NAME: RAHUL VARMA

ROLL No: S20200010212

1. Read the article and summarize it.

(<https://telanganatoday.com/eye-spy-much-before-pegasus>)

Pegasus:

Software made by the Israeli group NSO.

It appears that a very invasive tool can activate and aim the phone's camera and microphone.

Pegasus is everywhere. While the scope of the police investigation is much more limitless right now, this is nothing new.

Spies were an integral part of the state system. Before referring to all of these nefarious activities as "Western" it is wise to consider espionage in various cultures including the Vedic culture.

In the kinds of literatures Epic, Puranica, Arthasastra,

The first traces of covert military work became visible within the scope outlined by the Ramayana and the Mahabharata, each being epic pies. The Arthasastra of Kautilya could be a treasure trove of valuable data, In this Regard, the Dharmasastras wear down the subject with care and some detail.

In the Mahabharata, Bhishma advises Yudhishtira :   
The king must use his spies on all his advisors, friends and children in his city and provinces and in the territories of the chiefs under his command. Your spies must be used in such a way that they do not know each other.

Christopher Saint Andrew traces in his gigantic story The Key World: A History of Espionage in 2018 the growth of the system in ancient China, The Art of War, which created taxonomy of spies. The Apostle Andrew further states that "the Christian Testament contains many references to spies than any history of England or most other countries."   
  
Richard Hakluyt, the author of England's first collection of travel journals, was a geographer and possibly a spy

The auspices of Hakluyt’s Patronage and served as material for many authors, including Shakespeare, but these texts also clearly documented details of other regions for future travel, exploration, and perhaps even conquest.

In India, the Indians used spies throughout the 19th century, especially as part of the "mutiny". The unidentified "Angad", a kind of super spy, became legendary in 1857-58, but was never identified.   
Espionage was a prerequisite for arrest, torture, and even murder. Ronen Bergman's terrifying story of Israeli intelligence operations, Rise and Kill in 2018, documents the history of their murders, but also shows how the foundations of the state were built on surveillance.   
  
In the 19th century, and especially during the "mutiny", both the British and the Indians employed spies. 'Angad', a kind of super spy, became legendary but was never identified.

Watching goes electronic:   
During the planetary wars and later conflicts, undercover work, unsurprisingly, reached extraordinary heights, expectedly. John LeCarre, Alistair Maclean, and several popular alternative writers built their careers around espionage, the Cold War, and the "heroes", many of whom were women, of the secret world.

With the help of drones, satellites, artificial intelligence-based government operations, espionage is more or less Routine for organizations and even individuals. We constitute ourselves as "surveillance subjects" in the age of electronic surveillance

Surveillance subjects:   
Today we tend to only become voters after police investigations, from Aadhaar to COWIN.   
Contemporary police investigations are growing like mushrooms and are gradually clearing up the everyday routine of mass organizations.   
Citizens of Global Witness:   
Monitoring enables a global culture of witness in which citizen participation in humanitarian surveillance increases.

Citizens reporting that lawmakers violated traffic rules, lawmakers viewed pornography, including documented media evidence, altered public perception, and launched mass campaigns during the House of Representatives proceedings. Websites like (www.witness.org) invite citizens to document these violations and humanitarian crises. In the COVID 2020-21, the images taken by the citizens generated campaigns both in the form of oxygen supply and food for patients.

The SSP worked to draw the world's attention to the mass atrocities in Sudan and used its imagery and analysis to generate swift human rights and human security responses to generate an international cultural reminder of atrocities. Now, in this age of vigilance, it is not possible to affirm the spiritual object of the atrocities and misfortune.

2. Write your views on the idea of privacy and privacy breach in the backdrop of the present, technologically advanced social scenario.

People give more preference to their privateness and additionally the safety in their private life. They really do not want their private records to be reachable to others at any time.

Privacy issues have progressively gained a broader public and political debate.

Today, social media like what’s app, Face book, Instagram, messenger, twitter, Telegram, snap-chat have become the most popular in social media.

People share pictures, news, and almost something that’s happening in their lives.

The massive quantity of knowledge that people share on social media – some of that is incredibly personal –attracts different viewers outside of their sure circle of relatives associate degreed friends.

Some people from somewhere can record abundant of what you are doing on your social media and even you will not know.

Most people don’t follow these:

Each website on the web has their own privacy terms and even social media sites.

Before signing into any social media, it is essential which you simply browse and understand their privacy terms.

Pay some interest to the privacy terms of the facts you are registering and agreeing to proportion after you sign on for a partner diploma account with a social media platform.

For instance, what content material can be shared with the 1/3 party, are you capable of deleting your content material at the net web website online permanently.

Don’t accept friend requests or follow the person whom u don’t know.

Before accepting any follow or friend request, analysis concerning the person, and understand who they are, what they do, and what quite content they share. Before you post any photos or vedio’s on social media, think twice. Posting photos on social media is too risky in social networking activities. Advertising about photos may create you, your preferred ones, or your home a tempting target for cybercriminals.

Protection tips:

Pick out a strong and stable password.

Use different passwords on all your social media accounts.

Don’t use public devices to access your social media accounts.

Avoid using of public gadgets to get logging to your social media accounts.

Avoid clicking on social media links which are sent by your friend without knowing about the content in the link.

Secure your gadgets with countersign safety to guard your social media and exclusive information simply in case they may be taken or lost.

A lot of our lives are online as the era turns into greater advanced.

As a result, it's essential to understand a manner to guard yourself against hackers and online predators. However, you can't do this while not understanding what you're protective yourself from.

Several hackers are actually tech-savvy thieves with coins as their motive, however that's now no longer always the case. Hackers have exceptionally diverse motives. There are hackers available who attempt to stunt the content material or combat for a worthy cause. There are others who attack businesses or personal rivals. Still, others wish to observe their hacking skills out of curiosity or just for fun.

Hackers can usually try to gather information equivalent to master card numbers or checking account information. They will either use this information themselves or sell it to the highest bidder. They will jointly try to obtain enough personal information to steal your identity enough to open new revolving credit or take out a loan in your name, leaving you on the verge of paying your balance and damaging your credit score for years to come.

The Covid19 pandemic has resulted in an inevitable surge in the use of digital technologies due to social distancing rules and statewide bans. People and organizations around the world have had to adapt to new ways of working and living. Digital wave and new research problems.

Growing digitalization is driving companies and educational institutions to move to the home office (WORK FROM HOME). Block-chain technology will gain in importance and require research into design and regulations. Assignment, collaboration, motivation, and aspects of work overload. Workplace monitoring and technical stress issues will gain in importance with increasing digital presence. Online fraud is likely to increase, along with research into security management. Regulation of the internet, a key resource, will be crucial after the pandemic.

PLEASE BE AWARE OF HACKER, BE CAREFUL AND MAINTAIN PRIVACY ON SOCIAL MEDIA.

THANK YOU