frightening scenario is not supported by any evidence. Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations. Cyber-terrorism has attracted considerable attention, but to date, it has meant little more than propaganda, intelligence collection or the digital equivalent of graffiti, with groups defacing each other's websites. No critical infrastructures have been shut down by cyber attacks. Terrorists seek to make a political statement and to inflict psychological and physical damage on their targets. If terrorism is an act of violence to achieve political objects, how useful will terrorists find an economic weapon whose effects are gradual and cumulative? One of Al Qaeda's training manuals, "Military Studies in the Jihad Against the Tyrants" notes that explosives are the preferred weapon of terrorist because "explosives strike the enemy with sheer terror and fright." Explosions are dramatic, strike fear into the hearts of opponents and do lasting damage. Cyber attacks would not have the same dramatic and political effect that terrorists seek.[132]

A cyber attack, which might not even be noticed by its victims, or attributed to routine delays or outages, will not be their preferred weapon. If terrorism is an act of violence to create shock and achieve political objects, how useful will terrorists find an economic tool whose effects are at best gradual and cumulative? An analysis of the risk of cyber terrorism is also complicated by the tendency to initially attribute cyber events to military or terrorist efforts when their actual source is civilian recreational hackers. When DOD computer networks were penetrated in an attack that occurred in the late 1990s, the U.S. was quick to suspect potential opponents, particularly Iraq or China, as the culprit. U.S. officials debated the merits of an active defense and whether this was an act of war, justifying a counter-attack. As tension mounted, the U.S. discovered that far from being a hostile power, the source of the attack was two high school students in southern California. It is difficult, especially in the early stages of an incident, to determine if the attacker is a, terrorist, group, foreign state, criminals, or a teenager in California. However, a quick survey of incidents over the last four years suggests that criminals and bored teenagers are the most likely sources of attack. To this day, the vast majority of hacking incidents result from the actions of recreational hackers. While the press has reported that government officials are concerned over Al Qaeda plans to use the Internet to wage cyber-terrorism, these stories often recycle the same hypothetical scenarios previously attributed to foreign governments' cyber-warfare efforts.

The risk remains hypothetical but the antagonist has changed from hostile states to groups like Al Qaeda. The only new element attributed to Al Qaeda is that the group might use cyber attacks to disrupt emergency services in order to reinforce and multiply the effect of a physical attack. If cyber-attacks were feasible, the greatest risk they might pose to national security is as corollaries to more traditional modes of

[132]www.terror.net: How Modern Terrorism Uses the Internet, by Gabriel Weimann (Special Report 116, February 2004

attacks. Espionage opportunities created by a greater reliance on internet-accessible computer networks will create greater risk for national security than cyber attacks. Terrorist groups are likely to use the Internet to collect information on potential targets, and intelligence services can not only benefit from information openly available on the web but, more importantly, can benefit from the ability to clandestinely penetrate computer networks and collect information that is not publicly available. This is very different from hacking, in that in the event of a successful penetration of a hostile network, a terrorist group or an intelligence service will want to be as unobtrusive as possible.

A sophisticated opponent might hack into a system and sit there, collecting intelligence and working to remain unnoticed. It will not disrupt essential services or leave embarrassing messages on websites, but remain quietly in the background collecting information. Collection techniques for the Internet differ significantly from earlier signals and communications intercept techniques, and while different kinds of data will be collected, the overall effect may be to make some espionage activities much more rewarding. This topic, the implications for espionage of the greater use of computer networks and Internet protocols, deserves further study.[133]

4.5CYBER CRIME AND ECONOMY

Cyber attacks do pose a very real risk in their potential for crime and for imposing economic costs far out of proportion to the price of launching the attack. Hurricane Andrew, the most expensive natural disaster in U.S. history, caused $25 billion dollars in damage and the average annual cost from tornadoes, hurricanes, and flood damage in the U.S. is estimated to be $11 billion. In contrast, the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. Putting aside for the moment the question of how the estimates of the Love Bug's cost were calculated (these figures are probably over-estimates), the ability of a single university student in the Philippines to produce this level of damage using inexpensive equipment shows the potential risk from cybercrime to the global economy. The financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity, etc.) make up a large proportion of the reported cost of cyber attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. For example, if a Distributed Denial of Service attack prevents customers from reaching one online bookseller, they may instead go to another to purchase their books. The aggregate national sale of books could remain the same although the first bookseller's market share would decline.[134]

