# Organized CyberCrime and the State of User Privacy

**Devansh Parikh[1] Harshvardhan Shani[2] Suraj Dave[3] Mr. Piyush Patel[4]**
[1,2,3]UG student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]SAL College of Engineering Ahmedabad, India

*Abstract*— When you open your browser, surf web, connect with your friends, do you suspect you are being watched? Organized cyber crime is a crime which happens right in front of you but you are oblivious to it. The privacy of every user who accesses the internet, is compromised every second. Which sites you surf, what you buy online, what are your preferences, where are you going and what are you going to do next, imagine all these information used either by online Ad agencies that could lure you into buying their products or by government agencies to create a complete psychological profile and to spy on you. In this paper, initially we discuss the philosophical notion of privacy and debate the underlying ethics. We also present the current scenario, how the users are being targeted and affected. Furthermore we criticize the advent of worldwide surveillance, state its ramifications and brief on how it is undertaken and who are behind it. We also analyze the laws and policies that fail and in some cases even permit malpractices that take advantage of users. We provide a timeline of how cyberattacks started and state the most devastating ones, the methods used and the damage they caused. Ultimately we draw conclusions and propose solutions to some problems and outline some already researched techniques found to be superior and bring forth a new perspective on how the system can be improved and new laws enacted or enhanced.

***Key words:*** Organized Cybercrime, User Privacy, Data theft, Mass Surveillance, Cyberattacks, Cookies, NSA

## I. INTRODUCTION

What is cyber crime ? Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage.

It was 22:30 hours on October 29, 1969, The first ARPANET link was established between the University of California, Los Angeles (UCLA) and the Stanford Research Institute.[1] The first words passed through this network was "LOGIN", had they thought cross their mind that 48 years later privacy would be such a big issue, they would have taken privacy a little more seriously. Who would have thought Internet would become such prominent, about 48% of the world's population uses the Internet, with the middle east region showing an approximate 1825% increase in usage.[43] In 2015, the International Telecommunication Union estimated about 3.2 billion people, or almost half of the world's population, would be online by the end of the year.[2] The shocking terror attacks of 9/11 led to implementation of The Patriot Act. The Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records and track the activity of innocent Americans on the internet.[3] User's privacy is always at risk as all their online activities are tracked and sold for various purposes. As the internet grows, hackers are finding new ways to attack and compromise user's data and privacy. We discuss in detail about the notion of privacy, the Illusion of it, explain how cookies work and its flaws, net neutrality, state the laws and propose new ones and the types of malware and how it is used to infect all the users on internet.

## II. THE NOTION AND ILLUSION OF PRIVACY

Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information.[4] Every user has a right to privacy and under the Universal Declaration of Human Rights, article 12 states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[4] Many scholars have stated their views on what privacy is, the rights of users and how to protect user's privacy. Jurists Samuel D. Warren and Louis Brandeis wrote The Right to Privacy, an article in which they argued for the "right to be let alone", using that phrase as a definition of privacy. [5] The meaning of "let alone" has interpreted and commented in different ways, one such interpretation being the users have the right to seclude themselves from the attention of others and protect themselves from the observation of others. This vague concept made it complicated to describe policy in simple terms, but it did start the discussion of privacy rights and made people more aware and concerned about them. It is debated what control over privacy is and a claim that an individual or group has should be able to determine for themselves, how, when and to what extent the information is communicated to others. Charles Fried said that "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves." and control over personal information is one of the more popular theories of the meaning of privacy.[6] Privacy is sometimes defined

as a way of having secrecy, Richard Posner said that privacy is the right of people to "conceal information about themselves that others might use to their disadvantage".[7] The times have changed and we need to rethink both practically and ethically how privacy rights and laws should be drafted and modified to the best of our collective interests.

Currently the state of privacy isn't strictly as per its definition. The true meaning has been lost. PRISM is a secret program used by the US National Security Agency (NSA) to collect private information of users from at least 9 major US companies like Google, Facebook, Microsoft, Apple, etc. PRISM began in 2007 and operates under Foreign Intelligence Surveillance Act (FISA) and uses Section 702 to collect even encrypted data from the companies. Documents revealed that it is the number one source for raw intelligence used by NSA. It accounts for 91% of NSA's internet traffic

Acquired under FISA.[8] The program and its dangerous and unethical activities were revealed by whistleblower Edward Snowden who worked for NSA and CIA. Although the government defended its use of PRISM and also stated it will not be used on domestic citizens without a warrant. Obama, during his visit to Germany, stated that the NSA's data gathering practices constitute "a circumscribed, narrow system directed at us being able to protect our people."[9] Although the program requires a court order, the permission granted are atrocious. The section 702 grants the following provisions:

1) Prohibits the individual states from investigating, sanctioning of, or requiring disclosure by complicit telecoms or other persons.
2) Permits the government not to keep records of searches, and destroy existing records (it requires them to keep the records for a period of 10 years).
3) Grants telecommunications companies immunity for cooperation with authorities
4) Increased the time for warrantless surveillance from 48 hours to 7 days
5) Requires FISA court permission to target wiretaps at Americans who are overseas.
6) Allows eavesdropping in emergencies without court approval, provided the government files required papers within a week.

