Extreme Privacy in the context of South Asian Country
Bangladesh-India-Nepal

ATIQUE SHAHRIER KHANDAKER : 187861, HARI SHARAN GAJMER : 187585, and SAI SAGAR KONDURU RAVI KUMAR : 187862, Offenburg University Of Applied Science

In the 21 century, technology is an integral part of our lives, it plays a huge role in our day-to-day activities. With the use of technology comes the need for data. Data is facts and statistics collected for reference or analysis. By providing an enormous amount of data, we allow others to personally identify us, track us, guess our behavior and interests. Which means that we have lost or given up our right to privacy. In 1967 a new milestone was reached with the publication of Alan Westin's Privacy and Freedom when he defined privacy in terms of self-determination: privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. This report is inspired by the book Extreme Privacy: What it takes to Disappear (Second edition) 2020 by Michael Bazzell. In the book extreme privacy, the author Michael Bazzell has described what privacy is, and what methodologies can be used to achieve Privacy. It describes how a person can perform basic tasks, what information about them can be shared, what kind of technology can be used, and how it can be used concerning privacy. All the scenarios and methods mentioned in the book are with respect to the county USA. There are no documents that throw light on what privacy means and how it can be achieved in South Asian countries. This report is written to better understand what privacy means and how it can be achieved in countries like India, Bangladesh, and Nepal.

CCS Concepts: • **Security and Privacy** → *Anonymity, Pseudonymity* .

ACM Reference Format:

Atique Shahrier Khandaker : 187861, Hari Sharan gajmer : 187585, and Sai Sagar Konduru Ravi Kumar : 187862. 2021. Extreme Privacy in the context of South Asian Country Bangladesh-India-Nepal . *J. ACM* 37, 4 (January 2021), 48 pages. https://doi.org/10.1145/1122445.1122456

Authors' address: Atique Shahrier Khandaker : 187861; Hari Sharan gajmer : 187585; Sai Sagar Konduru Ravi Kumar : 187862, pfernand@stud.hs-offenburg.de, Offenburg University Of Applied Science.

0004-5411/2021/1-ART $15.00
https://doi.org/10.1145/1122445.1122456

Contents

1 INTRODUCTION

Privacy is the ability to sustain some things to yourself, despite their societal consequences. It relates to a person's ability to manage the degree, timing, and conditions of revealing personal information such as physiological, psychological, or intellectual information. Privacy is concerned with individuals, but confidentiality is concerned with data; privacy is a right that may be infringed, whereas confidentiality is a commitment that can be breached. So privacy refers to actions that you keep totally to yourself or a few trusted others. Privacy is not extinct, but it is under assault. We will become easily dominated, manipulated, and sense a lack of control over ourselves and our personal life if we do not have privacy. It provides the ability to pick whom we share our information and data with. It contributes to the protection of our physical safety, as an individual, and as an enterprise, against entities on which we rely or that are more powerful than us. Many companies, technology, campaigners, and others are working hard to enhance and preserve our privacy. We may enhance our privacy in several ways, including not sharing private data online, paying in cash rather than with a credit card, encrypting our email and backups, and reading the conditions before using services. We make use of digital technology extensively. Websites, online purchasing and selling, smartphones, cloud computing, voice interfaces or chat-bots, geo-location, banking and finance, social media, ATMs, and other technologies may leak our personal information. we need to maintain privacy on digital technologies as well as in the real world.

Towards extreme privacy, digital devices have a huge impact on our daily life. These devices make our life too much exposed in the world of digital. We know the digital world consists of digital devices. All these devices have two different periods. Like when the devices were not connected with the whole world, we could say that it was the offline period and after that, we can say it as an online period. When we lived in the 19th century and used only feature phones; their people had only basic features. During this period a person could only get a voice call and SMS. However, we were discoverable by only a less number of people. Today everything is open to everyone, almost every day through the devices and software we use tech companies collect data huge amounts of data. So, avoiding these types of data collection while using a mobile phone is tough. In the book, Extreme Privacy: What It Takes to Disappear by Michael Bazzell; There in chapter two the writer talks about various approaches and techniques related to private mobile device privacy.[1] He mentioned how a person could make himself fully disappear in the context of using private mobile devices. The whole scenario he describes in the background of The United States of America. Here we will discuss the privacy of south Asian countries, Bangladesh, India, and Nepal. South Asia is a continent with a population of about 1.4 billion people, making it one of the world's most populous regions. This alone indicates that major global challenges cannot be resolved without the participation of this area, particularly China, India, and Bangladesh. Technologies have impacted much in our lives in modern society. Nepal as it lies in between two India and China has always been affected by the change in technology and scenario of those major world players, a hardware giant of world China and software hub of India. India is a constitutional republic with a population that is extremely diversified. In addition, Bangladesh, formally the People's Republic of Bangladesh, is a South Asian country with a population of 1.3 billion people, it is the world's ninth most populated country. Therefore, all 3 countries must maintain a high priority on safeguarding the privacy, confidentiality, and security of data. The author Michael Bazzell in his book 'Extreme Privacy: What It takes to Disappear' describes different techniques related to privacy and how he can use these techniques and approaches to disguise himself from the reset of the user in the United States.[1]

In this paper, we will be addressing a few of the factors surrounding privacy in the context of Nepal, Bangladesh, and India. These days, People carelessly publish their personal data and information which they use in their everyday life. We leak our data not only by technology but also due to lack of education like sharing too much information to our trusty person, sharing our information on social networking sites, using our bank cards or credit card for payment, and so on. Despite our mistakes, attackers are always on a hunt to steal our information. A hacker, like any burglar, will select the most vulnerable targets available. Instead of stealing from your house or business with lock picks, they take our personal data from the software. The loss of privacy is the risk. Despite recent improvements, with peace returning to the region after years of conflict, countries like India, Bangladesh, and Nepal still face social and economic challenges, with illiteracy being one of the most important issues in the region. Therefore the result is losing their privacy due to lack of proper information about technologies. In this paper, each person has researched and written his ideas on how to achieve extreme privacy with respect to our countries.

2 PRIVATE MOBILE DEVICES

2.1 Bangladesh

Getting a new cellular phone in Bangladesh is not a tough deal. Most of the manufacturer of cellular devices company does not officially supply or making their sets in here. Only a few of them are doing their business in Bangladesh. So that most of the mobile devices are unofficial and these devices are not registered in the database of BTCL (Bangladesh Telecommunications Company Limited).[2] The security feature of an Apple mobile operating system is way higher than the android mobile operating system. For this reason, if anyone asks for better security services then experts always suggest using apple ones. In Bangladesh Apple has not any official store or dealer. All of the apple cellular devices came here in the luggage of international travelers or in any illegal way. These devices come in here in a different way but it is not illegal to use. Every shopping mall has one floor which is called a mobile floor and there it's easy to buy. Purchasing mobile phones using cash is a common way. After buying a phone one usually need an Apple ID for Apple devices and Gmail account for an Android phone. Initially, anyone can use a phone without ID´s but it is necessary when anyone wants to download any apps on their mobile.

Every mobile needs a SIM(Subscriber Identify Module) and buying a SIM in Bangladesh has some rules.[3] Everyone needs to be registered and for registration, one person needs 1. National Identity Card or Passport 2. Finger Print. These rules are given by the Ministry of Posts, Telecommunications, and Information Technology of the Government of Bangladesh. One person can buy a maximum of fifteen SIM cards in the following way. In Bangladesh, it is very much common to use SIM cards that are registered by others. In every shopping mall, there is some seller who sells this kind of SIM card. It costs more as these cards are registered by others Identification. This SIM card does not require any online activation.[4] The seller of the SIM card can activate it in few seconds. Here four company has the permission to provide network. Among them, Grameenphone has the strongest network connection. The call rate of every service operator is the same and this is a rule which is made by BTCL. So, that providers can only offer various packages of data. People try to keep in mind the data package and network when they need to choose a network operator. In the book of Michael Bazzell, he suggests for privacy "Devices should never be configured from home." Conducting configure process or If anyone wants to do some activation/purchasing any services then ones need to access WIFI. WIFI is almost common in very places in Bangladesh. Most of the WIFI networks are private but in public places, there are several options for WIFI. These open WIFI networks do not require any sign-in or registration.

The cloud services of Apple and Google are widely available in Bangladesh. Using these services for backup data is depreciate by the security experts. Recently a few years back we were faced various data breaches. So, for privacy reasons, it is better to use stock apps other than cloud services. Using cloud services is not a mandatory thing. Backup via USB cable manually is a good option.

Purchasing apps or services from apple stores or the play store is a common thing. Anyone can add their credit/master cards and could buy necessary services. But it is not a safe option to add cards as a payment option. So, the alternative way is to use apple or google payment cards as these are available and quite common for purchasing apps and services.

2.1.1 Secure Messaging: After a new device and new data plan, one mobile phone is fully set. As for extreme privacy, one can try to find an alternative option for communication. Using numbers provided by the cellular company can be traced easily or can find users' information. For this reason, several apps are used to do secure calling.

For secure communication now the top three apps are 1. Signal 2. Wire and 3. Three. Most of the apps need the name, email address, telephone number for signup/registration One can provide fake information to make a profile. Writer Michael Bazzell suggests using the MySudo app because it does not require any kind of personal information to signup/register. It has some unique features like one can create up to nine profiles and every profile has a unique telephone number. With these nine telephone numbers, one can make phone calls, receive calls, and send/receive text messages. It is a matter of sorrow that the MySudo app is not available in Bangladesh. MySudo is the product of Anonyme Labs and they are currently providing service only in seven countries.

2.1.2 Virtual Private Networks: Virtual Private Networks is a necessary thing in Bangladesh. It provides good security and privacy by routing the traffic. This traffic goes through a secure tunnel to the server and encrypts all the data between the device and that server. So that if anyone is monitoring the traffic then it reaches the server will not find useful. For this reason, it is difficult to track location and link the data of my traffic. So this way privacy is afforded. With the use of a VPN, one can maintain one privacy perfectly.

If you live in Bangladesh, you need to be concerned about two different security threats. The main things that one faces every time here are cybercrime and surveillance of government. Cybercrime is a common issue all over the world, but it has become increasingly high in Bangladesh. Bangladesh stood in the 73rd position out of 100 countries in the survey of the National Cyber Security Index which is released in 2018.[5] In recent years the Bangladesh Telecom Regulatory Commission passed a law to monitor internet activity, gather personal information of users, and the most common thing they do is block certain content relating to religion or government. Everyone is at risk for surveillance and privacy because of the broad language used in the laws. These rules also imply to the travelers of other countries. Many features of websites and apps are here is geo-blocking, So that one can face the problem when they try to use the social, music, and streaming video sites they are accustomed to using back home. To handle all of these problems and to make sure your privacy you must have to use VPN in Bangladesh. Here, most of the people used the free trial ones. So that most of the VPN companies do not provide services here. Here I mentioned some of the popular ones[6]:

- NordVPN: is the popular VPN service provider in Bangladesh. This has some good features like fast speeds, 5,500 servers in 59 countries, experience in providing privacy, unblocks geo-restricted content, six devices that can be connected. But it only selects the city location of servers, not specific servers.
- ExpressVPN : provides military-grade encryption standards, fast speeds, and a wide network. The main feature is 3,000 servers in 94 countries including Bangladesh, good encryption,

security, and privacy features, unblocks a large range of geo-restricted content. But it is a little more expensive.

- CyberGhost : has a better reputation in Bangladesh. They have stringent encryption, fast speeds, 5,745 servers in 90 countries including 48 servers in Bangladesh, they have an internal policy of not storing any user data, anti-malware defence, and anti-tracking.
  It only provides full support when we used paid subscription package that will increase security and privacy. Free providers are exempted from the main feature, only have some basic features for the limited time provided in the trial ones. Security expert Michael Bazzell suggests using Proton VPN, Open VPN, IPSec, and IK.Ev2 with its basic option. It offers a very secure environment.

2.1.3 Device Backup and Restoration: As of now, we discussed how should we have a fully configured mobile phone in Bangladesh. Now we need to make a backup for our cellular phone. Device backup and restoration is common privacy issue all over the world. If anyone wants to shift into a new device then it allows them to easily restore. The people of Bangladesh mainly use the basic option which is provided by the operating system. Like I phone users use iTunes on apple computers then connect the device via USB and then simply make backups. Android users do not need any kind of software. They just plug the phone via USB then copy from phone storage and paste it into the personal computer. Some people also use the direct service of various companies. As here most of the people using an android mobile phone and android operating system is used by other company. Like Samsung, Vivo, MI, and many others. All these companies now provide a backup service that can collect all the data from the user and then make a backup into their server. In this system, the main problem is that when any users changed their mobile they must have to buy the same companies phone. Otherwise, they cannot get the data from their old phone. This kind of backup system is a kind of trap by the companies.

There is also some other option like backup data into googles platform. For using this way one just needs to use all the services of Google and give them all the related permission. Then google just sync all the data from mobile phone users.

All these techniques have serious privacy-related issues. If anyone needs privacy then none of the above systems is suitable for them. Experts mainly suggest, to make secure extreme privacy of backup disable all the internet access with the personal computer then connect the cellular phone via USB and send all the data to the machine. This will create a clone copy on the computer.

Having a backup of your mobile device will be a huge benefit if the current mobile phone faces any accident or if need to shift into a second device. As people of Bangladesh has serious lack of knowledge of technology So that most of the people do not make any kind of backup for their mobile phone. If accidentally they lost their mobile they just lost all of their data. On the other hand, if anyone does backups then most people are used iTunes and google backup services. The main matter of sorrow is that none of this provides any privacy and that's why all the data are shifted into the wrong hands.

2.1.4 Secondary Device and Faraday Bag: In most countries, people used secondary devices because of privacy issues. In Bangladesh, most people used secondary device not because of privacy; only try to make the separate phone as personal, public. Here Bangladeshi want to keep separate all of the phone in context of working sector. When people use their phone it is always connected with the nearest network tower and this is how it is easy to know the person's data. So experts suggest keeping separate mobile phones for home and the phone which we used outside. It should not connect with the mobile tower around 5km near your house. Another method is experts suggest is done by the Faraday Bag. Faraday Bag is made of metallic fabric. It is used to block wireless signals, So that when anyone puts their mobile phone into the Faraday Bag. It blocks all the incoming and outgoing signals which can make through the mobile. It helps to make the mobile isolated and for this reason, no one can detect the data of the users. None of these above methods is used in Bangladesh. Here people used secondary mobile only because of their needs. Using secondary mobile concerning privacy is a kind of unexpected thing. Faraday Bag is also here used to cover electronic goods. Using faraday bags because of the protection of mobile devices is not a common thing in Bangladesh.

2.1.5 Camera and Microphone Blocking: Camera and Microphones are necessary options for a mobile phone. We used it in both fun and essential way. In many cases, these modules are used against us. Hackers can simply access these devices in various ways. Many famous companies also doing this thing like in 2019 Facebook was caught secretly enabling the front cameras of the user. Nowadays apps are taking unnecessary permission from the user and this is quite common. All most every social network required permissions to access microphones and cameras. Camera blocks are easy. Just need black electric tape to cover the mobile camera. This one is the same as the laptop camera cover. In Bangladesh people who are concern about their privacy mostly cover their laptop's camera. But cover-up mobiles camera with black electrical tapes is not a common approach

Microphone blocking is not an easy way. There are several microphones in one mobile. When we plugged in a headset the operating system makes the headset microphone default. So that others one is automatically closed down. If anyone has permission to access our microphone then they can easily listen to our conversation with any of the microphones. There are several ways of making the microphone silent. Like if the port of the microphone is 3.5mm then we can plug a broken 3.5 mm jack into the port. So that no one can hear any voice. On the other hand, if the plug is USB-C then they can buy a mic lock port. It's a small tiny piece of an object, nowadays this one is produced by many of the companies. It is a matter of sorrow that these kinds of devices are not available in Bangladesh. The main fact is people are not aware of such privacy concerns. So that in the market this kind of device is almost rare. Also, the people of Bangladesh are not serious about their privacy.

2.1.6 Mobile Device Firewall: The firewall creates a wall between devices with the outsider unauthorized networks/signals. When we turn on our device it tries to connect with several others network connections. Like all most apps and services need data and they do these things behind our back. To reduce this authorized sending data we can make a wall between it. There are several firewall apps in the App store which provide services both on iPhone and Android. It intercepts all local network traffic and provides an option to block any undesired transmissions. We can also find block options in it.

A less amount of people using a Mobile device firewall. There are many options but it is not that much popular. People of Bangladesh are concern about the firewall of the personal computer but when it is the turn in privacy and security in the mobile, they are not interested in it. But few people use Net Guard, Net Patcher, No Root, and Net Blocker Pro.