A small number of customers may choose not to bother going to another site if their first choice is unavailable, but some of these lost sales may well be recouped by later return to the sight by the customer. Businesses face greater damage from financial fraud and theft of intellectual property over the Internet, crimes that continue to grow in number. Emphasizing the transnational nature of cyber security issues, the last few years have seen the emergence of highly sophisticated criminal gangs capable of exploiting vulnerabilities in business networks. Their aim is not terror, but

[133]The Diplomacy of Counterterrorism: Lessons Learned, Ignored, and Disputed (Special Report 80, January 2002

[134]For terrorism and counterterrorism links, visit www.usip.org/library/topics/terrorism.html

fraud or the collection of economically valuable information. Theft of proprietary information remains the source of the most serious losses, according to surveys of large corporations and computer crime. These crimes must be differentiated from the denial of service attacks and the launching of viruses. Denial of services or viruses, while potentially damaging to business operations, do not pose the same level of risk.

Cybercrime is a serious and growing threat, but the risk to a nation-state in deploying cyber-weapons against a potential opponent's economy are probably too great for any country to contemplate these measures. For example, writers in some of China's military journals speculated that cyber attacks could disable American financial markets. The dilemma for this kind of attack is that China is as dependent on the same financial markets as the United States, and could suffer even more from disruption. With other critical infrastructures, the amount of damage that can be done is, from a strategic viewpoint, trivial, while the costs of discovery for a nation state could be very great. These constraints, however, do not apply to non-state actors like Al Qaeda. Cyber attacks could potentially be a useful tool (albeit not a fatal or determinative tool) for non- state actors who reject the global market economy.

4.6 LET'S SUM UP

The Internet is a new thing, and new things can appear more frightening than they really are. Much of the early analysis of cyber-threats and cyber security appears to have "The Sky is Falling" as its theme. The sky is not falling, and cyber weapons seem to be of limited value in attacking national power or intimidating citizens. The examples presented in this paper suggest that nations are more robust and resilient than the early theories of cyber terror assumed. To understand the vulnerability of critical infrastructures to cyber attack, we would need for each target infrastructure a much more detailed assessment of redundancy, normal rates of failure and response, the degree to which critical functions are accessible from public networks and the level of human control, monitoring and intervention in critical operations. This initial assessment suggests that infrastructures in large industrial countries are resistant to cyber attack. Terrorists or foreign militaries may well launch cyber attacks, but they are likely to be disappointed in the effect. Nations are more robust than the early analysts of cyber- terrorism and cyber-warfare give them credit for, and cyber attacks are less damaging than physical attacks. Digital Pearl Harbors are unlikely. Infrastructure systems, because they have to deal with failure on a routine basis, are also more flexible and responsive in restoring service than early analysts realized. Cyber attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective. However, if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cybercrime may be not be fully appreciated by many observers.

This is not a static situation, and the vulnerability of critical infrastructure to cyber attack could change if three things occur. Vulnerability could increase as societies move to a ubiquitous computing environment when more daily activities have become automated and rely on remote computer networks. The second is that vulnerability could increase as more industrial and infrastructure applications, especially those used for SCADA (Supervisory Control and Data Acquisition), move from relying on dedicated, proprietary networks to using the Internet and Internet protocols for their operations. This move to greater reliance on networks seems

guaranteed given the cost advantage of Internet communications protocols (Transmission Control Protocol/Internet Protocol), but it also creates new avenues of access. These changes will lead to increased vulnerabilities if countries do not balance the move to become more networked and more dependent on Internet protocols with efforts to improve network security, make law enforcement more effective, and ensure that critical infrastructures are robust and resilient. From a broader security perspective, nations now face a range of amorphous threats to their safety that are difficult for the traditional tools of national security to reach. The lines between domestic and foreign, private and public, or police and military are blurring, and the nature and requirements of national security are changing rapidly. The most important implications of these changes for cyber security may well be that national policies must adjust to growing interdependence among economies and emphasize the need for cooperation among nations to defeat cyber threats.

4.7FURTHER READING

- U.S. Strategic Bombing Survey, Summary Report (European War), 1945.
- Barton Gellman, " Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002
- DeNileon, Guy, "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2001, Volume 93, No. 5.

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the difference between routine failure and cyber attack?**

   On a national level, where dozens or even hundreds of different systems provide critical infrastructure services, failure is a routine occurrence at the system or regional level, with service denied to customers for hours or days. Cyber-terrorists would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect.

4.9 ACTIVITY

Explain the effect of cyber attack on economy. (1000-1500 words)

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

○

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in