These provisions granted by this law gives substantial power to the programs and organizations using it. One might wonder how much unethical use of this provisions have been made and how many more will be made, as no records will be kept and telecommunications companies have to comply. The number of requests made to 4 major companies and the data yielded from by the government is shown below.

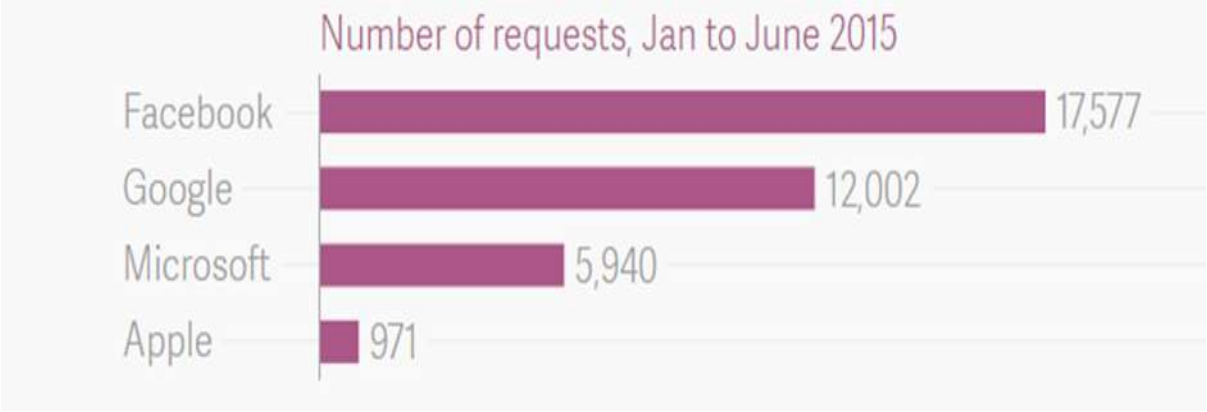


Fig. 1: Number of requests made by government to major companies in 2015 [16]


Fig. 2: Successful request percentage [16]

A staggering 17,577 No. of requests were made to Facebook in just a matter of 6 months. This shows how much government is trying to interfere in the lives of people. In a recent case of the San Bernardino shooter, FBI asked Apple to unlock the suspect's encrypted phone. Tim Cook says the FBI's request for a modified version of iOS amounts to a request for a "backdoor" that will create a "master key" that could be used to open all iPhones[10]. This went through great scrutiny as FBI asked a way to bypass authentication and access all the content. As apple refused due to obvious privacy concerns and their

policies, FBI charged apple a lawsuit. FBI dropped the lawsuit at last moment as it found a tool that could hack the phone which it bought from professional hackers for $1.3 Million. FBI has also declined to reveal the method used to hack the phone and in turn not reveal the vulnerability in the OS. FBI used a diplomatic cover stating it didn't buy the rights to the tool and hence it can't reveal any details related to it. This proves that FBI and the government is interested to gain access, either with the help of the company itself or by exploiting the vulnerability with some help from other professional hackers.

An alliance called as "Five Eyes" and bound by UKUSA agreement, a treaty for joint cooperation on signals intelligence, consisting of shared spying agencies of US, UK, Australia, New Zealand and Canada[17] was initially developed during the cold war to spy on communications of Soviet Union, but now it is used to monitor billions of private communications worldwide. Edward snowden described it as "supra-national intelligence organisation that doesn't answer to the known laws of its own countries"[18]. They used a software called Xkeyscore. Edward Snowden described it as a system capable of unlimited surveillance of anyone in the world. In an interview he explained what one could do with Xkeyscore as: "You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information."[12] Xkeyscore is passive program, it listens but does not transmit anything on the networks it targets. Xkeyscore consists of 700 servers at approximately 150 sites located all around the world,[13] the sources being spy planes, drones, backdoors,[40] satellites, third party intelligence agencies from various countries. From this sources, XKeyscore stores "full-take data", which are indexed by plug-ins that extract certain types of metadata (like phone numbers[41], E-mail addresses, log-ins, and user activity) and index them in metadata tables, which can be queried by analysts. XKeyscore has been integrated with MARINA, which is NSA's database for internet metadata.[14] The system continuously gets new data and so it stores the data only for 3-5 days and the metadata for 30 days. At some sites the data received per day is 20 TB and so is stored only for a day. One of the 3 subtypes of Xkeyscore, deep dive can process internet traffic at the data rates of 10 gigabits per second. Its capabilities are:

1) Look for the usage of Google Maps and terms entered into a search engine by known targets looking for suspicious things or places.
2) Look for "anomalies" without any specific person attached, like detecting the nationality of foreigners by analyzing the language used within intercepted emails.
3) Detect people who use encryption by doing searches like "all PGP usage in Iran".
4) Showing the usage of virtual private networks (VPNs) and machines that can potentially be hacked via TAO.
5) On July 3, 2014 ARD revealed that XKeyscore is used to closely monitor users of the Tor anonymity network[15], people who search for privacy-enhancing software on the web, and readers of Linux Journal.[16]

This shows how much capable the government is and what it can do with such powers. On the other side, NSA slides published claimed that Xkeyscore helped capture 300 terrorists by 2008. Now this is up for a debate that to what extent this powers should be utilized and who are to be targeted. Innocent people and their families are spied on, phone calls tapped, webcams and internet activity monitored. We need laws and policies that can decide this and ensure that the government does not circumvent it.

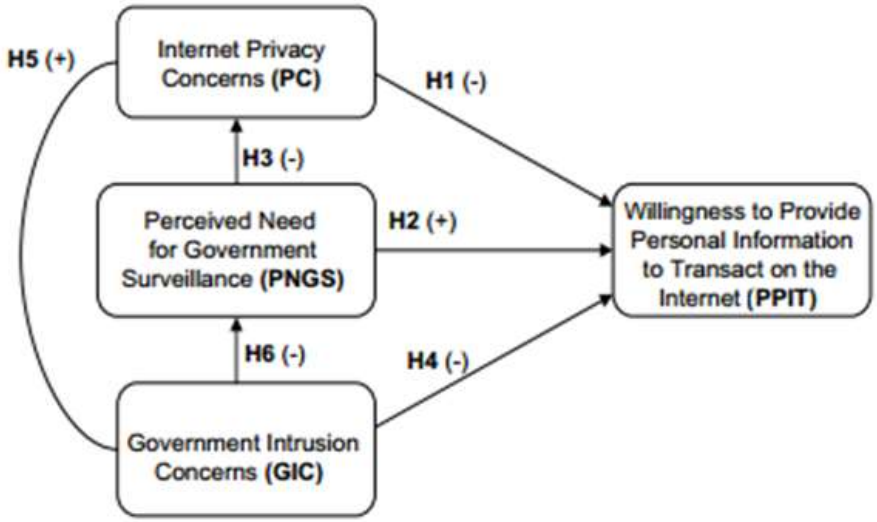


Fig. 3:

Researchers proposed a model to avoid using government surveillance and decrease the need for it.[44] The model basically shows that people should be given opportunity to willingly provide the information and if he doesn't and there is a perceived need, then it is decided if surveillance is absolutely necessary or not.

## III. THE SPIDERS

The spiders or web crawlers are used to crawl all the web pages available on the internet. A spider crawls by traversing links found on the initial pages it starts from. It builds an index of all the links traversed and stores in the database. They crawl

everything on the web excluding deep web. The size of deep web is estimated to be hundreds of times larger than the surface web. The deep web consists of some very valuable information and also is home to some of the most frightening content. The deep web is filled with markets of drugs, Counterfeit currency, Forged papers, firearms, human organs and hitmen. To crawl this deep web could be the key to a whole different region on the internet and might also help in stopping all the illegal activities carried on there. Researchers have proposed a new algorithm that could be able to crawl deep web with relative ease. A Q-value approximation algorithm that allows a crawler to select a query by learning from the experience of executed queries is proposed and they classify the stateof-art deep web crawling methods into three categories of baselines and demonstrate how our RL method outperforms them.[42]

## IV. CYBER ATTACKS, BREACHES AND THEIR AFTERMATH

Cyber attacks and breaches have been prevalent since the early times of internet and they are increasing every single day. It all began with Morris, first computer worm transmitted over internet. In 1988, a student from cornell university developed and spread this worm, which he claims were developed for the innocuous intention of exploring the vast cyberspace. The worm encountered a critical error and morphed into a virus which replicated itself and infected other computers on the internet. It affected 6000 computers and it was estimated it cost $10-100 Million in repair bills. This attack was the inspiration of a plethora of cyber attacks to come. A few prominent and most devastating attacks are listed below:

- In 1999, a 15 year old kid hacked US department of defense division and installed a backdoor which allowed him to intercept internal mails consisting of confidential military information. He later committed suicide due to allegations of him conspiring with other hacker to steal credit card information, which he denied in his suicide note.
- In 2000, a 15 year old kid from canada launched a DDOS attack on high profile websites like Amazon, CNN, ebay, yahoo, etc caused an estimated $1.2 Billion in damages.
- In 2009 in a classic act of government espionage, Chinese hackers implicated to be ordered by Chinese government, hacked and gained access to servers of Google. Google concluded that accounts of various chinese human rights activists were compromised and were routinely accessed without permission. Chinese government was accused of conspicuously disregarding human rights for years.
- The Melissa virus infected Microsoft word files and emailed the virus to the first 50 contacts of that user. It cost $80 Million in damages. Incidentally anti-virus sales saw a significant boost in sales. Its is conspired to be a trick to users to buy such a software and begin a new industry. Many pros don't use and deem use of anti-virus unnecessary. Leaks also suggest NSA exploited anti-virus softwares to spy on users[19]
- In 2002, a DDOS attack targeted towards all the 13 domain name system's root servers in US almost brought internet to a standstill. It lasted 1 hour and was considered the most complex attack at that time.
- In one of the biggest fraud cases in the history of US, a hacker named Gonzales stole credit and debit card details of millions of users from more than 250 institutions.
- In 2011, a hacker group called Lizard Squad hacked the Sony Playstation Network which compromised 77 million accounts and 12,000 credit card numbers. Sony's weak security measures and poor management caused Sony $171 Million and is considered one of the biggest cyberattack in history.
- Sony was hit with a massive attack once again in 2014. A hacker group named Guardians of Peace hacked Sony Pictures division. They used a Server Message Block worm tool consisting of listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool. The hackers leaked 100 TeraBytes of data and demanded to drop the release of its comedy movie "The Interview" about a plot of assassination of North Korean leader Kim Jong un and threatened to carry terrorists attacks. The US intelligence officials after careful evaluation, alleged the attack was sponsored by North Korea.[20]
- The Heartbleed bug found in 2014 is considered as the the biggest attack in the history with reports stating it affected 17%(half million) of all secure web servers certified by Trusted Authorities. The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library.The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.[21][22] eWEEK estimated a minimum of $500 Million in damages due to it[23]
- In a classic example of cyberwarfare a worm named Stuxnet believed to be a jointly built American-Israeli Cyberweapon and considered largest and costliest development effort in malware history.[24] It was built during the Bush administration to damage Iran's nuclear program. The Stuxnet specifically targeted PLCs, which allowed automation of electromechanical processes and exploited 4 Zero-day flaws. It had a rootkit component that prevented it from being detected. It was designed to change the centrifuges' rotor speed covertly, greatly increasing and then rapidly decreasing the speed. Stuxnet sabotaged 1/5th of Iran's nuclear centrifuges.[25]
- In the most recent case, in 2017, Cloudfare servers were found to be leaking sensitive cookies, Login credentials, API keys and authentication tokens from its servers to all the users who requested for service to any of its 6 million hosting customers

including Uber, fitbit and OKCupid. The vulnerability was patched in 7 hours, but it is yet to be determined how much damage it caused and it would be months to know if any of that leaked data was captured or stored by someone.

– The infamous hacktivist group Anonymous has also conducted a series of hacks since its inception and is considered the most elite hacker group. The have carried attacks like Project Chanology, Federal attack, Dark discovery, ISIS attack, WTO attack and Donald Trump's Website hack to name just a few. They have a very decentralized command structure that operate on ideas rather than directives[26] They are often called "freedom fighters" and "RobinHoods". In 2012, the Time magazine called Anonymous one of the "100 Most Influential people" in the world.[27]

These are a few of many cyber attacks happened till date and certainly they are rising every day. It is estimated that by 2020, the average cost of a data breach would be $150 million. With global annual cost forecast of $2.1 Trillion.[28] Even in 2015, 707 million records were exposed, with 2100 websites who had their data breached containing 2 billion entries in total.[29] For the fiscal year 2017, President Obama proposed a military defense budget of $523.9 billion and the budget for Cyber security of $19 billion.[30][31] With this budget proposal it is perspicuous were the main focus lies and how seriously major issues are dealt with. With the ever increasing risk and the inevitability of a cyber war lurking in our near future, it is essential we take right steps and measures to best avoid it.

## V. COOKIES

A Cookie is a small piece of encrypted text file created by a browser on the client's computer. They are also known as browser cookies or tracking cookies. Cookies are meant to store stateful information for the websites and to track the browsing activities of the user. One of the most common methods used by servers using cookies to know whether the user is logged in or not, and which account they are logged in with. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in.

Cookies have multiple benefits but cookies can also be used for malicious purposes. A supercookie is a cookie with an origin of a top level domain (such as .com) or a public suffix (such as .co.in). Ordinary cookies, by contrast, have an origin of a specific domain name, such as example.com.[11] Supercookie can be used for malicious purposes and therefore is blocked by web browsers. If it is unblocked, a person having control of a malicious website can create and set up a supercookie. It enables him to disrupt legitimate requests to another website that shares the same .com domains or public suffix such as .co.in

A Zombie cookie is a subtype of cookie which can recreate itself even after it is deleted. It does so by storing the contents of cookies on various locations such as Flash Local shared object, HTML5 WEB Storage, and other server-side and even client-side locations. When the absence of the cookie is detected it is resurrected.