2.1.7 Pagers: Pager is a small A pager wireless telecommunications device. It mainly receives and displays alphanumeric or voice messages. There are three types of pagers like one type of pagers only sends the message, one can send a call and message and the other one can do both. It is a great thing to use who are concern about privacy thing. Because it will not connect with any signals. It is easy to keep data safe. But nowadays it is not that much available. It is quite tough to get one in Bangladesh. Big companies and chain shops import these devices on their own. In Bangladesh, people used pagers in the sector of restaurants and industry to communicate with the customer or staff. Moreover, we can say that it is used as a beeper in Bangladesh.

2.2 India

Gone are those days where people use fixed landline devices to make calls and communicate. It's the era of mobile smartphone devices, and every Individual in India now has a personal mobile smartphone device and, in some cases, multiple mobile devices per person. The limitation of using a mobile smartphone device is that an enormous amount of data is collected on every mobile device and is transmitted back to the company servers who benefit from your usage.

If a person needs extreme privacy just resetting the currently owned mobile device does not help. Each mobile device has an embedded serial number and while setting up the device, you either need an apple account, google account, or a Microsoft account based on the manufacturer of the mobile device. When the account is used to set up the mobile device the serial number is linked to the account and stored in the database of the manufacturer. So, it is easy to link your accounts and all your hardware where this account is used.Therefore, new devices should be purchased, and we need to ensure that the device is not associated with you while purchasing the device. This can do done by purchasing the device using cash (which is a common way in India) and a store where there is no surveillance or by hiding your identity by wearing a cowboy hat. If you still think this is risky you can ask any of your friends to purchase the device on your behalf who does not care about privacy. After this is done you can create a new (Apple, Microsoft, or Google) account with pseudo name and information which does not link to you and set up the device. Another approach is to buy a used mobile device that is not linked to you. In India it is also common practice to purchase a used mobile device, you have various platforms like eBay, OLX, and Facebook marketplace to purchase used devices. In few parts of India there are flea markets called "Chor Bazaar"[7] (translates to 'Thief market', there is a popular saying "if you lose anything you can buy it back from Chor Bazaar") from where you can buy used or stolen mobile devices, with cash and without providing any personal details in the absence of surveillance. But we never know the ownership history of that device, there might be a case (extremely rare) where the device was previously owned by a "wanted" criminal who is under the radar of the authorities. The agents would have the legal authority to monitor the activities on the device. There are workarounds for such situations in India, right next to the flea markets you have few mobile technicians who can change the serial number or the IMEI (International Mobile Equipment Identity) number of a mobile device in few minutes at the cost of approx. 10EUR and there you have a mobile device that is not linked to you and with a completely new serial number. Once you have obtained the unlinked device, we need to tweak few configuration settings such as disabling cloud services, cloud storage, turning off location services, carefully allow permissions to files, camera, and microphone, calendar, contacts, and gallery.

Now that the mobile device is configured to provide you with the utmost privacy, we need to obtain a SIM (Subscriber Identity Module) card for cellular services. According to TRAI, (Telecom Regulatory Authority of India), to buy a SIM in India we need a national identity card, a photo, and a biometric fingerprint. we can use one of the following identity cards, Aadhaar card (Aadhaar is a 12-digit unique identity number that residents and passport holders of India can obtain voluntarily based on their biometric and demographic data), or Voter ID (The Indian voter ID card is an identity document issued by the Election Commission of India to domiciles of India who have reached the age of 18, which serves as an identity proof for Indian citizens while casting their ballot in the country’s elections), or PAN card (PAN is a unique identification number that enables each tax-paying entity of India with the following: Proof of Identity. Proof of Address. Mandatory for Filing Taxes. Registration of Business). Without this information, one cannot obtain a SIM card legally in India. There are no restrictions on the number of SIMs purchased by an individual. There are several Mobile stores on very main street in India where they sell both mobile devices and SIM cards legally. Once the required personal information is provided at the mobile store a verification call arrives after a couple of days from the service provider. The SIM cardholder needs to verify the personal details that were provided while purchasing the SIM card, only then the SIM and the services are activated. There are illegal ways to obtain a SIM card that are pre-activated. The seller provides his personal information while purchasing the SIM card, activates it, and then sells the SIM card, these SIM cards are usually overpriced since no personal information is a need, and since it is pre-activated it can be used instantly. The major cellular service providers are BSNL, Airtel, Reliance Communications, and Vodafone. Only BSNL is a national service provider, which is owned by the gov of India, the rest are private companies. However, there is no option to legally buy a SIM card anonymously in India without providing any details.

Now that we know how to obtain a SIM without providing personal details let’s discuss how to recharge the SIM cards anonymously to ensure privacy. The common way that most people recharge their SIM cards is through Internet banking, they make use of their credit/ Debit cards to make payments to the service providers, which does not help maintain privacy. There is an approach in India that can be used to recharge SIM cards while also maintaining privacy. We can go to the nearest mobile store pay them in cash and provide our phone number to be recharged and the SIM will be recharged. If we do not want to risk providing the phone number at the mobile store, then we can purchase recharge cards at the mobile stores by paying in cash and then recharge the SIM cards. However, there is only one service provider in India “Vodafone” which allows a user to recharge the SIM cards without providing the phone numbers at the mobile store. To avail of the Vodafone Private Recharge option, a user needs to send a toll-free SMS ‘Private’ to 12604. It provides a 10-digit code to the customer that can be used for subsequent recharges till midnight of the same day. This code needs to be provided at the mobile store.

2.2.1 Secure Messaging: Once we have hands-on a mobile device and a SIM card which is not connected to you, we need to discuss how we can communicate securely, ideally using the services of the cellular provider is not a good option since the companies store the data, they even have access to the contents of the messages. The stored data can be leaked intentionally or accidentally.

In India majority of the population does not care about privacy. As a result of this none of the companies take data protection seriously and there are no companies that offer secure calling and secure messaging services. People make calls using cellular services and make use of WhatsApp features to send messages, share files, and video calls.

Ever since the privacy policy of WhatsApp has been updated recently, there is a rise in the popularity of apps like Signal, Wire, and Threema. Signal requires your phone number to use their services however, Wire and Threema does not need your phone number to use their services. After WhatsApp updated the privacy policy only a handful of people shifted completely to signal.

The number of service providers for secure messaging and calling is quite low in India as users generally do not take privacy seriously. The services of apps like MYSudo which is mentioned by Writer Michael Bazzell in the book Extreme privacy are not available in India.

2.2.2 Virtual Private Network: A virtual private network, or VPN, is an encrypted connection between a device and a network via the Internet. The encrypted connection aids in the secure transmission of sensitive data. It protects against eavesdropping on the traffic and allows the user to work remotely. In India people generally do not use VPN daily, it is used only when a user wants to access any geo-blocked or access censored internet content. VPN is also used while streaming or downloading copyrighted content to protect themselves from government surveillance and avoid fines. There are no laws associated with using VPNs in India. Most people use Free VPN services in India, however, here are some of the paid and best VPN's in India:

- NordVPN- it provides strong security and digital privacy features, as well as a dependable network of servers that can stream and download at high speeds. Apps that are simple to use.
- Surfshark- Best value for money. It has a lot of unblocking power, fast speeds, and a lot of security features. Allows you to simultaneously connect all of your gadgets.
- ExpressVPN- Servers that are quick and have excellent security and privacy features. This is a good alternative, although it isn't the cheapest on the list.
- CyberGhost- Apps that are simple to use are a good choice for beginners. A low-cost service with high security and fast speeds.

2.2.3 Device Backup and Restoration: Backing up and restoring mobile devices is a common procedure mobile users go through quite often. Though it seems simple we need to take precautions while backing up and restoring personal data with keeping privacy in mind. In India, most people use the common approach to back up and restore mobile devices. If the user has an iPhone, they just connect it to the PC and make use of the iTunes application to take a backup of the device. Apples' backup and restore process is quite sound. It can back up even the device's configuration along with the data, This is quite convenient when you purchase a new iPhone, You need not configure it again. You have all the data and the configuration settings that were on your old iPhone on a brand-new device. If the user has an android or windows mobile device, they need no software to back up the data. They can just connect the mobile device to the computer and back up the data, however, there are only a few options to backup the configuration of the mobile device. If android users need to back up the configuration settings as well then, they will have to use brand-specific apps to backup the data and configuration settings. Here are some examples, Samsung has an app called Smart Switch, Sony has an Xperia companion app, OnePlus has a OnePlus Switch app, Xiaomi has a Mi Mover app and so only. But one disadvantage of using these applications is that you will have to use a new mobile device that is of the same brand to restore all the data and the configuration settings. Google offers few back-ups and restores services for android devices however it requires permissions to all files and storage, the data gets backed up to Google servers and is then restored on the new device.

After looking at all the options, it is not suggested to used brand-specific backup applications and google services as these services backup the data on the cloud and even collect some data which is stored and used by the companies. Most users in India use these services as they do not worry much about privacy. However, it is suggested to disconnect the mobile device and the computer from the internet and back up the devices using a USB cable. This is by far the safest option.

2.2.4 Secondary Device and Faraday Bag: With the rise in usage of mobile devices and availability of cheap mobile devices, people in India in recent days use secondary mobile devices. In the book extreme privacy written by Michael Bazzel, it is explained how secondary mobile devices can be used to maintain privacy by disabling the primary mobile device when required so that you are not tracked down to your home location. However, in India, people use secondary devices to separate their private/personal devices from professional/official devices. I have never come across individuals using secondary mobile devices to protect their privacy. Most both the devices are always connected to cellular services, which can be tracked and located easily by any bounty hunter.

In the book Extreme privacy, it is suggested by the writer that the primary mobile device should not be connected to cellular services or the internet within 5km from your residence. It is suggested so to make sure your residence location is not traceable to any bounty tracker or locator. This can be achieved by placing the primary device into a Faraday Bag when you are 5km away from your house at an intersection. Faraday Bags are made of flexible metallic fabric, they are commonly used to prevent remote wiping or tampering of wireless devices confiscated during criminal investigations, they can also be employed by the general public to safeguard against data theft or improve digital privacy. Placing the mobile devices in the Faraday Bags gives the tracker no clue in which direction your house is located at. However, such methods are not used in India.

2.2.5 Camera and Microphone Blocking: Every mobile device has a microphone that is used while making calls, and a camera using which pictures are taken. These are one of the essential components of a mobile device. However, without our knowledge, these components can be used against us. We all know how recorded audio of our conversation and personal images can be used by an adversary against us. Even the thought of it can be terrifying. Malicious software installed unintentionally can enable the microphone and the camera without our knowledge. In the recent past, Facebook was penalized for secretly enabling the microphone and front camera of mobile devices while viewing the feeds in the app. I have also known instances where you talk about some product to any of your friends or family when your phone is around and immediately you tend to see ads related to that product on Facebook, Instagram, and Amazon. So, we need to make sure this issue is taken care of.

You can block your camera on your mobile devices just like you do on your laptops. You can stick black electrical tape on the camera, or you can use phone covers/ protectors that come with a camera blocking mechanism. I would suggest blocking only the front camera, blocking the back/primary camera might be a hassle sometimes as we tend to use it quite often.

Blocking the microphone is a little complicated. A mobile device might have multiple microphones and it is very hard to disable each one of them. The best approach would be to use a wired earphone with an inline microphone. When such an earphone is plugged in the microphones in the mobile device are disabled and only the microphone which is part of the earphone works. So we can make use of this method to disable the mobile device microphones. We can use an earphone with a broken mic (however this approach is not the most conventional) or we can use mic plugs that virtually disables the microphones of the mobile device. There are few options available on amazon which can be easily purchased. However such practices are not quite common in India. Microphone locks and camera covers are not easily available in India.

2.3 Nepal

Before the turn of the century, getting a cellular phone in Nepal was a difficult task. It was outstanding matter in our country, because only a handful of wealthy and privileged people were allowed to get cellular phones and Sim (Subscriber Identity Module) cards in Nepal. For instance, I remember one of my uncles got his SIM card and phone from Nokia around 2004 and we all were ecstatic by seeing a new technology. But within the next 5 years, getting a SIM card and phone was not a big deal in our community as you can get it easily.

Currently getting a SIM card is not hard in our country, the government rule is that you must be over 16 years or above to get a SIM card. Nepalese citizen should have their valid government ID and their fingerprint in the form to get a SIM card from any dealer. There is major two telecommunication in Nepal, one is state-owned Nepal Telecom, and another is NCELL, but other businesses are also coming into the market but mostly from outside the Kathmandu valley. Most of the activation of SIM can be done by the seller and by using a toll-free number but people in cities tend to activate their cell SIM themselves as they have access to their private WIFI. As per Michael Bazzell 'Devices should never be configured from home' as it risks exposing your location.

Nowadays mobile phones have changed how we think and do business. There are almost more than 4 billion people online and governance of these businesses is essential to safeguard our data. As the digital economy was evolving at a rapid rate, the emergence of COVID has increased the use of digital technology and business around the world. Not just digital business has flourished around the world but the e-learning, work from home, and other benefits of digital technology have impacted our lives in such a way that we cannot imagine.

Recently we cannot imagine a life without a single digital product. These products have created a lavish market but there is also a dark side we must take into consideration. In Nepal government has taken this matter seriously and with urgency. A few cybersecurity breaches in the private and governmental institutions of Nepal must threaten the economy and infrastructure of the country. That had let the country pass the 'Individual Privacy Act, 2018' and formulated the 'Information Technology Bill, 2018 to regulate digital security.

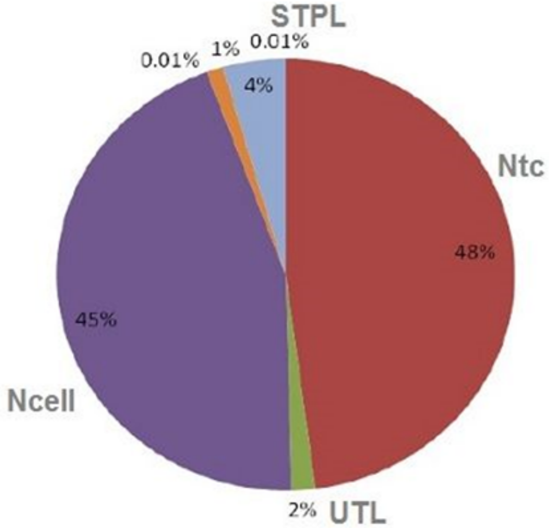


Fig. 1. Telecommunication users in Nepal of the different service provider
[8]

2.3.1 Secure Messaging: In Nepal, Nepal Telecom (NT) and NCELL are the major players in the cell phone industry almost capturing more than 95% of the market shares. When we purchase the pre-paid SIM card, the individual contractor can activate the SIM using the company's portal provided to them and individuals must set up the data plan as per the instruction provided by the company respectively. Then the 4G will be activated for the given user. The SIM card number will be provided by the company itself and users are not allowed to choose the number. This process indicates that all the user information is kept by the companies and that information can be obtained by the authorized personnel to track the user, so it is very hard to remain anonymity.

Michael Bazzel pointed out that there should be three main requirements for secure messaging which include Zero-Knowledge, message expiration, and encrypted voice calling. Xero knowledge means the provider not sharing information with any third party or internal staff as well as information does not intercept anything. Message expiration indicates message automatically remove from the recipient as well as sender after a certain time. Encrypted voice calling includes calls does not intercept by anyone in any form. Michael Bazzell suggested several apps as per his preference. Mainly he uses Wire, Wickr Signal, Session, and MySudo. He prefers Wire over all others as it is free for personal use and has been adopted by many within the community, but it required an email address to create an account and can be communicated on any platform either through text, audio, and video. On the other hand, Wickr is the earliest secure communications app and can be used on desktops only. Another is Signal which has a large user base but needs a phone number to create an account which creates privacy violations. With Session, a random username is created when the session is started without any of your private details and verification. It is new in the service and only text communication is allowed within the network. Finally, with MySudo, any communication channel within its network is possible but it is only available in the Android version and at a certain place only.

2.3.2 Virtual Private Networks: Encryption is necessary because it allows users to access secure data that you don't want others to see or use. Businesses typically use it to safeguard corporate secrets, governments use it to safeguard confidential information, and many individuals use it to safeguard personal data from securing their transactions, conversations, identities, and so on.

VPN is a good solution for privacy, not anonymity. As a South Asian nation, we need to go through the proper channel when we need to do any work. The main concern is cyber crime which is growing at an alarming rate in our country. Due to negligence of the companies, banking sector, and other things, if we need to do any online transaction, the security is not proper, and often cyber criminals will be able to get the information easily as the infrastructure is not secure. With VPN we are responsible for our privacy.