Another application of cookies is Web Profiling, also known as cookie profiling. The cookies which are stored as a permanent cookie are used to track the user's online activities. Cookie profiling is done by storing cookies on the users system as soon as the user lands on a online page. It does not matter whether the cookie is temporary or a permanent cookie, a 'log' is created. It doesn't only occur while we are on a particular site but the entire time we browse the web. These information is used to create a user profile. This profile is then used to target the person with advertisements according to the browsing patterns, websites visited etc. The user profile is also sometimes sold to online retailers, e-commerce websites, marketers who in turn use it to target their customers and increase their customer base. Cookie profiling is not as of yet a cybercrime like Internet phishing which is now officially a cybercrime. The act of buying user profiles from advertisers can be considered a heinous and detestable act. We would like to speculate here that, what if, the user profiles collected by marketers and online retailers are in some manner acquired illegally by some unknown third party, and the user's' information is used for some spiteful purpose, then who would be responsible for our data/identity theft ?

Data collection these days have been easy task due to the Internet. This leads to privacy violations at social networking sites. Facebook in particular, like any other websites, utilizes cookies in order to monitor its users. The problem with Facebook using cookies is that even if the user signs out from the site, it does not stop tracking. Facebook actually uses two types of cookies; which are inserted when you sign up. One of these cookies is inserted when you open up the home page of the website. Additionally, Facebook uses different parameters for logged-in users, logged-off members, and non-members. These cookies record several different information about the user like e-mail address, password, friends, types of post, things you like, among others. These cookies also record date, time, and websites you visited. With these cookies, Facebook can paint a picture of your browsing behavior and can identify your religious affiliations, political leanings, and many other things about you. Facebook says that it does not "share your information with advertisers without your consent". But targeted advertising is always activated, there is no opt-in and no opt-out option.[39]

Attackers can now bypass the secure protocols of the https and reveal private session information. Modern browsers like Google's Chrome, Mozilla's Firefox and Apple's Safari, currently are unable to provide protection against the attack vector. A 'cookie injection attack' as described by Xiaofeng Zheng, it can be mounted by the man-in-the-middle attackers. They set cookies throughout their invasive session. These cookies then facilitate the disclosure of any private data that is transmitting in the session. This is possible because although cookies can contain a 'secure flag' which limits their use to HTTPS connections, the cookie itself has no provenance or chain-of-custody, so there is no mechanism by which it can be determined how it was originally set[32]. The reason attackers use cookies is that, cookies can traverse the sites in a manner which practically no other protocol is allowed to do.

There are many different approaches in which cookies can be used to hinder our privacy, some of these are:

*A. Cookie Theft:*

The attacker posts an auction that includes a link to what is advertised to be additional pictures or information about the object in the auction. Instead, when users click on the link, their cookie for the auction Web site is sent to the attacker's server, where a CGI script logs the information. Now the attacker can look through the list of cookies and pick some of the most recent cookies to use to try to log in to the auction site and spoof the user.

*B. Cookie Poisoning:*

The attacker visits an E-commerce site and adds an expensive item to his shopping cart. Then, the user examines the cookie stored on his system from that site to see whether the cookie includes the total cost of the items in the attacker's cart.

The attacker then modifies the cookie on his system to change the total to be $5.00 and resaves the cookie. Then, the user returns to the E-commerce site and checks his cart to see that the total is now $5.00 and proceeds to order the items with the false cost.

*C. Cross-Site Cooking:*

The attacker crafts a cookie for the domain ".com.uk" and sets up a Web site to distribute the cookie. Then, the attacker posts a link to his Web site on various bulletin boards or via e-mail, and when the users click on the link, they are given the attacker's crafted cookie that can then overwrite or disrupt the real business they do with Web sites in that international domain[33].

To overcome these problems, On May 26th 2011 new laws were introduced in Europe for the implementation of the cookies. Previously users were given an option to 'opt out', while the new law states that websites will need to specifically gain the consent of their users and they must 'opt in' to store cookies on their computer or any other device. Another alternative was suggested in the CERT and the Zheng paper, where the HSTS(HTTP Strict Transport Security) should be implemented at the server level to mitigate the vulnerability[32]. So what does the new law state?

The new requirement is that cookies can only be placed on machines where the user or subscriber has given their consent.

6 (1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.
(2) The requirements are that the subscriber or user of that terminal equipment--
(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
(b) has given his or her consent.
(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.

"(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.
(4) Paragraph (1) shall not apply to the technical storage of, or access to, information--
(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

*D. Alternatives to cookies:*

Researchers have proposed various techniques and methods that can be used as alternatives to cookies.