Overview: Best VPNs for Nepal in 2021

- ExpressVPN: 3,000 lightning-fast servers in 94 countries, including Nepal, all with 256-bit encryption and security protocol for unlimited geo-unblocking and the best VPN experience
- Surfshark VPN: It comes with 256-bit encryption, an adblocker of 3,200 servers in 65+ countries.
- NordVPN: is Nepal's fastest VPN, capable of delivering speeds of 80+ Mbps over a 100 Mbps connection. With super-fast speeds, it has over 5,200 servers in 59 countries. 256-bit encryption, Double VPN, Onion Over VPN, obfuscated servers, NordLynx, and are all included.
- CyberGhost: Nepal's Best Torrenting VPN - 7,000+ servers in 91 countries, each designed for torrenting and P2P in its way. It has a kill button, leak protection, and 256-bit encryption, among other features.
- IPVanish: 256-bit encryption, OpenVPN protocol, unlimited bandwidth, Sock5 proxy, and other features are included. There are almost 1,600 servers available in over 75 countries and it even allows for 10 simultaneous connections.[9]

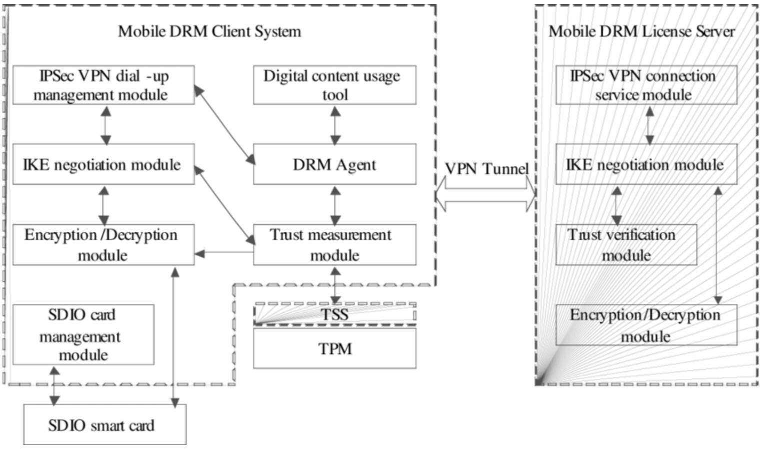

Mobile DRM Client System
IPSec VPN dial -up management module
Digital content usage tool
IKE negotiation module
DRM Agent
Encryption /Decryption module
Trust measurement module
SDIO card management module
TSS
TPM
SDIO smart card
VPN Tunnel
Mobile DRM License Server
IPSec VPN connection service module
IKE negotiation module
Trust verification module
Encryption/Decryption module

Fig. 2. Architecture of trusted authentication enabled mobile DRM based on IPSec VPN [10]

As cybercrimes are growing in our country, the government have become very vigilant and have increased surveillance in private citizen with the help of ISPs as well as upgrading infrastructure in the policing system and setting up new cybercriminal department in the policing system. They have started to gather all the personal information and also have censored various websites and content. The freedoms of speech of the individual personal have been quashed and if we go against the government by writing a post on Facebook or a blog then there is a high chance we are going to get caught. So VPN is very important either for a mobile device or desktop.

As per my understanding, most people use ExpressVPN in Nepal as it has good privacy features. People in Nepal tend to go for free VPN rather than going to the subscription-based services as Nepal's GDP is not that high and it is hard for online payment to work in Nepal.

2.3.3 Secondary Devices and Faraday Bag: In Micheal Bazzell book,who is cyber security expert, he has emphasizes that using only one device at a time is a very risky business as it undermines privacy. When a cellular device is connected to the network, then it will broadcast the location to the nearest tower. It can be tricky as it undermines the privacy of a person by disclosing their location. For this reason, only people tend to use two phones one for personal use and another for work purposes which will be activated only in working time. But that is not a viable solution as sometimes in certain situations work phone should be used in home and it will disclose your location to the tower.

As per Mr. Bazzell, he tends to connect his iPod Touch to his wireless network. As iPod touch uses a unique Apple ID and allows his iPod to connect to his primary device which intent help him connect to the internet and communicate with his secure channel.

In Nepal, people tend to keep a secondary device which is another phone to separate their work phone and personal phone. They are not concerned about privacy or anonymity.

Faraday bags are military-grade isolation bag in a portable and small format which acts as a guard shield for the surveillance of the device with the help of thick copper and plastic and blocks electromagnetic fields. It blocks various signals such as Wi-Fi, Bluetooth, RFID, GPS, and others reaching the devices to prevent you from tracking. People tend to use Faraday Bags to put their cell phones and devices in it so that they can become anonymous, and their privacy will be intact.

In Nepal, I have not learned that people must use Faraday bays because it is not common practice.

2.3.4 Camera and Microphone Blocking: One of the notable features in our mobile phone is the use of a camera and microphone and it is kind of essential thing we need to have in our device. Different means of communication are happening through the use of a camera and microphone. But there is also a very dark side looming through it. In the book, Michael Bazzell pointed out that as recent as 2019 Facebook, one of the popular apps in the world was caught secretly enabling the front camera when going through the feed which was very concerning as it undermines the privacy and anonymity of the person. Not just hackers use the camera but the company apps such as Facebook, Amazon, and others have access to the camera and photos which is the cause of concern. The blocking camera is quite easy and fast. We just need black electrical tape or a dedicated sticker to block the camera. As per Mr. Bazzell, he supports people blocking front-facing cameras at least so that the image of the concerned people won't be reviled. People concern about privacy and anonymity in Nepal tends to block the front camera of their phone and use it when necessary only.

Mobile Phone devices have a couple of microphones in them and are not easily disabled. The disabling microphone is very tricky. Various applications can listen to our conversations if it has permission to access microphones. So it is very important to make microphones close down automatically when it is not in use. Michael Bazzell suggests us few things for securing microphones. One of the easiest and fast ways to block microphones is on 3.5 mm microphones with the help of a broken port of 3.5 mm jack. If we place that broken 3.5 mm jack in Microsoft, then it won't work and our conversation is secured and not recorded by any application. Another is Mic-Lock which various companies offer and is more reliable. It acts as a headset so OS will make the mic a default option and silence the device. In the newer device which uses a USB connection, some companies are offering Mic-Block port for the devices. As per my knowledge, most people do not care about these things in Nepal.

2.3.5 Pagers: Currently in Nepal Pagers do exist, but they are not used by the public. That used to be different when major sources of communication between people in Nepal relied on pagers. I have a little knowledge about it as I have seen my uncles using it. It is a wireless device used for communication between two people either through a text or a voice message. From a privacy point of view, it is one of the security devices as it does not share anything except your communication number.

3 PRIVATE DIGITAL LIFE

3.1 Bangladesh

We already discussed that digital life consists of all the digital equipment. A computer is one of the very important pieces of digital equipment. After the covid-19 situation now, we realized its importance more. For privacy reasons, we always have a huge amount of risk when using the computer. It can disclose a lot of details about users. When a user visits any site it can locate and store the user's location and other data. If your system has lacked security then it is obvious to become a victim to a ransomware attack. This kind of security issue can be avoided, but not with the stock settings provided by the company. One has to make a change to make security stronger. Many times we are intentionally or unintentionally seek and change many configurations to possess true digital privacy. These things are common whole over the world. People of Bangladesh have also done these kinds of things. It is because of the less knowledge of security and privacy concerning digital equipment. If anyone needs private digital life then making computers or laptops secure is an essential thing in Bangladesh.

Buying a computer is not an issue in Bangladesh. In every big city, there are several markets for computer and laptop equipment. The main two famous tech-mall is situated in Dhaka. One is BCS-Computer city and the other one is Multiplan-Computer city center. One can find all the types of computers and laptops here. Most of the people of Bangladesh are comfortable in the use of computers rather than laptops. The main fact behind it is if you have a computer then you can modify it as you want also the price of laptops is high. Here people are not that much aware of security or privacy. The computers part and laptops none of them are manufactured in here. The most pathetic part is that only SAMSUNG and HUAWEI directly doing their business in Bangladesh. The other brands have some importers and they mainly import the accessories of famous brands. The warranty is also given by the local importer companies; you can not get the official warranty from the company. So that importer of these things makes the price as their wish. For this reason, in the terms of quality, these products are not that much good but in the terms of cost, it is expensive. Another important thing is that as I already say that most of the famous companies are not doing direct business here; so people of Bangladesh neve can buy the latest technological things. One must have to wait 6 months to one year for that product and on that time maybe something new would be launched by the companies.

3.1.1 Computer Operating System: After buying a computer or laptop; then the first thing one person need is an operating system. The operating system is one of the major things in aspects of security. There are many operating systems but among the Windows, mac os and Linux is the majority persons used. If you want to install Windows or Mac os then you have to buy it. It is a matter of sorrow that a little number of Bangladeshi people are only used the authorized version of the operating system. On the other hand, Linux is an open-source operating system and also it is the most secured operating system among all. But people here are not interested to use Linux. Every shop installs a cracked or pirated version of the operating system after buying a new computer or laptop. As all of them have fewer headaches about privacy and security

From the book Extreme Privacy: What It Takes to Disappear by Michael Bazzell; we know that his preference of choice is Linux Debian.[1] Here in Bangladesh, one can found a person who uses Linux Debian. Some people are doing studies or work in the field of tech; only those persons are using Linux Debian. But the number of users is few. Installing a Linux machine is an easier process. The Second choice of the book writer is an Apple macOS device. In terms of security apples also collect user's data regularly but they are only using it for their purpose. When an Apple device is connected to the internet apple collects all the information which are provided through the Apple ID account. All their product has a unique serial number. So then they just put all the records in that serial number. This information is stored by them so that apple employees and anyone with the court orders can see the details or if any kind of data breach happens then all the information is gone into public. As much as people use these products the more data can be stored by apple. Moreover, this kind of data is never possible to remove if anyone re installs their device the serial number will remain the same. Mac product users are rare in Bangladesh. As I already said in my previous chapter that Apple has no official shop in Bangladesh. All of these are illegally coming into Bangladesh. In terms of Mac pc and laptops, some of the importers import them the legal way. But the price range is too high that it is tough to use for ordinary people. The most common os you can find in a Bangladeshi peoples computer or laptop is Windows os.

Microsoft also collects similar information like an apple through its various features. It is quite common to see various keyloggers, malicious software, and monitoring applications intentionally installed on their devices by an attacker. This is happening because it is easy to do in windows os. I think most of the people of Bangladesh mainly think about user comfortable rather than security. For this reason, it's obvious to use Windows os. Moreover, when people buy a computer or laptop here they got the pirated or crack version of windows os into it. That's why here people are mostly using Windows os. The writer also refuses to use people the Google Chromebook because with it no one can make use of their private digital life. Google Chromebook is not that much popular in Bangladesh. Only some tech enthusiasts people use it for the experience.

3.1.2 Password Manager: Password is one of the main features in the field of security and privacy. Managing it in a good way can make you secure from many difficulties. If anyone does not manage it appropriately then their personal information can be published into public. There are many cases we can see in Bangladesh which are now happening because of improper password management.[11] Much fake news is spreading and blackmailing with personal things is a common thing. These kinds of the incident are increasing day by day but people are not that much aware of how to make the password more secure. I think the lacking of proper tech knowledge is behind it.

Several free online sites are mainly using to check the breached password. Before setting a password anyone can check it from that site.[12] If anyone makes a breached password then it is quite easy for one to break it. This kind of site not only gives you the information of password also provides information about username and email.

For making a secure password there are many apps and software. All of them are similar in their activity. Using an offline password manager is a good option. Bangladeshi people are not that much interested to use a password manager. On the other hand, it is popular to use a password manager in the government and private office. Because it is secure and with this important files and documents will be kept safe. Here they try to use the paid ones. So the govt and private companies can be risk-free. Using this companies can create new, secure, randomly generated passwords for their email. So that in the future they don't need to remember it, but their password manager will. The only thing officials need to remember is the password of the manager.

3.1.3 Two Factor Authentication: Two-factor authentication or 2FA is a process of authenticating the real user of a service. In Bangladesh, almost all government services use these authenticate processes. Some of the private companies use these services. It is a kind of security check which makes sure the real user is accessing the service. All the banks of Bangladesh use this in the banks, email accounts, social networks, credit card companies, online shopping, and sometimes software applications. The main thing is that when a person logged in to any online service then the service provider sends an OTP or verification link. With this, you can be logged into the service. This link or OTP mainly sends to the mobile phone or email address that is provided for the creation of the service. The above services are given by private or government services but we don't use them in our hardware and software. It is also possible to use these services in our account and hardware devices. The hardware 2FA we called here as hardware token and the software 2FA we called as a software token.

- Hardware Token: It is a small device that plugs into the USB port. When one person wants to log in to a website they have to pass the 2FA. The site will be sending a one-time code to the service. After confirmation, the correct OTP was used, and then it provides access to the service. Without the presence of this physical USB device, no one cannot gain access to the accounts.

- Software Token: Hardware token is best to use but if a service does not support a hardware token, then one can use software-based 2FA. Here the first one has to set up their account. After finishing it whenever a person wants to log in they must have to put OTP. One can use a multi-device with the same account.

In Bangladesh above Hardware token and Software token, both are available. People use mainly software token because it does not require any devices. On the other hand in software token it is free and one can use multi-devices with it. So that it is more comfortable to use and easy to access. If you have an online account on any government website in Bangladesh then every time you log in to your account you have to put the OTP. It is mainly they provide because the security means that no one can use the account of other persons.

3.1.4 Encrypted Storage Backup: It refers to software encryption on a device that automatically converting data on a drive into a form that cannot be understood by anyone. Without the password, no one can understand the format of the file. It is not possible to access without the proper password. This is an extremely important way if anyone has some important files in a device and somehow they lost it then this will help. It is also important to make backup data of the encrypted files. This is a kind of extreme privacy that you cannot see in Bangladesh in the field of ordinary people. However different government and private companies used this kind of way of data storage. All kinds of confidential data are stored in this way. The backup process is pretty much common. The main difference is that people create data backup in Bangladesh but they do backup raw data. So that if their data will be going into the wrong hand then they might face consequences. Making a backup of encrypted data is not a common incident. Maybe this process is followed by the confidential government and private organizations.

3.1.5 Private Web Browser: Internet is an essential thing and for surfing in the world of the internet we need a browser. There are many browsers which are offering various services according to the aspects of security, user experience, comfortable and many other things. The writer of Extreme security recommended using the Firefox web browser.[1] Apple computer has Safari. Windows has Microsoft Edge which has some bad records because of the previous version of it. So people are not that much interested to use the new version of the Windows browser. Firefox is an open-source web browser so it allows users to modify any configuration settings and some of these deal with privacy and security concerns. Firefox respects the concerns of one's privacy and security more than other browsers. Several ad blocker options can be enabled as an extension this might helps one to block many pop-ups and auto-play media. For this, the user of browser make secure and load much faster.

In Bangladesh, people are using also google chrome. This one is much faster and user-friendly. But from the perspective of user security, it is not a good option. Most every possible data is collected by google with their services. If anyone wants to make some privacy it is not possible with google chrome. Here if you try to make an assumption that how many people are using google chrome you will find the above 60% of people using it. People use chrome and Firefox most of the time. There are several ways to make a private web browser in Firefox and the writer of extreme privacy explained all the techniques in his books. If anyone follows all those steps it is easier for one to make his private web browser. It is a matter of sorrow that here the Bangladeshi never think about security and privacy the main thing they are concern about is which is faster and more user-friendly.

3.1.6 Domain Name Service: In Bangladesh, the main ISP business is covered by various companies. The main thing they have to do first they need permission which is given by the Bangladesh Telecommunication Regulatory Commission (BTRC). The BTRC gave them several types of terms and because of it, they have to provide reports about users, user's location, and many other things.[13] As they doing business they have to provide every possible thing when the government asked them. The main works of the DNS are to translates domain names. Like atiqueshahrier.com is website DNS change it into IP addresses. In a normal internet configuration, ISP conducts your DNS queries. SO that ISP knows everything which we do on the internet. As this company is run by the local service provider and they take the bill in the offline system in Bangladesh; So ISP knows who you are and what you are doing on the internet. It is not possible here to do it anonymously. This information's are very much important nowadays various companies using these reports because of the marketing purpose. It can be avoided with some simple tricks and these are given by the writer of the extreme privacy. He recommended changing the DNS with 1.1.1.1 and 1.0.0.1.[1] If you change the number then now you are using the Cloudflare DNS service. I also tried these types of things in Bangladesh but the main problem arises that is the internet speed is going down. That's why people are not changing the DNS in Bangladesh. They sacrifice privacy because of the internet speed.

3.1.7 Email Usage and Other Service: Email is an official or sometimes unofficial way of our communication. All most all the most important works done by email. The Bangladeshi government and private organizations are also ahead in this sector. Many of these organizations using various kinds of email web services. So that they can use their domain name in the email. This looks very professional when you represent your company. Many famous companies also give this kind of service. Like google hosts this kind of service; that is why any company can buy this kind of service and could use all the services of google. The most wanted thing the companies are wanted to use is their domain name. And they also provide that. The most pathetic part is that it gives you all the services and outlook but it never gives you the actual security. If courts order them to hand over all the data of your account then they are obliged to do it. Sometimes data breaches happen at that time all your data will become in the public place. It can make many consequences to a government and private organization.