- JSON Web Token(JWT) is self contained packet that can be used in place of session cookies. Unlike cookies, JWTs must be explicitly attached to each HTTP request by the web application.
- The HTTP protocol contains access authentication protocols, which allow access to a web page only when they provide the correct username and password. If the server requires such credentials for granting access to a web page, the browser requests, stores and sends the credentials with every page request. The user can be tracked using this method.
- Various other techniques like the use of ip address to track the data, using query strings on URL, use of identifiers and etags, use of web storage, browser cache and browser fingerprint can be used to store data and for identification of user. A new type of cookie called Net cookie is proposed by a few Stanford researchers to combat Net Neutrality[38].But all these methods have some drawbacks that hinder the chances of destroying the cookie's dominant prevalence.[34]

## VI. THE ULTIMATE SOLUTION: TOR BROWSER

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.[35] Tor can be used for protection against surveillance and tracking. It was initially developed by US Naval Research Laboratory to hide the US communications online. It was later founder as a nonprofit organization and funded by US government, University of Cambridge, Human rights watch, Google and a few others.

*A. HOW TOR WORKS:*

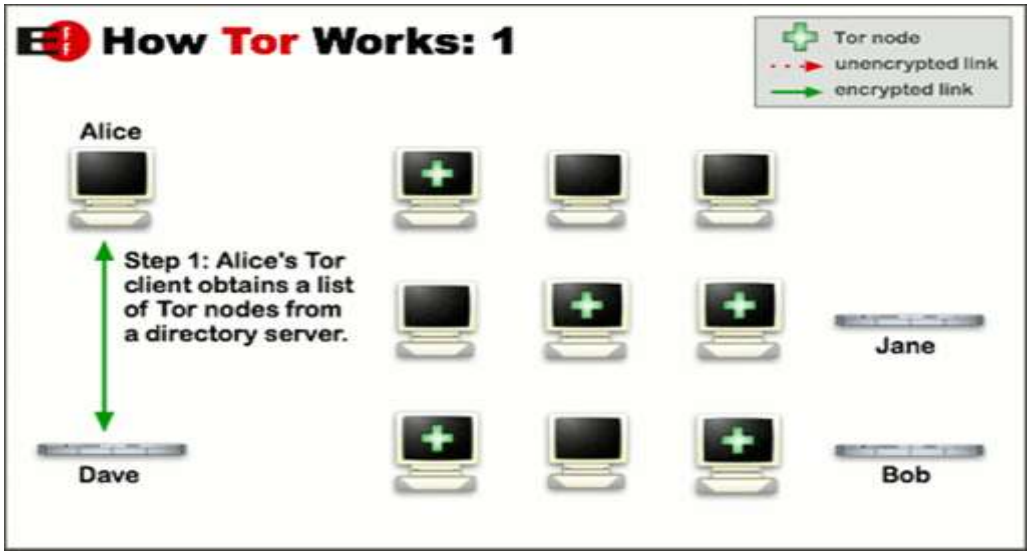


Fig. 4: How TOR Works- Step 1 [36]

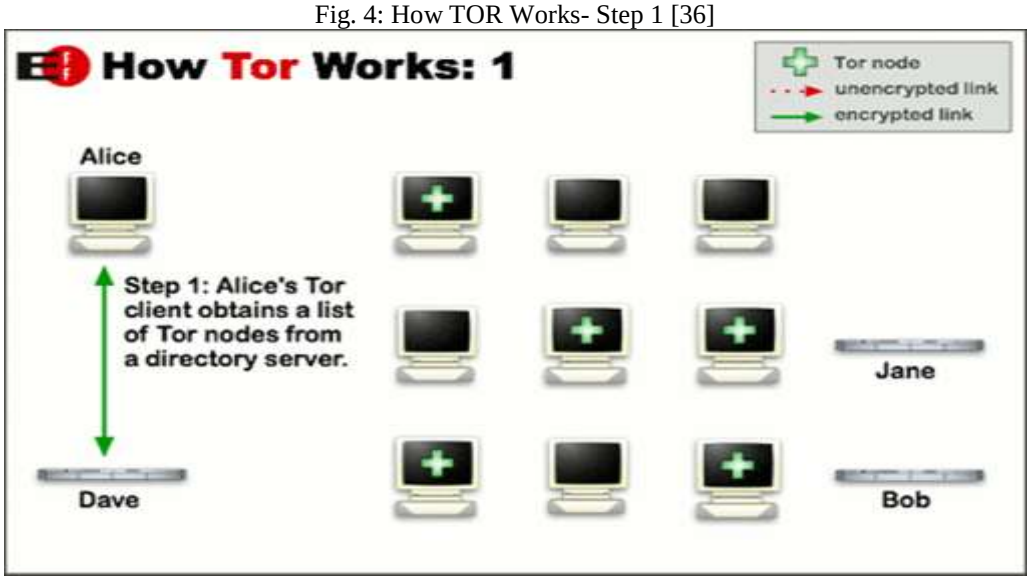


Fig. 5: How TOR Works- Step 2 [36]

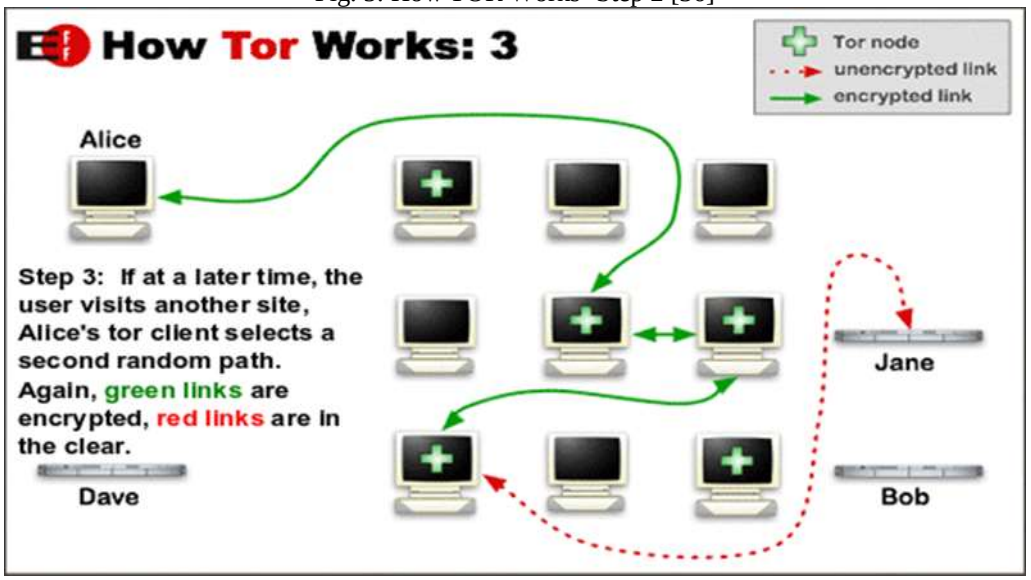


Fig. 6: How TOR Works- Step 3 [36]

Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of

taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going. To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination. Tor only works for TCP streams and can be used by any application with SOCKS support. For efficiency, the Tor software uses the same circuit for connections that happen within the same ten minutes or so. Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones.[36]

Tor is the most sophisticated tool available to the users that protects their privacy and provide a perfect experience for the user. Tor isn't invulnerable and even it falls prey to some specific types of attacks, but the odds of detection of your true identity is approximately 1 in 2 million.[37] This is by far the best tool that can be used to protect our privacy until new laws and policies guarantee our anonymity online.

## VII. CONCLUSION

User's activities are monitored, phone calls wiretapped and location tracked. The state of user's privacy has never been more obscure. Organized cybercrimes are blooming as the laws and policies fail to confine the omnipotent government and spying agencies. We need to redefine what privacy is and upto what extent the interference of tech giants and the government is deemed ethical. The power has always been with those who rebel and initiate a new beginning and it is high time for us to take action. We can either just submit or unite and fight for our privacy, our freedom and bring forth the change necessary.