That's why the writer of the book Extreme privacy suggests using ProtonMail (protonmail.com).[1] This service is free of cost and it provides Switzerland-hosted communications. They have true zero-knowledge data. Because they encrypted an email before sending it from the device. So server got only the encrypted version of the mail. If the court orders them to hand over all the documents then the authority can't give the exact data. They can only provide a bunch of encrypted files. It is only possible whenever mail is sent from a normal mail address to ProtonMail. It will have a very strong password and two-factor authentication system. This service is not that popular in Bangladesh. Most of them are using Gmail because of their services. Another reason is that above 90% of the user use an android mobile phone. A basic requirement for android users is to provide a Gmail id as an account. Previously people used yahoo mail but due to the data breach, only a few people use yahoo services.

Email forwarding is almost a common concept. If anyone has several email account then one can use the services of email forwarding. All the major email service providers gave this feature. It is easy for one to access all the accounts. So that at a time one person can see all their emails. After this allows you to receive the emails being sent to your old accounts. It is not possible to send emails from these old accounts. In Bangladesh people used it for personal usage. Companies are not using this kind of service. ProtonMail also offering an encrypted calendar service. It is also an encrypted, zero-knowledge calendar. We store our daily and future schedule in the calendar and it is a sensitive thing where all our plan one can find. With these details, one can identify anyone's location, medical history many other things. A huge amount of people this kind of services of Google and Microsoft via mobile and computer. ProtonMail uses the same strategy as an email address. I think only a few Bangladeshi people are aware of this kind of feature.

3.1.8 File Sharing: Most of the time we need to send large-size files to another person and at that time mainly used cloud services. Because of with the mail we can send only 25MB and some time if we try to send 25MB files then the mail face some delivery problem. In Bangladesh, people mostly used google drive to send a large number of files. Also, one drive is quite popular. But the main problem is these platforms keep the data for their record. If you delete it then you can find it in the trash bin. After few days they removed it. No one can assure that these data are permanently deleted. The writer of Extreme privacy suggests a service of Firefox Send.[1] This service allows one user to upload a file up to 1GB in size and generates a link to share. The person with the link has only 24 hours to download the file. It is permanently deleted after the first successful download. On the other hand, if no one downloads the file it will automatically delete after 24 hrs. Additionally, data is protected with end-to-end encryption. This feature also prevents Firefox employees or anyone else who has server access to see the files. This Firefox send is not that common in Bangladesh. Mostly google drive and one drive is used by people.

3.2 India

Computers have become a major part of our lives. We use it for educational purposes, for our jobs and entertainment as well. It is the most important equipment in our digital life. Now that Covid has hit our lives, the importance of computers in our lives has increased. An average person spends 8 - 10 hours in front of the computer every day. Computers disclose a lot of information about you, your interests, and your behavior as well which is quite concerning when you take privacy into account. Having a secure computer is one of the most important things in today's world. The security posture of your computer decides whether you will be a victim to an attacker or not. You can be prone to a ransomware attack, or you can be spied on by a criminal. The attack can take place due to various reasons like, using unpatched or vulnerable applications, avoiding malicious sites, and having misconfigured settings on your computer. We can avoid being attacked by intentionally tweaking the default settings on the computers.

The choice of the operating system plays an important role in achieving privacy. In India, people choose an operating system based on some factors like price, intended use of the computer, and compatibility. The preferred OS in India is Windows, 70% of Indians use a windows OS since it is cheaply available and is compatible with their intended use. Users in India are not very familiar with Mac products and devices since they are very expensive and are not affordable by all.

We all know that Windows OS is more vulnerable when compared to most other OS like Linux and Mac. So we can assume the security posture of the users in India. As mentioned, the book Extreme Privacy: What It Takes to Disappear by Michael Bazzell; the preferred choice and safest operating system are Linux Debian which is directly installed on the computer. Users in India do use Linux OS but most of the time it is installed on a virtual machine. Mac products possess much better security when compared to Windows systems since the vulnerabilities on mac devices are less common. Apple collects data from the devices constantly for their use and store them in their servers but does not sell them. It is always suggested to use a brand-new device and configure them securely rather than resetting the previously used devices since the manufacturer already has your information linked to the device on their servers. Since 70% of Indian users use windows let us see

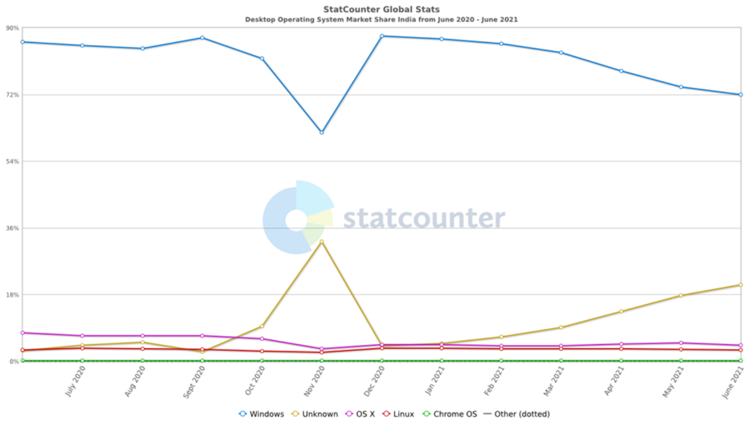


Fig. 3. os market share

how to secure a new Windows computer.

3.2.1 Securing a new Microsoft Windows Computer: Windows 7 is a less invasive OS when compared to Windows 10. However, since Microsoft has stopped support for windows 7 and you no longer receive security updates, we will have to consider using Windows 10 OS.

With Windows 10 you can skip account creation you need not provide your name, email, and home address. A Microsoft account is not required to complete the initial setup and to receive important updates. However, Microsoft's Telemetry service continuously collects Typed text on the keyboard, index of all media files on the computer, browsing history, search history, location details, webcam data, privacy settings across all Microsoft ecosystems, and much more, sending it to their servers in Seattle. Microsoft claims that this data is to enhance user experience however a person can be easily identifiable using the collected data. We will look at few options to disable the data collection. First, we need to set up the new device purchased. While setting it up it gives two options to choose from, "Express settings" or "Custom Settings". You need to choose custom settings so that you have more customizable options for your new system. Here you can disable all the non-essential options like collect keystrokes, location activity. Once this is done the computer will boot to a start-up screen where it requests you to create an account. You can choose to skip this step. Next, it would ask for a username and a password where a generic name can be provided, and a strong password should be set. This should complete the initial boot process and once the system is booted you need to make sure all the system updates are applied.

Once the computer is set up, you need to encrypt the hard drive to protect your data. Windows has a proprietary encryption program called Microsoft Bitlocker which is available for windows 10 pro machines and can be activated in the control panel. Unfortunately, it is not available for the windows 10 home version of the OS. An alternative for the windows Bitlocker is VeraCrypt for full disk encryption. Encrypting the drive provides a huge layer of security. If a person steals your desktop, the content can not be accessed without the password. If the drive is removed and connected to a different machine the data can not be read.

Usually In India using a Bitlocker is only common in Corporate provided machines, a normal user would purchase windows 10 home edition and Bitlocker is not available. A normal user does not encrypt the drives on his machines most of the time.

Every windows computer needs an antivirus, the most preferred one is windows defender which comes preinstalled with every windows computer for free. It is built to protect against attacks especially aimed at windows computers and updates itself from windows updates. It is true that it collects data from the user's computer and sends it back to the company servers, however, it is not too concerning when compared to the default data collection by the windows OS itself. Third-party antivirus is quite an overhead when compared to windows defender, they are memory and process-intensive and they collect a lot of data.

In India, it is quite common to use McAfee and Avast antivirus which comes as a free trial with most Windows PCs. After the free trial ends most of the users do not pay for a subscription, they just use the windows defender. Few users also disable the windows defender when they try to crack paid applications so that they can use it for free. Most of the crack files contain viruses, however, in India users are more concerned about being able to use a paid application for free over the security of the PC and data.

If there is anyone who is very concerned about the data collection by Microsoft from their windows PC's then they must look at a free utility OO ShutUp 10 which helps users to have full control over which functions in Windows 10 they wish to use, and you decide which data is shared to Microsoft. It is a very simple interface that lets you disable unwanted functions. It can be run directly on your PC without installing it.

3.2.2 Password Manager: There are two problems with passwords, the first is using simple passwords which can be cracked easily and the latter is unable to remember a long and complex password. Most users tend to use simple, same passwords or recycled passwords across all the accounts which is a high risk. There is a large number of breached databases available on the internet these days and there are high chances your email and password are in one of the databases. Few websites like "haveibeenpwned.com" offer an option to enter the email or user name and check if the password was exposed in a breach. These breached databases are put for sale and can be purchased by a malicious attacker who can compromise all your accounts.

In India, users tend to use the same passwords across all the accounts, or simple passwords, or basic personal information like phone number, date of birth, vehicle numbers, and so on. With little or no reconnaissance, a user's account can be compromised in India. Most Indians do not tend to use complex and long passwords since they are hard to remember, and they do not use password managers as well. The most common password manager used by users in India is the ones that are available in browsers, which can store the password and autofill them when required to log in.

To achieve extreme privacy and security, it is always suggested to use an offline password manager, specifically KeePassXC as suggested in the book Extreme Privacy: What It Takes to Disappear by Michael Bazzell

KeePassXC is a free, open-source, and cross-platform password manager which securely stores passwords using industry-standard encryption. It does not synchronize the data on the Internet, it stores the database on the hard drive of the fully encrypted PC. It can auto-type the passwords into desktop applications and can also be used to log in to websites by using a browser extension. It provides an option to generate passwords of lengths 40 and 50 as well which is quite complex and hard to crack. It is very important to have a backup of the database created, on an encrypted USB drive Just to be prepared for a data loss. So all you need to remember is one complex password of the password manager to get access to all your other passwords.

For users who prefer the convenience and need to use a cloud-based password manager, Bitwarden is highly recommended.

3.2.3 Two Factor Authentication: 2FA is an authentication method in which a user can get access to a website or application by presenting 2 different pieces of evidence to the authentication mechanism to prove that he/she is the right or legal user. It acts as an extra layer of security. It protects the user from an unknown person trying to gain access to the website or the application on the user's behalf. In cases where a password is compromised, it is highly unlikely that someone has your 2FA information as well.

Likely, you are already using a 2FA. For example, when you try to log in to your bank website, it would ask you for your username and password, which are the basic authentication details. In addition to this information, you might be asked to check your email or SMS for a pin that needs to be provided as 2FA information to authenticate yourself. This pin is called "Token" These Tokens can be hardware, software, or SMS-based.

- Hardware token: It is the oldest form of 2FA, the hardware tokens are small and have a display screen that displays a code and refreshes every 30 seconds. Other types of hardware tokens are USB tokens or USB fingerprint tokens which need to be plugged into the PC for authentication. It is not preferred by many since the hardware tokens come at a cost and are easy to lose because of their size. This type of 2FA is used for high-risk applications. The most preferred one is Yubikey.
- SMS token: This type of 2FA works based on SMS, when username and password are provided on the website, an SMS with the one-time password (OTP) is sent to your registered phone number. This type of 2FA is used for low-risk applications.
- Software Token: It is the most popular form of 2FA, it is available for free and can be installed on multiple platforms like desktop, mobile phones, and wearables, some even work offline. The most common ones are Microsoft and google authenticators and the most preferred one is Authy.

The most common 2FA method used in India is the SMS token method. The majority of the banks and government websites send OTP to user's phone numbers to authenticate them. Hardware tokens are used in corporate offices where high-risk applications are used.

3.2.4 Encrypted Storage Backup: In the above section, we saw how the full disk encryption is done using Windows Bitlocker. In this section, we speak about software encryption for portable drives like USB and external HDD. Software encryption helps in protecting the information in the drive-by by converting the data to an unreadable format. It can not be decrypted by an unauthorized person with a decryption password. This comes in handy when you have important data backed up on your USB drives and you lose your drive. You do not have to worry a lot since the data is unreadable or inaccessible without the password. Backing up important data on an encrypted drive comes in handy when there is a data loss on your PC. You can always be assured that the most important data is always backed up on the encrypted drive.

To create an encrypted drive and backup the following steps needs to be followed. First, we need to select the appropriate backup device and the size of the device. Then we need to use encryption software to create a backup folder in the drive, you can decide the size of the folder. Once everything is set up, we can back up the files into the encrypted folder that is most important to us.

If you think you can get into deep trouble anytime, then it is ideal to have an extreme backup strategy that involves storing an encrypted backup storage device at an offsite location. The offsite location can be a trusted friend's house or a place you visit often. You can back up the utmost important data onto a Micro SD card which has an encrypted folder and place it in a wall socket. This device can be updated when you visit the place where it is stored.

In India, it is quite uncommon to have encrypted storage and backup devices. Generally, people use google drive or other cloud storage solutions to back up their important data. You can hardly find a handful of people who would have encrypted backup devices.

3.2.5 Private Web Browser: Surfing the internet is one of the most common tasks performed on a PC. Before we start surfing the internet, we need to configure a secure browser. Windows has Microsoft edge and Apple has Safari web browsers, however, these browsers collect a lot of data and sends it back to the company servers and there is no option to stop or limit the data collection. Therefore, the preferred web browser is Firefox as suggested in the book Extreme Privacy: What It Takes to Disappear by Michael Bazzell. Installing Firefox is easy, you get on-screen instructions to install it and you can apply default settings while installation.

Once the application is installed and run, we can apply numerous modifications to secure it and limit the data collection. We can turn off "recommended extensions and features as you browse" options so that data is not collected. We can prevent Firefox from opening its sites and services in new tabs. We can change the default search engine from Google to DuckDuckGo. Under privacy and security options we can enable content blocking. We can set the browser to never ask to save passwords, delete cookies, browser history, download history, and site data when the browser is closed. We can limit the permissions for Location, camera, and microphone services. Overall Firefox allows a user to tweak many settings which deal with privacy and security. There are also several browser extensions available for Firefox like uBlock Origine, it blocks several tracking behaviors and security vulnerabilities and is highly customizable.

Another important browser to take into consideration is the Tor Browser. It is open-source software for enabling anonymous communication. It hides a user's location and uses from anyone doing network surveillance or traffic analysis by routing Internet traffic over a free, global volunteer overlay network with over 6,000 relays. Tor's purpose is to safeguard its users' privacy, as well as their freedom and capacity to communicate in confidentially. Using Tor makes it difficult to trace the internet activity to the user. It is free for use and available for Windows, Mac, and Linux.

The majority of users in India use google chrome as their default browser, they only use safari or Microsoft Edge to download google chrome. They store all their passwords in the browser, and they generally do not tweak any settings to avoid data collection.

3.2.6 Email Usage: Today everyone needs an email address, we need it for formal communications, for subscribing to services. Anything you need to buy, sell and use needs an email address today. In India, the most common email service used is either Gmail or Yahoo mail, but the popularity of yahoo mail is disappearing these days. Since there is very little emphasis on privacy and security, almost every email user has a Gmail account since it is easier to set up and there are numerous services available with a Gmail account like google photos, google drive, google contacts, and so on. You can also sign up for several services online with a Gmail account with just a click. Google can track all the emails and even read them if required, when an email is opened, they collect information like the device, IP address, and the location from which it was opened. Therefore, it is suggested to use the ProtonMail email service.

ProtonMail is a free open-source service whose servers are hosted in Switzerland, which means that the data is protected by strict Swiss privacy laws, and they cannot hand over the data of any user even by court order, unlike Gmail. The emails are encrypted end to end, which means even the employees can not decrypt the email and read the content. Even if there is a data breach at ProtonMail the attackers would not be able to look at the contents of the emails since they are encrypted. There is no need to provide personal information for the creation of an email account with Proton. They do not store any IP logs as well, which is a good sign keeping privacy in mind.

A user can create a ProtonMail account and use it as a primary email account going forward, since the user might already have a Gmail or Yahoo account and they receive many important emails and need this account to verify themselves for many services, they need not deactivate it. Instead of opening emails on this account, the user can use email forwarding services which are allowed by all major email providers. So the emails received on the old accounts will be forwarded to the ProtonMail account. The usage of this ProtonMail account can be avoided for newsletters and junk accounts. A separate email service can be used for junk mails and newsletters. An account from Blur (dnt.abine.com) provides an email masking service. It allows you to create numerous random and unique email addresses, any email sent to this address is forwarded to the personal email account. This way the sender does not know your true email address.