## REFERENCES

[1] "History Of The Internet". En.wikipedia.org. N.p., 2017. Web. 10 Mar. 2017.
[2] "Internet Used By 3.2 Billion People In 2015 - BBC News". BBC News. N.p., 2015. Web. 10 Mar. 2017.
[3] "Surveillance Under The Patriot Act". American Civil Liberties Union. Web. 10 Mar. 2017.
[4] "Privacy". En.wikipedia.org. N.p., 2017. Web. 10 Mar. 2017.
[5] Solove, Daniel J. (2008). Understanding Privacy. Cambridge, Mass.: Harvard wUniversity Press. ISBN 9780674027725. Pg 15-17,
[6] The quotation is from Alan Westin.Westin, Alan F.; Blom-Cooper, Louis (1970). Privacy and freedom. London: Bodley Head. p. 7. ISBN 978-0370013251.
[7] Posner, Richard A. (1983). The economics of justice (5. print ed.). Cambridge, Mass.: Harvard University Press. p. 271. ISBN 978-0674235267.
[8] Staff (June 6, 2013). "NSA Slides Explain the PRISM Data-Collection Program". The Washington Post. Retrieved June 15, 2013.
[9] Wong, Joon. "Here'S How Often Apple, Google, And Others Handed Over Data When The US Government Asked For It". Quartz. N.p., 2017. Web. 10 Mar. 2017.
[10] "HTTP Cookie". En.wikipedia.org. N.p., 2017. Web. 10 Mar. 2017.
[11] "Snowden Interview Transcript". NDR. n.d. Archived from the original on January 28, 2014. Retrieved 27 January 2014.
[12] Greenwald, Glenn; Casado, Roberto Kaz e José (July 6, 2013). "EUA expandem o aparato de vigilância continuamente – Software de vigilância usa mais de 700 servidores espalhados pelo mundo"
[13] "XKeyscore Presentation from 2008 – Read in Full". The Guardian. Retrieved August 6, 2013.
[14] Jacob Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge (3 July 2014). "NSA targets the privacy-conscious". Panorama. Norddeutscher Rundfunk. Retrieved 4 July 2014.
[15] "NSA: Linux Journal is an "extremist forum" and its readers get flagged for extra surveillance"
[16] "Five Eyes". United States Army Combined Arms Center. Archived from the original on 2 February 2014. Retrieved 18 January 2014.
[17] "Supranational Union". En.wikipedia.org. N.p., 2008. Web. 11 Mar. 2017.
[18] "NSA And GCHQ Attacked Antivirus Software So That They Could Spy On People, Leaks Indicate - Belfasttelegraph.Co.Uk". BelfastTelegraph.co.uk. N.p., 2015. Web. 10 Mar. 2017.
[19] "Sony Pictures Hack". En.wikipedia.org. N.p., 2014. Web. 11 Mar. 2017.
[20] Paul Mutton ,"Half A Million Widely Trusted Websites Vulnerable To Heartbleed Bug | Netcraft". News.netcraft.com. N.p., 2014. Web. 10 Mar. 2017.
[21] http://www.codenomicon.com/, Codenomicon. "Heartbleed Bug". Heartbleed.com. N.p., 2017. Web. 10 Mar. 2017.
[22] Sean Michael Kerner, "Heartbleed SSL Flaw's True Cost Will Take Time To Tally". Eweek.com. N.p., 2017. Web. 10 Mar. 2017.
[23] "Experts Warn Of New Windows Shortcut Flaw — Krebs On Security". Krebsonsecurity.com. N.p., 2017. Web. 10 Mar. 2017.

[24] G. Lilienthal and N. Ahmad, "Cyber-attack as inevitable kinetic war", Computer Law & Security Review, vol. 31, no. 3, pp. 390-400, 2015.
[25] Kelly 2012, p. 1678
[26] Barton Gellman, "The 100 Most Influential People In The World".N.p., Wednesday, Apr. 18, 2012
[27] "Data Breach Costs Will Soar To $2T: Juniper". News.cuna.org. N.p., 2017. Web. 10 Mar. 2017.
[28] Catalin Cimpanu, "Data Breaches Exposed 707 Million Records During 2015"
[29] "Department Of Defense (Dod) Releases Fiscal Year 2017 President'S Budg". U.S. DEPARTMENT OF DEFENSE. N.p., 2017. Web. 10 Mar. 2017.

[30] Reuters,"Department Of Defense (Dod) Releases Fiscal Year 2017 President'S Budg". U.S. DEPARTMENT OF DEFENSE. N.p., 2017. Web. 10 Mar. 2017.
[31] Anderson, Martin. "Cookies Can Facilitate Attacks On Secure Web Sites". The Stack. N.p., 2017. Web. 10 Mar. 2017.
[32] Maura A. van der Linden,"Vulnerability Case Study: Cookie Tampering". Infosectoday.com. N.p., 2017. Web. 10 Mar. 2017.
[33] "HTTP Cookie". En.wikipedia.org. N.p., 2017. Web. 10 Mar. 2017.
[34] The Tor Project, Inc. "Tor Project: FAQ". Torproject.org. N.p., 2017. Web. 10 Mar. 2017.
[35] The Tor Project, Inc. "Tor Project: Overview". Torproject.org. N.p., 2017. Web. 10 Mar. 2017.
[36] Porup, J.M. "Building A New Tor That Can Resist Next-Generation State Surveillance". Ars Technica. N.p., 2017. Web. 10 Mar. 2017.
[37] Yiannis Yiakoumis, Sachin Katti, and Nick McKeown ,Neutral Net Neutrality. 1st ed. Stanford University, 2014. Web. 10 Mar. 2017.
[38] Fuchs, Christian. The Internet & Surveillance - Research Paper Series. 1st ed. 2011. Web. 10 Mar. 2017.
[39] More NSA revelations: backdoors, snooping tools and worldwide reactions", Network Security, vol. 2014, no. 1, pp. 1-20, 2014.
[40] H. Hodson, "NSA's wasted data", New Scientist, vol. 221, no. 2952, p. 5, 2014.
[41] Q. Zheng, Z. Wu, X. Cheng, L. Jiang and J. Liu, "Learning to crawl deep web", Information Systems, vol. 38, no. 6, pp. 801-819, 2013.
[42] F. Aloul, "The Need for Effective Information Security Awareness", Journal of Advances in Information Technology, vol. 3, no. 3, 2012.