Another option for an email masking service is AnonAddy (anonaddy.com). It allows you to create any number of emails using your username. For example, if the user name is privacy techniques, You can create a username-based email address like test@privacytechniques.annonaddy.com, 123@privacytechniques.annonaddy.com, khjkdhskldfj@privacytechniques.annonaddy.com, and so on. Any email sent to this email address will be forwarded to the primary account. It also provides an option to create random emails like asjjkasd@anaonaddy.com. The username-based emails address can be created on the fly, but the random email address needs to be created on their website.

These techniques are very useful in India as there is no governance on the number of spam emails and newsletters sent to an account daily. But most users in India do not use such techniques as privacy is not of utmost importance to them.

3.3 Nepal

In this section, I have presented how private digital life in Nepal has taken an important role. After becoming a federal republic, Nepal has started an economic revolution to promote progress and prosperity. As a result, information technology and communication are in high demand (ICT). ICT has a positive impact on education, health, tourism, employment, finance, agriculture, and environmental protection and promotion. The federal government and the private sector have yet to institutionalize and leverage the immense benefits of digital technology, such as the competitive edge it provides in terms of long-term growth, objectivity and better governance, and responsive service delivery.

Digital transformation: Policymakers and planners must keep up with the global digital transition to eliminate information poverty. Policy planning and management, a lack of information and a robust database, disconnected enterprises, inefficient marketplaces, inadequate service delivery, disempowerment, and corruption have all been problems in Nepal. Digital transformation involves the involvement of a diverse set of stakeholders to meet certain socio-economic goals. The ICT revolution has been disregarded in Nepal's development thinking in the past due to a lack of vision. Only 21% of Nepal's total population has access to the internet. [14]

The rapid adoption of the internet and mobile wireless communications is a crucial trend influencing Nepal's digital transformation 14. As a result, the "National Information and Communication Technology Policy, 2015" 15 ("ICP") has been a major policy initiative. Emphasizing the importance of maximizing IT's economic and revolutionary potential.

Nepal passed the Privacy Act in September 2018. The Privacy Act, which implemented the fundamental right to privacy 18, has had a considerable impact on the legal use of "personal information."[15]

I have presented how different kinds of digital equipment and infrastructure are used in Nepal and how can we make their privacy while using.

3.3.1 New Hardware (Apple): Apple is the most dominating technology in the world today, despite fierce competition among all products, the Apple is the most popular and reliable device among all people, especially in Nepal and around the world. Apple products are being stood against other brands, such as all Android and giant companies like Samsung and others, it is still the most favorite phone for smartphones users. Apple is well known for its smooth design, user-friendly, high-speed browsing, and available in all the major countries in the world including Nepal. Some several other features and advantages make the iPhone a must-love smartphone globally.

Apple goods are available in Nepal through authorized distributors or grey markets. Purchasing Apple products from authorized dealers ensures that you are getting authentic products, but they are high priced. Similarly, buying on the black market is less expensive, but you risk getting non-genuine or refurbished goods. Even though the first iPhone was released in 2007, it took a long time for Nepal to get its hands on the much-anticipated smartphone. Nepal's authorized Apple product distributor is Generation Next Communications Pvt. Ltd, who was the first to bring in Nepal's local market. However, Apple iPhone sales in Nepal were hampered by high costs. Many people were unable to purchase iPhones due to financial constraints. In Nepal, the mac book is often used by senior officers, companies' bosses, and rich people.[16] On the other hand, the Apple smartphone is mainly used by teens and those who are Apple product lovers. Every digital product including apples needs to make secure to maintain privacy. To achieve extreme privacy, it should be protected by malicious online attacks however it has less than Microsoft products. Most of the Apple users in Nepal are related to a non-technical person rather than a technical. Therefore, in my opinion, the following is a mandatory list of configurations and modifications when issuing a new Apple product to the client.

3.3.1.1 FaceTime in iPhone:

FaceTime, which uses the phone's front-facing camera to enable high-definition video calls with other iPhone users, is a major utility specific to the iPhone and other Apple products. Many apple users in Nepal believe that the apple product is much safer than any others. As we all believe that Apple does not store our FaceTime and Group FaceTime calls on their servers. And during transit, these calls are protected with end-to-end encryption. But back at the beginning of 'A bug in Group FaceTime made it possible for a hacker to discreetly spy and listen in on you in 2019. A user may set up a group FaceTime call that allowed them to see and hear a receiver without them answering the call because of the issue.[17] Before you make a FaceTime call, I suggest to every Apple user must do the following:

- Make sure you are connected to a secure network. Free Wi-Fi in hotels, restaurants, and airports should be avoided; even if the business providing the Wi-Fi is legitimate, someone in the region could be advertising an insecure network. Even if that were the case, the call would be encrypted, making it impossible for them to listen in.
- Make sure the person you are calling is someone you can trust. They could record or picture the call and exploit the information for harmful purposes.
- Keep your phone up to date.

3.3.1.2 Mac OS Security and Privacy:

We know that macOS is more secure than other operating systems and that it has its security and privacy preferences. There is no need to install third-party antivirus software because it comes with its own Mac cleaner. Managing the information Mac makes available to others through the internet utilizing the privacy plane of security and privacy preferences. There are several uses for privacy preferences in security and privacy settings. To update your privacy settings on a Mac, go to the Apple menu, select System Preferences, then Security Privacy, and finally Privacy. Location Services, Contacts, Calendars, Reminders, Photos, Cameras, Microphones, Accessibility, and more features are available in Privacy. We can modify all these features to make it secure or private on macOS. Along with Privacy, there are FileVault and Firewall choices. FileVault secures the data on your disk by encrypting its contents automatically. When Firewall is enabled, it blocks all incoming connections except for those required for basic Internet services, such as DHCP and IPSec.[18]

3.3.2 Two Factor Authentication: It's a two-step authentication security technique that requires users to provide two different authentication elements to verify their identity. We have been using some type of 2FA without even realizing it. When we log in to a secure site, they ask us to check our email/phone number for an OTP code that is 2FA. It is essential to utilize 2FA in every web-based enterprise. 2FA is used in Nepal by enterprises, banks, credit cards, digital wallets, social networks, email accounts, software applications, and a variety of other web industries. 2FA sends OTP codes to their internal computer system via text messages or email and it improves security sustainability. Hardware tokens, software tokens, and SMS tokens are the three forms of 2FA. The most prevalent form of authentication is SMS tokens in Nepal.

SMS Token: SMS as a method of 2FA is commonly used because it works for almost everyone. People in Nepal had mobile phones and could receive texts; thus, the SMS token was quite beneficial. It's easy to implement and can be done on a large scale, and it doesn't require anything more than a working SIM card in the phone. SMS authentication may be set up using a variety of tried-and-true platforms for companies.

Sensing messages provided an additional layer of protection and a simple solution for banks and other businesses to encrypt critical data. We were a part of it, and we received a one-time PIN or password message, which we had to input into a site or app to complete the operation. In Nepal, an online payment software named Khalti Digital Wallet is using SMS tokens as an example of 2FA. To verify identification, the app generates a random OTP and sends it to the registered phone numbers and email addresses. The OTP is used in the Khalti App to sign up, reset passwords, load funds, and make online payments.[19]

3.3.3 New Hardware : Windows and Linux: Microsoft is well-known computer software, consumer electronics, personal computer, and related service provider. Microsoft's Windows operating system, Office suite, and Internet Explorer, and Edge web browsers are top software products in the world. Besides IT industries Microsoft helps Nepal with different public services like earthquake relief, poverty relief funds, education in remote areas, etc. According to Operating System Market Share in Nepal. - June 2021, the android user is 69.97%, Windows 19.57%, iOS 6.78%, Unknown 1.75%, OS X 1.35% and Linux 0.46%.[20]

Most enterprise and small organizations have been used MS products, during my past work experience my employer was using Microsoft products. Therefore, it is requiring maintaining privacy and security option in any version of Windows. During my work experience in Nepal, I have been also facing several issues and problems while using Microsoft Windows. As an IT person, I must support either an individual or team and is vital for the smooth running of a business. Mostly in a corporate office, the active version of Microsoft is installed therefore, any official download and updates are easily available. In Nepal there is not any strict cyber law therefore people can easily download any illegal product keys and crack.

Most enterprise and small organizations have been used MS products, during my past work experience my employer was using Microsoft products. Therefore, it is requiring maintaining privacy and security option in any version of Windows. During my work experience in Nepal, I have been also facing several issues and problems while using Microsoft Windows. . As an IT affiliated person, I must support either an individual or team and is vital for the smooth running of a business. Mostly in a corporate office, the active version of Microsoft is installed therefore, any official download and updates are easily available. In Nepal there is not any strict cyber law therefore people can easily download any illegal product keys and crack.

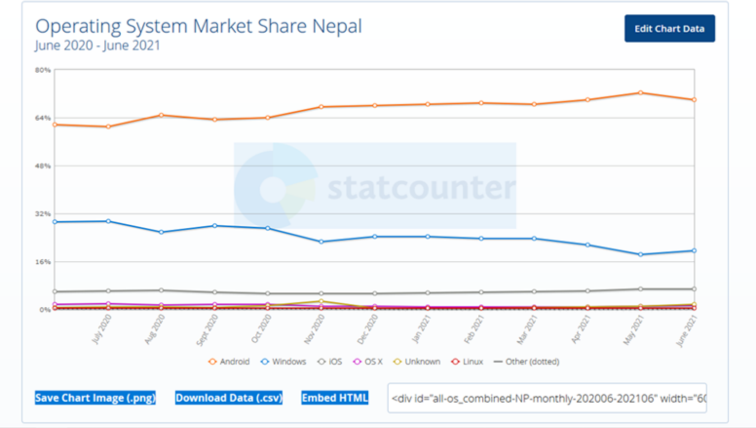


Fig. 4. Operating System used in Nepal
[21]

As I have already mentioned, In Nepal, Windows OS is more common and user-friendly than the other operating system. Third-party software is commonly installed by Nepalese individuals, putting their privacy at risk. Microsoft is working to protect the privacy of users and organizations. Control, Transparency, Security, Strong legal protection, No content-based targeting, and Benefits to you are the six major privacy principles they applied. These are the fundamental ideas that underpin Microsoft's commitment to user privacy. For their privacy, users may change Browser data, Search history, Location data, and Edit Cortana's Notebook in Microsoft Privacy Settings.

Microsoft computers are readily compromised, and attackers can get complete access to them. Microsoft Defender, as well as a firewall and network protection, are included in Windows for security purposes. Firewall and network protection allow us to examine the condition of Microsoft Defender as well as the network to which the device is connected. Furthermore, we may use the firewall to accept or ban apps to safeguard our privacy from third-party apps. In addition to boosting Microsoft's security, we may install alternative trusted antivirus software such as AVG antivirus, Bitdefender, Kaspersky, and others. In Nepal, the majority of individuals use Kaspersky antivirus to protect their data from intruders.

Linux, a kernel or operating system published under an open-source license whose features set is very similar to that of UNIX. The kernel is a program at the foundation of the Linux operating system that handles basic tasks such as allowing hardware and software to connect. In Nepal, most of the offices small and big companies used Linux as their system servers. When I was employed with different companies i.e Worldlink Communications Pvt, ltd, Yetiairlines Domestic Pvt. Ltd, both companies were using Linux as the servers because of their high security and data privacy. Attackers cant easily infect the system however, we must have to be well familiar to use Linux and its kernel.

As I discussed, most home users used Windows than Linux, If the user is well known of Linux then they are using Linux as personal in the context of Nepal. In Nepal, most business companies are using Linux rather than the Government sector.

While installation, we have a variety of version options, including Linux, Debian, Ubuntu, and others. Debian is an older operating system than Ubuntu, while Ubuntu is a newer operating system that is based on Debian; both are being developed. Under Linux, all programs and systems are controlled by a set of commands that are input into a terminal. In general, the terminal is the most often used tool in Linux. Like installing, removing, and upgrading tools, location, copying, pasting, and creating files, and all other activities are done on Terminal.

3.3.4 Password Vulnerabilities. Nepal is in the developing phases of digitization, and increased internet access has resulted in more people abusing social networking sites, leading to an increase in cybercrime. There have been numerous incidents of celebrities' social media accounts and ATM passwords being hacked in recent years. In the year 2020, a 14-years-old boy hacked a movie star's Facebook account and demanded money by texting their Facebook pals. 'Deepashree Niraula' and Saroj Khanal, are the famous persons who were victims. They filed a report with the Nepal Police Cyber Crime Bureau after knowing that hackers had accessed their account and sought money from mutual friends via Facebook. It occurs as a result of insecure passwords being used in social media accounts. Such as using their name, birth date, phone number, and just using single small letter words, and so on. Because these are weak passwords, attackers can quickly crack them using Kali Linux tools. In addition, using the social engineering toolkit in Kali Linux, the attacker creates phishing pages for social media sites and then sends links to victims. The attacker obtains the victims' ids and passwords after they enter them in false pages. To thwart such attacks, Nepalese people began to employ strong passwords that included capital and small letters, digits, and symbols. People began to use VPNs in public places and avoid unsafe phishing sites.

Another example is the hacking of a Nepalese ATM booth. Using electronic devices and their computers, a group of Chinese people hacked a bank cash machine from several ATMs in Kathmandu. When the manager discovered unusual activity in the bank accounts, he reported it to the Nepal police. They detained a Chinese group, confiscated their passports, electronic equipment, and computers, and recovered more than 12 million rupees. To dismantle ATMs Hackers utilized master keys to open machines and also cracked ATM security systems utilizing electronic devices and computers. Because most ATMs were borrowed from China and installed by the Chinese, as well as the usage of outdated security systems in Nepal. Nepal should deploy modern and sophisticated security measures to prevent such assaults, as well as appoint cybersecurity professionals.[22]

They are vulnerable, even utilizing strong passwords and current security technologies (SSL, TSL). On several websites, the majority of people used similar passwords. As a result, a data breach at one site could provide the attacker access to all accounts. To avoid password leaks, we must use strong and unique passwords across several sites. The solution is to use a password manager.

3.3.5 Password Manager: It is computer software that produces, stores, and manages the passwords for users' applications and services. It aids in the retrieval and generation of complex passwords, as well as their storage in an encrypted database or execution on demand. In Nepal, there are a variety of password managers available, including web-browser-based (such as Chrome and Mozilla's password manager), cloud-based, desktop, and portable. And the examples are KeePass, 1Password, Dashlane, Enpass, and so on.[23]

3.3.6 Email Usage . Email (electronic mail) refers to the electronic exchange of computer-stored information via telecommunication. Typically, messages are encoded in ASCII text. ASCII is an acronym that stands for American Standard Code for Information Interchange. Almost everyone in Nepal enjoys using it, and it is becoming increasingly popular. It is now one of the first activities performed on the internet. It is a quick technique of exchanging messages that saves time and money. Earlier, firms in Nepal solely used email. It was not used for personal purposes at the time. With time, email has become widely used for personal reasons by all users, because the majority of them own electronic devices capable of exchanging messages.

We are all aware that email is sent through the internet. Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), and Internet Access Message Protocol (IMAP) are servers that are utilized amongst clients to successfully transmit and receive messages. SMTP Server handles message transmission and is utilized by the sender. Imap is in charge of maintaining and retrieving messages from the receiving server and it syncs messages across all devices. POP3 is similarly used to receive emails, but it downloads messages from the server to a single device before deleting them from the server.[24]

3.3.7 Private Web Browser Configuration: Before accessing the internet and connecting to several browsers to secure accounts, you need to first configure a secure web browser. Web browsers are the most frequently utilized portal for end-users to access the internet. Safari, Mozilla Firefox, Google Chrome, Microsoft Edge, and more other browsers are used in Nepal. In macOS, Windows, and Linux, Safari, Microsoft Edge, and Mozilla Firefox come preloaded, accordingly. Google Chrome, Opera, and other third-party browsers should be required to be installed. Furthermore, preloaded and installed browsers are not configured securely, necessitating the necessity for us to safeguard our browsers. Safari: We know that Mac is secure than windows and is known for security and privacy. Safari browser also offers security and privacy settings. To configure, launch Safari and make the following changes.

- Select Safari from menu options.
- Choose Preferences… option and a popup window will appear.
- Click on the Security tab
- Enable Fraudulent sites to improve security.
- For Privacy, click on the Privacy tab.
- Enable Website tracking and web advertising to prevent cross-site tracking and allow privacy-preserving measurement of ad effectiveness.

Google Chrome: It is presently the most widely used browser in Nepal. First, launch Chrome and make the modifications.

Mozilla Firefox: I like the Firefox browser since it is more secure than others and has more functions. It is the default browser in Kali Linux. For configuration, launch Firefox and make modifications for your privacy and security.

- Click on the Customize and control icon on the upper right side.
- Select Preferences in the drop-down menu that appears.[25]

3.3.8 Tor Browser: Onion routing is a method of communicating anonymously over a computer network. Messages are encased in layers of encryption, like the layers of an onion, in an onion network. The encrypted data is sent across a network of onion routers, which "peel" away from a single layer to reveal the data's next destination. According to a survey, roughly 500 connections to Tor are made each day from Nepal. Tor is a free program that allows anonymous communication and gives users access to the dark web, which is a collection of hidden content on the internet.[26] Tor makes it more difficult to track down a user's online behavior, which includes "visits to Web sites, online posts, instant chats, and other types of communication." Tor's purpose is to safeguard its users' privacy, as well as their freedom and capacity to communicate in confidence, by preventing their Internet activity from being monitored. My previous work experience includes working as a Network Engineer at one of Nepal's leading ISPs, Worldlink Communication PVT.ltd, where my responsibilities included checking daily network status and bandwidth monitoring, as well as all network-related tasks. Our network monitoring system could only show bandwidth utilization, but we had no idea what the actual source and sites were if it was Tor beside any other websites. And therefore, our assumptions were always the dark web like the Onion routing.

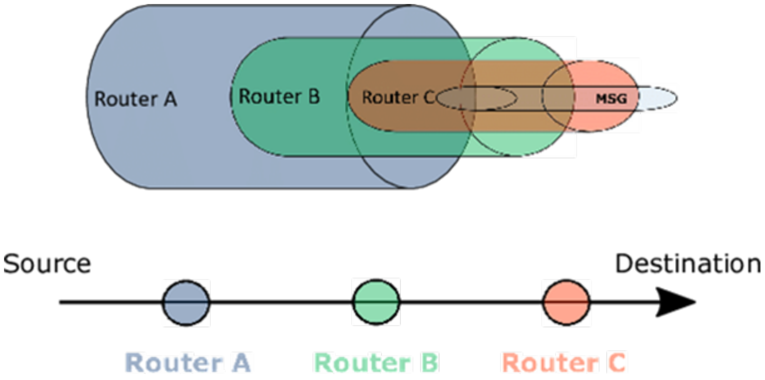


Fig. 5. Onion routing layers
[27]

I have heard nowadays some ISPs have blocked the Tor network in Nepal. To make confirm I called two different persons, one from ISP where I worked before, and another was internet user. As I am a former employee, I easily could get contact the senior network administrator and another person was the user of that ISP. According to my former colleague, the Nepal Telecommunication Authority (NTA) is responsible to make laws and policies of the internet in Nepal. Nepal's telecommunications regulator is the Nepal Telecommunications Authority. It is a self-governing body that was founded in February 1998 under the Telecommunications Act of 1997 and the Telecommunications Regulation of 1998. But now all the network from any Tor and any dark web has been opened and there is not any restriction for any dark web. Because some user and diplomatic person really need privacy and anonymity.

Since most criminal activities in Nepal are carried out using onion routing, a drug market is another part of the dark web where Nepalis may be found in plenty. Drugs such as hash, opium, and charas are claimed to originate from Nepal, yet they are discovered to be shipped from other nations. And another example is the most undesirable portions of the dark web where Nepali presence was commonly noted, according to the ThreatNix official site, were child pornography forums. Nepal has recently been a hotspot for pedophiles from all over the world, with two foreign people detained and charged with pedophilia just last year.

Tor is the most secure for blocking trackers, defend against surveillance resist fingerprint, multi-layered encryption in Nepal also. According to my research, many people don't have a good idea

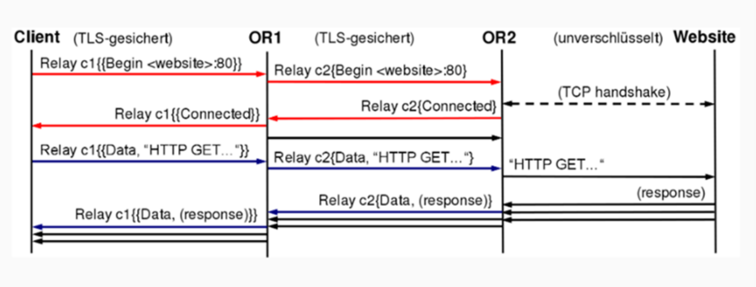

Client
(TLS-gesichert)
OR1
(TLS-gesichert)
OR2
(unverschlüsselt)
Website
Relay c1{{Begin <website>:80}}
Relay c2{Begin <website>:80}
(TCP handshake)
Relay c1{{Connected}}
Relay c2{Connected}
Relay c1{{Data, "HTTP GET..."}}
Relay c2{Data, "HTTP GET..."}
"HTTP GET..."
(response)
Relay c2{Data, (response)}
Relay c1{{Data, (response)}}

Fig. 6. The Onion routing data transmission and digital mixing

about Onion routing in Nepal. But many technical people are aware of Tor and its uses. Therefore, not only in Nepal Tor can be very useful for message encryption and privacy. By using Tor there are lots of users to become anonymous if you have to make your data and message privately. As Michael Bazell also recommended Tor can be the main option to make extreme privacy during the following scenarios.[18]

- International Travel: If you travel in Nepal and if you feel VPN is blocked and normal connectivity is not secure. For this instance, Tor will bypass all the restrictions easily and the message can easily bypass the network protocol.
- Hotel and Guesthouse: In Nepal, if you are using free wi-fi in hotels or guest houses or any available zones I suggest you not use any secure communication. Because there are many cases of leaking data privacy via the free network. In case of any urgent matter, I suggest to every user to use Tor.
- Social sites and Networks: There is some evidence in Nepal that some famous politicians and celebrities' social media get hacked. Our former Prime Minister Mr. Sushil Koirala Twitter was hacked. Every social network user can make data privacy by using the Tor network.

3.3.9 Traveling with Devices: Nepal is one of the tourist destination countries in the world where visitors can make holidays adventure and make it memorable. We all have our technological gadgets and goods with us at the same time. While traveling to Nepal, it may come across a border security officer and be required to provide them access to private and confidential data. Sometimes they attempt to gain access to a device, so we should prepare ourselves for an unpleasant meeting. Some of the confidential data must not be seen by the authority also though it is required to access. I feel that disclosing your personal information to a third party is inappropriate. As a result, we must plan ahead of time for this possibility to prevent the temptation to give our data to research.

3.3.10 Domestic Travel (Land and Air): The Popular mean of transportation in Nepal are bikes and public vehicles. Besides, people are using private vehicles. But if you are a tourist you can hire rental cars and bikes also, Although the Nepalese constitution states that traffic officers have no power to inspect our devices, officers frequently seize control of our devices and extract our data from them. Therefore, we must encrypt and back up all of our data. If you are caught commenting on a crime, you will lose your right to privacy, and if a search order is granted for your device, your data will be extracted. Also, when you fly, there is a scanner that can show authorities what you are carrying, and if an officer notices anything suspicious about you, they will take you and your gadget into custody to be examined.

Currently, Apple and Android smartphones are more focused on encrypting user data to provide maximum security. They have developed a fingerprint, face-unlock, and PIN-based unlock system. If the operating system's security mechanism is highly secure, the PIN-based unlock system is more secure than the other two. Otherwise, officers can force you to give up your biometrics and simply access your gadgets using facial recognition. As a result, I prefer to utilize a PIN-based unlocking mechanism to safeguard my data.

4 PRIVATE TEMPORARY HOUSING

4.1 Bangladesh

In the above two sections, we discussed Private mobile devices and Private Digital Life in context of the Bangladesh. Now we know everything about electronic devices. But with these things, one cannot make sure of their privacy. Private Temporary Housing is another important part if anyone wants to concern about their anonymity and privacy. Here in this chapter, I discussed the whole scenario of making a temporary private home anonymously.

If we talk about temporary housing or short time housing then we can think about the hotels and resorts. On the other hand, if we talk about living in any place for a long time then it can be rental homes. So here we discussed all of these into two sections.

4.1.1 Short Term Housing: Short terms housing means a place where a person thinks about living for only for few days. In Bangladesh, it is possible only in hotels and resorts. For these hotels and resorts, it is good to make a reservation because sometimes it is tough to get one. In Bangladesh, there are two ways you can reserve short-term housing. The number one option is with money and another one is without money. Most of the hotels and resorts don't have an online reservation system. So people make a reservation by phone call and if they require money then you can send money by some popular mobile banking system. On every road, one could find a mobile banking agent. With their help, you can send money for the reservation. Using an anonymous name is possible because you don't have to provide any kind of identification proof. Without any big hotels, all of them collect information by pen and paper. This process is kind of common here they write down the information which you will tell. There will not be any crosscheck and any other thing. They put all these into their register book.

Some of the booking websites nowadays making some deals with the hotels and resorts and there you can get some good deal. But they need all your information and also it is not possible to book with a mobile banking system. These booking sites need a credit card. So it is good to avoid online booking sites. Some of the booking sites don't need any pre-booking money. Like if anyone booked a hotel by booking.com they don't need to register for booking. Also here one can find the various option where one person doesn't have to pay first. Here for booking, you have to provide your name and mail address. These two things one can provide fake ones as there will not be any checks. The famous way of booking in Bangladesh is; collect the phone number from google then call them to make a reservation with fake details and if they require booking money send the money with local mobile banking agent. On the other hand, if anyone wants to live in the big hotels then they can't make a reservation with correct information. So if anyone wants to make their privacy then it is better to avoid big hotels. Then they can use the option of resorts. Resorts are not located inside the middle of the city. All of them are outside of the main city but one can get all the facilities of big hotels. Resorts are also don't ask for documents; one person can book without details. If anyone thinks about also the safety issues then it is better to stay in the resorts rather than small hotels. All of these resorts are private property so that they have their security persons. Using fake names is normal in Bangladesh as it is not a fraud case.

There is some check-in technique we can see in other countries. Like self-check-in service or digital key. In the self-check-in, you can get all the info about your room and book through their app and you just have to collect keys from the reception. On the other hand, if any hotel offers you digital key services you can use the key directly to unlock your room. The matter of sorrow is that none of the hotels in Bangladesh offer these kinds of services. Here you found the old techniques. In Bangladesh, one can found all the international chain hotels. It is possible to avail of all the offers. The most popular hotels of international chains are Marriott International, Sheraton, Le Meridien, Radisson, Westin, Novotel, and Hilton.[28]

"According to Bangladesh Parjatan Corporation (BPC) officials, roughly 500,000 foreigners arrived in Bangladesh in 2012 with above 80% of them on business and official tours and the remaining as tourists."[29]

There is another option one can find in the whole world its name is Airbnb. It is also an easy and comfortable way for a temporary stay. Anyone can register on this platform with fake names, mail addresses, and telephone numbers. Then they have to select the period and the provider can give you the keys directly or they can keep it somewhere and you just have to collect it. In many cases, one doesn't have to collect the keys from the owner. One person can collect the information and contact the owner directly without the platform. Another famous way to book hotels in Bangladesh is by the agency. There are various famous agencies or online sites that can book hotels and resorts for one person. There one person doesn't have to give any kind of information. The process is to call the agency and they will book the hotels and resorts for you here you just have to share which kind of temporary place you want. The booking will be confirmed after sending the money through mobile banking. Then you just have to go to that hotel or resort and you have to mention the agency name and booking name they will give you the keys. There are so many agencies in Bangladesh but the popular ones are Obokash, Travelzoo Bangladesh Ltd, Airways, Hajee Air Travels, and many more. It is possible to find the travel agency from google.[30]

4.1.2 Long Term Housing: Long-term housing is a place where people think to stay for more time like it could be at least three months to more than a year. In Bangladesh, it is possible only in flats and apartments. It is a very common scenario here. Most of the people take rental flats and apartments for living. The owner of the rental home post the advertisement of rent at the gate of the apartment or another way is online. The most common scenario is that the rental advertisement you can find on the building gate or notice board. There they mention all the details of the apartment. If anyone wants to see then they can see it physically. On the website, it is also possible to found all the details information and pictures. It is also possible to take the phone number of the owner and talk with him offline. BD housing and B property is the largest online website for rental homes. Some owners of the house make a contract and some of them do not make it. For a rental home, one must have to give at least two months' rent in advance and have to make a contract on stamp paper. Their one has to provide all their information like National Identity Number, permanent address information and others. This kind of contract differs from owner to owner. If you want to live in one place for only six months then usually the owner doesn't make any rent agreement. It is good to ask the owner about the agreement before rent homes. Then they can give details of which kind of papers they want and also it is possible to know that the owner is interested in doing a contract or not. The payment of rent home usually everyone pays by cash. It is common practice in Bangladesh.

4.1.3 Hidden Cameras and Unauthorized Entry. One person should always be aware of the hidden recording device and unauthorized access to the place where they are living for a short-term or long-term stay. This kind of things also happen in Bangladesh but the amount of such incident is not that much high. This incident happens mostly in a small hotel. There room serviceman usually doing and the owner is not aware of that. The big hotels are aware of these kinds of things and do regular checks and monitor their employee. It is a kind of criminal offense in Bangladesh. But it is good for one person to always be aware of such kinds of things. Sometimes if someone records one's activity and then blackmail them via phone or another way. So it is good to concern about privacy and not to give accurate details information to the service provider.

One should visually inspect all areas of each room after entering into one room. These cameras are placed in appropriate small holes. One other way is to turn off all room lights and identify any led lights emitting from devices. From the book Extreme Privacy: What It Takes to Disappear by Michael Bazzell; he suggests if anyone finds these kinds of devices in the room then contact the police and file an official report. With the help of police retrieve the device and maintain control of it as evidence. Never complain directly to the hotel staff. This could destroy the device and a cover-up. Another trick he suggests is that with an old Android mobile phone which possesses the open-source privacy app Haven (https://guardianproject.github.io/haven). Haven is an Android app that uses on-device sensors to provide physical area monitoring and protection. Haven transforms any Android phone into a motion, sound, vibration, and light detector that keeps an eye out for unwelcome visitors and burglars.

In Bangladesh, it is an obvious situation to be aware of if you lived in a small hotel but it is the best option to be aware always as one knows when this kind of situation will happen. If any couple stays in the hotel or a single woman then it is good to measures all of these concerns. This kind of case happens regularly in Bangladesh.

4.2 India

Today, if a person needs a Temporary house to stay in for the short or long term, they will have to book the house by providing the personal Identifiable details and pay them by cash or other means of payment. Think about the amount of identifiable information a person is providing to the hotel or any other housing service provider. It may not seem to be a risk to provide details to a hotel but imagine if there was a data breach of a hotel chain that you often visit on your vacation or holidays. The hacker has all your personal information, like your name, mobile phone number, date of birth, your permanent residence address, your photo ID, they also know when you usually travel, and so on. The amount of information that is in the wrong hands is quite concerning to a person who wants to have a private life.

In this chapter, we will be discussing how to obtain temporary housing in India and how it can be obtained privately (If an option is available).

First, we will discuss how to obtain a Temporary house for a short stay. In India people generally prefer Hotels or Motels for a short stay, they can be easily obtained either by walking into a hotel or just a quick search on the internet. With the new stricter hospitality regulations in India, every housing service provider needs to collect a set of information and always needs to be present in their records. It is also made mandatory to have at least one surveillance camera in the hotel, preferably in the reception. With everything going digital these days, most hotels have to tie up with a service-based company like OYO, ClearTrip, Yatra, MakeMyTrip, and many more where hotels can list their rooms based on availability. Users can log on to these service provider's websites or mobile applications, perform a location-based search, look at the pricing and book a room in a hotel. Once the booking is done, the user must go to the hotel and provide any one of the Government ID proof like Aadhar card, PAN card, Voter ID, or Driving license. They make a scan of the ID and then once the payment is made, the keys to the rooms are given. I have had a personal experience where I have turned down a room at a hotel since I forgot to carry my Government ID. The hotel strictly does not accept any other kinds of ID, they might face legal action or penalties if they fail to collect government ids. There is a very minute chance of obtaining a room in a hotel without an ID in a not-so-good locality and not-so-good facility. But staying in such hotels is risky.

Now speaking about top Hospitality companies in India, several Indian and international hotel chains in India have 5-star hotels and resorts all over India. Companies like Hyatt, hotel Leela venture, Marriott International, Radisson Blu, Shangri LA, Taj hotels are the most popular ones. Only Taj hotels and The Leela Groups are GDPR compliant.[31] These kinds of hotels or resorts are only preferred by rich people in India. The hotels collect all kinds of information from the customers and have a huge database. It is mandatory to provide Government ID proof here as well. Many hotels provide an option to book a room online and check-in Online, some hotels in India also have digital keys where a customer can use his/ her mobile phone to unlock the room. So a person can skip the front desk or the reception but if a person books a room online a government ID has to be uploaded on their website before the payment can be made.

All of these regulations have come into place due to frequent scenarios where criminal offenders come to a city, stay at a hotel for a long period, commit crimes and leave with no marks. It makes it very difficult to the law enforcers to track down the criminals if there were no IDs collected by the hotels.

Now let us look at how to rent a home for a long period or indefinitely. In India, if you want to rent a home in a locality, you will either have to find the broker who deals in that area, or you will have to physically visit the locality to find To-let bords hung on the building. Listings in newspapers are quite uncommon these days. In the recent past there are listings available online on websites like 99acers.com, housing.com, quicker, OLX, and so on. The seller posts ads on these websites by paying some fee for the service. Users who need to find a house for rent can visit these websites and find contact details and information about the property. If the user visits the locality, then he/she can find To-Let boards hung on the property which includes the contact number. They can directly contact the landlord and fix a deal.

To make a deal, the landlord will request some documents to verify the tenant. Documents like photo ID, bank statement, and a canceled check will be required. After these documents are provided a contract is made a witness will have to sign the contract as well.[32] Sometimes it is required to pay 6 months or 1-year rent as a deposit.

Finding a landlord who is willing to rent his property without a legal contract and necessary documents is quite difficult but not impossible. But when a tenant is ready to pay a price above and beyond the standard rental price for not creating any contract and requesting any documents, the landlords tend to comply. We all know that cash is king.

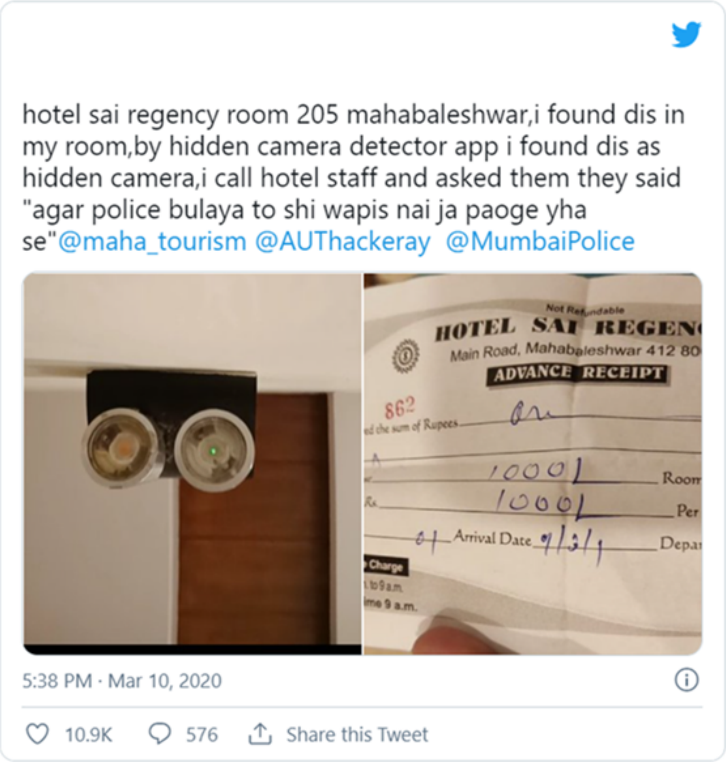
Having discussed all the options to rent a temporary house, we can conclude that it is absolutely difficult to rent a house privately without disclosing personal information.

4.2.1 Hidden camera and Unauthorized Entry: If a person is renting a room in a hotel, Airbnb, or resort, they always have to be aware of hidden cameras and unauthorized access to your space. There are many incidents these days where people are victims of such practices. Imagine if a person is recorded using a hidden camera during the period of stay at a hotel and if someone has access to the keys of the hotel room and can get in while the person who has rented the hotel room is out visiting someplace. All these scenarios are quite scary.

Such incidents happen in India regularly. You can find details about such incidents in the newspapers quite often. In India, such incidents are not reported most often as people fear that the compromising photos or videos can be published online by the holder.

In India, it is still Taboo or quite uncommon for young couples or unmarried couples to live together in a room at a hotel. When such couples try to book a room and if the hotel manager or in charge is a creep, then they try to allocate a room which has hidden cameras installed in it. They collect all the personal information of the couples while the booking is done. Once the couple checks out of the hotel, the creep retrieves the data from the cameras and sends the images or videos to the couple using the details which were provided. They might be exhorted for some money or other gains. This is a tough situation for the couple. They don't want their friends or family to know or see such things so most often than not they end up paying a huge amount of money to the creep to get the photos and videos deleted, sometimes even that can not be guaranteed. The videos can be uploaded to porn sites with their names included.

Many such incidents are happening in all parts of India. Be it in hotel rooms, changing rooms in a clothing outlet, public washrooms, and many other places.[33] When people find the hidden cameras and question the people responsible, they are threatened for their life, and most often than not the victim tend to obey what the threatener says.



hotel sai regency room 205 mahabaleshwar,i found dis in my room,by hidden camera detector app i found dis as hidden camera,i call hotel staff and asked them they said "agar police bulaya to shi wapis nai ja paoge yha se"@maha_tourism @AUThackeray @MumbaiPolice

5:38 PM · Mar 10, 2020

Fig. 7. Hotel hide camera in room
[34]

Here is one such incident where a man found a hidden camera in a hotel room and when he questioned the hotel staff he was told "You won't be able to return from here if you call the police."

But the police's investigation appears to have unearthed a very different story. First, when they examined the LED equipment, they found no hidden cameras. As well, an examination of other lights in the room revealed nothing fishy. Second, it emerged that the customer had had an argument with the hotel owner about billing and that he'd threatened to make allegations about a hidden camera. When the owner asked him to accompany him to the police station so an investigation could reveal any such cameras, the customer said he didn't want to pursue the issue and left.

Probably the evidence was cleaned off, the customer was threatened, and the police were paid to speak against the customer. You never know the truth in such incidences as these kinds of incidents are quite common in India. The accuser suddenly tells that he/she does not want to pursue the case which was filed by them as they would have been paid huge money to withdraw the case or their family would be put in danger.

One should follow basic checks to make sure such incidents do not occur, like inspecting the whole room, look for inappropriate holes, led lights, unusual smoke detectors, and vents. A person how travels very often can purchase an infrared imager unit that is easily available on the internet. This device comes in different price ranges. For a cheaper option, a person can use his or her phone with different detecting applications and scan the whole room.

4.3 Nepal

'Anonymity is a piece of cake when it comes to the Federal Democratic Republic of Nepal.' Different research said that Nepal is the land of making better privacy and anonymity. Nepal is separated into three topographic regions: the Himalaya to the north, the Mahabharat range and the Churia Hills to the middle, and the Terai to the south. The Himalayas and its foothills form the country's northern boundary, covering 16 percent of the total land area. This is Nepal's least populated region, with less than 8% of the population living there. The country's height ranges from less than 100 meters above sea level in the Terai to 8,848 meters at the top of Mt. Everest, all within a 150-kilometer radius, resulting in climatic conditions ranging from sub-tropical to the Arctic.[35]

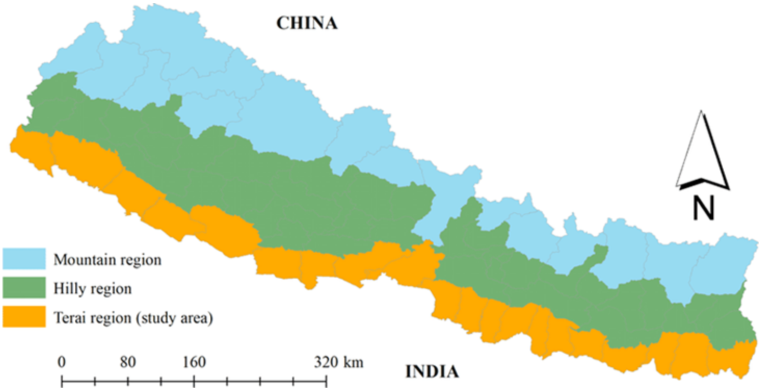


Fig. 8. Regions of Nepal
[36]

The reason I gave the geographic information about Nepal is, it is the place where we can make ourselves the most anonymity and privacy. About 70% of people are living in a remote part of

Nepal where it is very hard to get proper transportation and technologies. Still, there are some places in Nepal where people are having a very hard life, due to a lack of electricity and health service it is very hard to get their information. Internet services and digitalization are not provided by the Government to those areas due to the hard land structure. Therefore, this could be the 'place of heaven' where we can make ourselves anonymous. ' A famous French serial killer once stated in 2013: ' who was most wanted criminal and noticed by Interpol was hiding in Nepal for several years but later he was arrested by Nepal Police. According to him 'he felt more secure and could maintain anonymity in Nepal.

4.3.1 Hotel in Nepal: Well, let me also clarify your dilemma regarding the privacy of the inhabitants of our country. If you are in Nepal, your private life matters, and great care is taken regarding your data protection. In Nepal, various hotel booking applications such as OYO hotels and rooms and booking.com are in trend where you do not need to showcase your citizenship or Identity Card. You can just book a room via the application portal and get the keys from the reception when you show them your booking confirmation. For recordkeeping, the receptionist may ask you to fill up a form with your name, address, and phone number, which they would not even care to cross-check if all the data are valid. Unless there is any police investigation taking place at the premises, I don't think they will perform any genuine record keeping. Likewise, the payment of your accommodation fees is also possible when you are checking out from the hotel and with hand-in-cash. This means you are not exposed to any risk of your credit card information, nor will your real identification be exposed.

The concept of digital keys is not yet available in the local hotels and resorts in our country. Due to the lack of data keeping, attainment of anonymity is quite feasible in Nepal. However, it is always better not to be too friendly with the hotel keeper or the receptionist, or any staff of the hotel, as the members of the hospitality group may be able to monitor your activities and pass them on to your stalker or investigator.

There are some International Hotel chains present in some cities of the country such as Courtyard, Holiday Inn, Hyatt Regency, Crowne Plaza, Marriott, etc. These hotels run as per their hospitality policy and depending upon that, one may need to show their passport/ citizenship before check-in. Likewise, the hotels mandate the customers to pay via credit card which could leak your data and whereabouts to a third person and you will be registered in the system. So, it is always better to opt for some medium-priced hotels or resorts for better anonymity and privacy. The concept of digital keys is not yet available in the local hotels and resorts in our country. Due to the lack of data keeping, attainment of anonymity is quite feasible in Nepal. However, it is always better not to be too friendly with the hotel keeper or the receptionist, or any staff of the hotel, as the members of the hospitality group may be able to monitor your activities and pass them on to your stalker or investigator.

4.3.2 Rental Homes: It is not a common practice in Nepal for the landlord to keep any personal data or records of the tenant. Most of the rental contracts are made on a trust basis and completely verbal, which indicates that there are no written documents. It was only until December 2019 that the Government directed the Police Authority to keep records of the landlords and the tenants. The majority of the illegal activities, conducted either by a single person or a group, were found to have been located in rental homes registered in the name of the landlord. Due to the lack of document-proofing of the tenants, the criminals escape out easily just because they used an alias name and address or a fake name while registering at the hotel. In the capital city of the Country, Kathmandu, various illegal activities like theft, robbery, swindling, banking fraud, cybercrime, sexual offense, when investigated, were found to be conducted by people using such methodologies to disguise themselves.

4.3.3 Hidden Camera and Unauthorized Entry: Although it is feasible for you to live somewhere anonymously, it is also potentially easy that there are the chances your data can be disclosed to anyone without your permission or information. The cluster of local hotels and resorts founded in major tourist-targeted areas go through no major identification procedures, which means they do not care to check your citizenship/passport as long as you pay them well (they will be more than happy if you pre-pay them). However, there are also cases where they would promote sex trafficking, illegal activities, etc., sometimes without any knowledge of the clients/customers. Hidden cameras in the bathroom, changing rooms in the swimming pools or recreation area, and the hotel rooms could not be uncommon. The software mentioned by Michael Bazell in his book could be a major boon to check these activities and go for effective actions if you find any.

5 PRIVATE EMPLOYMENT

5.1 Bangladesh

Employment is the state of having work that is paid. If anyone employs someone is to pay them to work. The person or company employs employees. In terms of privacy; Private employment means as long as one person paid in cash and does not provide any details to the employer. In many countries this kind of behavior of work is illegal. Like: America, Germany, etc. On the other hand, it is not an issue in Bangladesh. As long as you are not connected with any illegal trading or activities. Most employers want or asked for the details of the employees. Because if one person wants to run a business then they must have to be registered and need a license. In this chapter, we are going to discuss private employment or the ways of minimizing exposure in the context of Bangladesh.

5.1.1 Traditional Employment: In the traditional way of employment in Bangladesh; The company asked for all the details of one employee. Like the name, address, date of birth, tax no, national identification, bank details, certificates, and many other documents. After confirming about the job the company asked for this kind of paper. It is kind of mandatory for every office. Some companies force to open a salary bank account to their favorite bank. With these documents the companies can check the background of an employee also they have to provide this information to the local police station for safety reasons. So that the privacy of one candidate will be broken. Here it is tough to provide fake documents because of every document they will check.

In the book of book, Extreme Privacy: What It Takes to Disappear by Michael Bazzell; here the writer talks about a company Equifax Inc.[1] It is an American multinational consumer credit reporting agency. Equifax collects and aggregates information on over 800 million individual consumers. So in the USA, they checked the profile with third-party agencies. After that, the company will be added to the consumer profile and shared. In 2017 breach of over 150 million people's full Equifax profiles. It is a good thing that in Bangladesh we don't have any third parties. Only companies checked by their self but it also can not possible in many times. These are kind of pen and papers rules.

If one person works in a mid-level company their it is not mandatory to provide all the documents. Some companies pay their employees in cash. So that they dose not need any kind of bank account. It is possible to make all the fake documents of one person in Bangladesh. As a result, if any person wants to concern about their privacy and doesn't want to share their details then they can make a fake one. One common scenario regarding academic certificates is that No university will provide you the original certificate before convocation. Also, universities don't do it regularly like almost every university takes at least 2 years to make a convocation program. Before the program, they only provide a provisional certificate. So anyone can make a fake provisional certificate. After joining the companies if any person stays for more time then no one asks for the certificates again. In almost every company after joining they will provide a new sim and email address. Only for the official purpose, it is given. So if anyone doesn't want to share their contact information then they can simply use these credentials.

If anyone got a government job in Bangladesh then it is impossible to make private all the information. The government agency named "National Security Intelligence" checked every background of a person.[37] If they also have some anti-government activity then it is impossible to join. They physically checked all the given data. They also checked the candidate's address and talks with the neighbors. Moreover, they do a previous history check. That's why it is not possible in Bangladesh to hide private information in government jobs.

All of these scenarios happened with or without consent from the employees. It is a common scenario in Bangladesh. Moreover, for government jobs it is mandatory. There is no second option for privacy in this field. Now almost every company put employees picture and details in their management software and company website. If anyone has private vehicle then for parking purpose ones have to prove the ownership of it. So companies asked for vehicles papers. Without papers, most of the people don't provide the parking facility to the employees. Some companies have now the system of figure print for attendance purposes. They take the fingerprint of employees to maintain the incoming and outgoing time of employees. If any company follows these rules then everyone must have to follow them.

In many countries, some careers need a license to do the work. Like in USA hair stylists, Ham radio operators, nurses, veterinarians, and many other professions. In Bangladesh, only in few careers does one need a license or registration. There it is mandatory and the national security agency checked all the background and gave clearance.

Overall, in traditional employment, it is not possible to maintain privacy. When it is in terms of Bangladesh sometimes some companies need every detail sometimes they don't need it. On the other hand for government jobs and licensed-based jobs, it is mandatory. There are a kind of open rules now that the details provided at any time during the employment process will become public information.

5.1.2 Self-Employment: When we talk about self-employment in the context of Bangladesh it refers to the personal business of one. This can be of various types. There are countless career choices for the self-employed. Here no one asked you every time for personal information. But for some of the official works like license, registration, rent, and other different things one needs to submit some basic papers. In comparison to traditional employment, it carries the same risk of public exposure. Here without proper information, it is impossible to get the official papers.[38]

There are three types of business structure runs by the local people.

(1) Limited Company
  (a) Private Limited Company
  (b) Public Limited Company
(2) Partnership Firm
(3) Sole Proprietorship

Registrar of Joint Stock Companies And Firms is for large scale of business. One cannot open a Private Limited Company. For this minimum of two and, a maximum of fifty directors is required.

On the other hand, for Public Limited Company minimum number of the member should be seven and the maximum is unlimited. When anyone wants to open a Joint Venture Company minimum number of the member should be two and maximum fifty. Out of all members minimum, one should be Bangladeshi and minimum one should be Foreigner. In Bangladesh no scope to start a Limited Company by one man. That's why it is quite tough to make all the information private. Registrar of Joint Stock registers foreign company and Branch Office, Liaison Office, Representative Office of Multinational Company. Joint Venture Companies are also registered at the Registrar of Joint Stock Companies And Firms. [39]

To open a business like a sole proprietorship in Bangladesh the first thing one person need is a Trade license. Trade license is issued by the local city corporation office, paurashava, and union parishad. Without this, it is not counted as a legal business. For these number one person have to submit personal details. It is impossible in Bangladesh to get a Trade license without personal information. After application with small government fees, one can get your trade license in a couple of days.

5.1.3 Nomad Business: There is a way of doing business nowadays very popular in Bangladesh. In this way, it is possible to make hide one's full identity. In Bangladesh online shopping is very much popular. Everyone purchases various products through these sites. No one needs any kind of paper to do this business.

The common way of doing this business is here using Facebook, YouTube, and Instagram. These three are so much popular here. For this kind of business no paper works need. Just need a page or account on these sites. Here seller posts all the good items. The communication between the buyer and sell is done in the message. The payment system is the traditional way like payment on delivery. For delivery, there are several options and one person can register with them with fake details. The most popular delivery companies are here are Pathao Courier, Sheba Delivery, REDX Delivery, eCourier, Delivery Tiger, and Sonar Courier.[40] These are the best option. Here one has to send all the packages with the price list and addresses of the buyer at the package point. They take usually 72 hours to send the delivery. The seller gets the money at the end of the week. There are several options for receiving the payment. One can use mobile banking or banking. Moreover, it is also possible to use another person's payment details. They don't have any restrictions.

On the other hand, there is no restriction to doing this kind of business on the side of the government. As there are no rules and regulations for such kind of business. So it is legal to do such kind of online business. There is some kind of policy but it is not a final one. For those people who did this kind of business, it is tough to know their details. Only one phone number they provide. They don't need any office address. Their activity is a kind of cloud business type. People of Bangladesh are now so much habituated. The main security of the customer is they don't have to pay in advance; the payment method is cash on delivery which attracts the customers. It is a safer option in the context of seller privacy in Bangladesh. No paper works no background check is needed.[41]

5.2 India

Let's discuss traditional employment in India. If a person applies for a job in India, they will be asked for Personal Identifiable details like name, DOB, address, a government photo ID, a couple of passport photos, and educational qualification documents. In some cases, it is mandatory to provide a passport as well. This information is required for a background check, companies usually have a team who performs the background check or they make use of a third-party service for the check.

This information is passed on to the third parties if it is required. We all know how concerning this can be after the Equifax breach, more than 150 million people's profiles were leaked. They also collect your PAN (Personal Identifiable Number) which is related to Tax and bank details for the payments. It is absolutely necessary to provide true details to the employer in India, else you might face legal actions if it is found that you have provided incorrect details. The techniques mentioned by Writer Michael Bazzell in the book Extreme privacy like providing MySudo phone number and Po Box address does not apply in India as we do not have a concept of PO Boxes and services of MySudo is not available in India. Earlier all the records were with pen a paper but after the digitalization, all the data is stored and is prone to be leaked.

If you have a job in an IT company, public service sector and any huge company in India, you can consider you have provided most of your personal data to them and you have already given up on your right to privacy.

If you think privacy comes above everything for you and if it is ok for you to not work in any of the above-mentioned sectors then there are various options for a person in India to have private employment.

5.2.1 Self Employment: It is quite opposite to traditional employment, Self employment can be advantageous in many ways with regards to privacy. If donr in a right manner you don't have to provide any personal details to anyone. There are different kinds of jobs you can choose when you consider self employment. One can choose freelancing jobs where the person need not provide much information to the person he is working for, he can just meet them in person, discuss the job, complete it and deliver it once the payment is done, the payment can be collected in case so that there are no records of any transactions and you do not have to share your bank details as well. These jobs are easy to find. A person can list his services on few job portals using pseudo names and a temporary email just created for the job. A person needing this service can contact the service provider by the email provided and the job can be done.

An other option is farming, if you are self employed as a farmer you need to provide any details for employment, you need not register anywhere to do farming. Most of the farmers use their own lands to grow crops, buy the raw materials required for the produce at any government shops at subsidised prices without an ID and pay with cash. You can hire few labours and pay them daily wages by cash. Sell the produce at farmers markets which are available in every districts and get paid in cash. There is no personal data involved, You don't have to provide or collect any personal data.

Other option is having your own business, This business can be any kind which does not need a government approval and which is legal. You are your own boss, You can create multiple sources of income by cash and no one has any records of the business.

Overall having a private employment is very easy in India, it is because there are various jobs available which do not need a registration or a contract. As long as the job pays you by cash you can consider that you are safe with regards to privacy.

6 PHYSICAL PRIVACY SECURITY

6.1 Nepal

6.1.1 Physical Privacy Security: Nowadays, we use IoT devices, and the privacy and security of physical objects are critical to the applications that use them. The primary role of an IoT system is to gather data from the real environment and conduct tasks for users based on their requests. In the Internet of Things, cyber entities are mapped to physical items that may interact with one another.

They work together to achieve a certain task. The Internet of Things, as an application-driven network, is also used in daily life, such as smart home, e-health, environment monitoring, and so on. At the moment, Nepalese people utilize IoT gadgets to simplify their smart homes. At the same time, these devices raise privacy and security concerns.

Smart Home (SH) technologies increase the quality of life, home security, and facilitate elderly care. Objects such as housing devices, technology, and consumer electronics are incorporated into smart homes via communication, information, and sensors. To meet the needs of users, they may be accessed, managed, and monitored. Although SH technologies are becoming more widely available to end-users, the present level of adoption in Nepal remains low due to privacy and security concerns.

6.1.2 Make your Home Privacy: To preserve privacy, cybersecurity is given a lot of attention. Currently, the Nepalese government has assigned security experts to prevent, safeguard, and secure people's important data. IoT devices are also capable of safeguarding end users' privacy. There are several IoT technologies available to protect user privacy in SH, including CCTV, motion detectors, face identification gate unlock, fire alarms, biometric scanners, and so on. Although these technologies can be controlled by third parties and can observe them, we need to integrate these technologies with different networks to protect our privacy. Furthermore, adopting these technologies improves your privacy while also advancing your lifestyle.

When you start working from home, it is tempting to get caught up in personal tasks during work hours. You also manage to protect your dignity, which is important because working in an office with more than twenty individuals would not protect your privacy. Because of the corona epidemic, Nepalese began working from home; as a result, work efficiency rose, and employees were able to complete a variety of personal activities in addition to their work. Large corporations give electronic devices such as laptop computers to their employees for them to accomplish their jobs. Since the company's important data may be stored on the laptop, you must keep in mind that you must also maintain the company's privacy policy when working from it. You will have access to the company's emails, as well as web administration and crucial information. Therefore, you must safeguard these items when working from home to protect your privacy. When working from home, information security is a top priority. Computer security is the phrase used to describe the safeguards that protect computer systems and networks from harm to hardware, software, and data. Employees should have the necessary tools to maintain cybersecurity, such as a VPN, firewall, antivirus software, encrypted communication, data backup, 2FA, and so on. It assists us in adhering to both our personal and corporate privacy policies.

6.1.3 Home Security System: Smart Home includes all IoT security gadgets to enhance home security. And all of these gadgets are interconnected to the home network to execute tasks as desired by the user; moreover, users may manage and monitor them. These IoT gadgets, such as smart door locks, smart light bulbs, motion sensors, cameras, fire alarms, and so on, are linked to sensors, and if something unexpected happens, the sensor triggers, and the devices begin to execute programmed tasks.

For example, if a thief breaches the smart gate lock, he will enter the home via smart light bulbs and motion detector cameras. At that time, the sensor will detect unusual activity and the bulb will glow, and the motion detector camera will capture him and notify the owner via a ringing smartphone. Currently, in Nepal, households, offices, and businesses employ building management security systems to protect their valuables from theft.

6.1.4 Fire alarm System: The fire alarm system employs a variety of technologies, including visual and aural signalization, as well as sensors that detect fire, smoke, and carbon monoxide. If the sensor detects smoke, an audio device is triggered to notify the user that a fire has been detected, and a watering system is activated to water the area where the fire has been detected. A signal is also sent to the monitoring system to indicate the position of the fire in the building. Government and corporate buildings employ fire detection and alarm systems where hundreds of people work in addition to typical homes, but in the case of an SH, this system is also designed to alert and avoid a major fire disaster. There are several types of fire alarm systems based on their functioning in Nepal. They are automated, addressable, conventional, and have one or two stages. Buildings with more than three stories utilize two stages and an addressable fire alarm system to alert people and activate the water system. In most smart homes, an automated fire alarm system is utilized to warn the owner by activating the alarm or sending a message to the owner's smartphone.

7 CONCLUSION

South Asia is becoming increasingly digitized and modernized. Since the technologies arrived, Bangladesh, India, and Nepal have used far more of them. In the recent past, people of these countries are depending on technologies in their daily life. The maturing mobile digital ecosystems in Bangladesh, India, and Nepal have set the stage for mobile phone and software manufacturers to turn their attention to new markets. Moreover, South Asia is also predicted to become the engine that propels global digital life into a new era similar to regions like the USA and Europe. With the rise in digitization, there are more data collected daily. People in South Asian countries do not know what kinds of data or information can be shared what can not be shared. They tend to share all kinds of personally identifiable information even when it is not required. Companies that store these data do not have a strong security posture, this often leads to data leaks. We all know how threatening it can be when a person with malicious intent has data about us using which we can be identified and tracked. The majority of the people in India, Nepal, and Bangladesh do not care about data leaks, they do not read privacy policies when they provide information about them to a company. You can easily find personal information of people in India, Bangladesh, and Nepal on the internet. Most people in these countries do not know what privacy means and do not care about having privacy. This report can be used for better understanding what privacy means, why it is important to have privacy, how it can be achieved and what are the best practices.

REFERENCES

[1] Michael Bazzell. Extreme Privacy: What It Takes to Disappear, 2021. [Online; accessed 17-July-2021].

[2] Bangladesh Telecommunications Company Limited. https://en.wikipedia.org/wiki/BTCL. [Online; accessed 17-July-2021].

[3] SIM Card Registration Check Online (GP, Robi, Airtel) Biometric SIM. https://allresultbd.com/sim-card-registration-check/. [Online; accessed 17-July-2021].

[4] Bangladesh to block 20.5 lakh illegal SIM cards today. https://www.newagebd.net/article/70794/bangladesh-to-block-205-lakh-illegal-sim-cards-today. [Online; accessed 17-July-2021].

[5] Bangladesh 73rd on National Cyber Security Index. https://www.dhakatribune.com/technology/2018/05/29/bangladesh-ranks-73-in-global-cyber-security-index. [Online; accessed 17-July-2021].

[6] 7 Best VPNs for Bangladesh in 2021. https://www.comparitech.com/blog/vpn-privacy/best-vpn-bangladesh/. [Online; accessed 17-July-2021].

[7] Chor Bazaar, Mumbai. https://en.wikipedia.org/wiki/Chor_Bazaar,_Mumbai. [Online; accessed 17-July-2021].

[8] Nepal Telecom, Nepal Telecom growth rate is highest among all telcos . https://www.nepalitelecom.com/2016/12/nepal-telecom-growth-rate-highest-among-telcos.html. [Online; accessed 17-July-2021].

[9] VPN ranks of Nepal, The Best VPN For Nepal (July 2021 Updated) . https://www.vpnranks.com/countries/nepal/. [Online; accessed 17-July-2021].

[10] Jian Wang, Zhiyong Zhang, Fei Xiang, and Weihua Yu. Trusted license distribution system based on ipsec vpn for mobile drm. *The Open Electrical & Electronic Engineering Journal*, 8(1), 2014.

[11] Police arrest youths for blackmailing on Facebook. https://www.thefinancialexpress.com.bd/national/crime/police-arrest-youths-for-blackmailing-on-facebook-1548498221. [Online; accessed 17-July-2021].

[12] Checking for Pwned Passwords in Active Directory. https://specopssoft.com/blog/checking-pwned-passwords-active-directory/. [Online; accessed 17-July-2021].

[13] Bangladesh Telecommunication Regulatory Commission- ISP. http://www.btrc.gov.bd/internet-service-provider. [Online; accessed 17-July-2021].

[14] The Kathmandu Post Towards . https://kathmandupost.com/opinion/2018/09/30/towards-a-digital-nepal. [Online; accessed 17-July-2021].

[15] Introduction to Digital Security Laws in Nepal, Sri Lanka, and Bangladesh . https://www.ikigailaw.com/introduction-to-digital-security-laws-in-nepal-sri-lanka-and-bangladesh/. [Online; accessed 17-July-2021].

[16] History of iPhone in Nepal. https://www.nepalisansar.com/special-stories/10-reasons-why-nepalese-love-to-buy-iphone/. [Online; accessed 17-July-2021].

[17] Is Apple FaceTime safe? . https://www.macworld.co.uk/news/is-apple-facetime-safe-3785750/#:~:text=Back%20at%20the%20beginning%20of,without%20them%20answering%20the%20call. [Online; accessed 17-July-2021].

[18] Mac OS User GuideChange Privacy preferences on Mac . https://support.apple.com/guide/mac-help/change-privacy-preferences-on-mac-mh32356/mac. [Online; accessed 17-July-2021].

[19] Techtarget Network, Definitiontwo-factor authentication (2FA) By Linda RosencrancePeter Loshin . https://searchsecurity.techtarget.com/definition/two-factor-authentication. [Online; accessed 17-July-2021].

[20] Operating System Market Share Worldwide . https://gs.statcounter.com/os-market-share. [Online; accessed 17-July-2021].

[21] Operating System User Of Nepal. https://gs.statcounter.com/os-market-share/all/nepal. [Online; accessed 17-July-2021].

[22] 14-year old arrested for hacking social media accounts of celebrities . https://tkpo.st/3dHPEAPhttps://kathmandupost.com/national/2021/04/06/14-year-old-arrested-for-hacking-social-media-accounts-of-celebrities. [Online; accessed 17-July-2021].

[23] Password manager. https://www.malwarebytes.com/what-is-password-manager. [Online; accessed 17-July-2021].

[24] How does email work? Lisa McKnight . https://www.namecheap.com/guru-guides/how-does-email-work/. [Online; accessed 17-July-2021].

[25] How to access Internet browser settings? . https://www.computerhope.com/issues/ch001918.htm. [Online; accessed 17-July-2021].

[26] Justin McCrary and Heather Royer. The effect of female education on fertility and infant health: evidence from school entry policies using exact date of birth. *American economic review*, 101(1):158–95, 2011.

[27] Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, and Claudia Diaz. A survey on routing in anonymous communication protocols. *ACM Computing Surveys (CSUR)*, 51(3):1–39, 2018.

[28] Dhaka to see six new luxury hotels. https://www.thedailystar.net/business/dhaka-see-six-new-luxury-hotels-1572655. [Online; accessed 17-July-2021].

[29] Hotel industry sees bright prospect in Bangladesh. https://www.risingbd.com/english/risingbd-special/news/25818. [Online; accessed 17-July-2021].

[30] Top 10 Travel Agencies In Bangladesh. https://airwaysbd.com/travel-agency-bangladesh/. [Online; accessed 17-July-2021].

[31] Data breach: Hospitality sector yet to comply with GDPR . https://economictimes.indiatimes.com/tech/internet/data-breach-hospitality-sector-yet-to-comply-with-gdpr/articleshow/64362442.cms?from=mdr. [Online; accessed 17-July-2021].

[32] Rent Agreement Laws. https://legaldocs.co.in/blog/rent-agreement-laws-in-india. [Online; accessed 17-July-2021].

[33] Fabindia 'hidden camera' case: More women were filmed. https://www.hindustantimes.com/india/fabindia-hidden-camera-case-more-women-were-filmed/story-UfAmKkCiRa9oU8xdzdvREM.html. [Online; accessed 17-July-2021].

[34] Man says Mahabaleshwar hotel hid camera in room. What cops found. https://www.indiatoday.in/india/story/mahabaleshwar-hotel-hidden-camera-claim-1654332-2020-03-11. [Online; accessed 17-July-2021].

[35] Geography of Nepal . http://web.gps.caltech.edu/~avouac/nepal_trip/geography.htm. [Online; accessed 17-July-2021].

[36] My Republica, Who is right, who is wrong on Nepal-India battle of maps. https://myrepublica.nagariknetwork.com/news/who-is-right-who-is-wrong-on-nepal-india-battle-of-maps/. [Online; accessed 17-July-2021].

[37] National Security Intelligence. https://en.wikipedia.org/wiki/National_Security_Intelligence. [Online; accessed 17-July-2021].

[38] How to Register a Company in Bangladesh. https://tahmidurrahman.com/how-to-open-a-company-in-bangladesh/. [Online; accessed 17-July-2021].

[39] Private Limited Company Registration in Bangladesh. https://supremeip.com/company-incorporation/. [Online; accessed 17-July-2021].

[40] 6 Best Online Courier and Delivery Services In Bangladesh. https://deshiz.com/online-courier-delivery-services-bangladesh/. [Online; accessed 17-July-2021].

[41] E-Commerce Company Formation in Bangladesh| Complete Overview of Starting an E-commerce Business. https://tahmidurrahman.com/e-commerce-business-in-bangladesh/. [Online; accessed 17-July-2021].