Privacy and Security Implications of Public Wi-Fi - A Case Study

(I) Introduction

Recognizing internet as a critical tool for day-to-day work and facilitating increased access to it in the past few years,[1] the Indian Government as well as Governments across the world have rolled out plans for offering public Wi-Fi. However, privacy risks of using public Wi-Fi have also been flagged across jurisdictions, which will be discussed in this paper. Apart from highlighting key privacy concerns associated with the use of free public Wi-Fi, this case study aims to analyse the privacy policies of two of the Internet Service Providers in India-namely Tata Docomo[2] and D-VoiS[3], which offer public Wi-Fi services in Bangalore city against the indicators listed under the Ranking Digital Rights project[4], as well as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[5]. Based on this analysis, this paper shall list key recommendations to these ISPs to ensure sound privacy policies and practices with a view to have a balanced framework and ecosystem in light of key privacy considerations, especially in light of public Wi-Fi.

(II) Global scenario

Security and privacy concerns around the use of free and public Wi-Fi have been raised in India[6] as well as across the globe. In various cities like Bangalore, Delhi, Hyderabad, New York, London, Paris, etc., privacy experts have raised concerns over the public Wi-Fi systems at metro stations, malls, payphones and other such public places.[7]

For many years, New York City has been in the process of developing a "free" public Wi-Fi project called LinkNYC[8] to bring wireless Internet access to the residents of the city. However, privacy concerns have been raised by the users and privacy advocates like the New York Civil

---

[1] The Financial Express, 'Free wi-fi: Digital Dilemma', February 22, 2015, http://www.financialexpress.com/article/economy/free-Wi-Fi-digital-dilemma/45804/

[2] Tata Docomo, http://www.tatadocomo.com/

[3] D-VoIS Communication Pvt. Ltd. http://www.dvois.com/

[4] Ranking Digital Rights, https://rankingdigitalrights.org/

[5] the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Available at : http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf

[6] See : http://indianexpress.com/article/technology/technology-others/public-wifi-can-be-used-to-steal-private-information-it-security-expert/, http://www.aljazeera.com/indepth/features/2016/03/india-unlocking-public-wi-fi-hotspots-160308072320835.html , http://www.business-standard.com/article/technology/indians-most-willing-to-share-personal-data-over-public-wifi-116083000673_1.html and http://articles.economictimes.indiatimes.com/2015-05-20/news/62413108_1_corporate-espionage-hotspots-bengaluru-airport

[7] Scroll, 'Free wifi in Delhi is good news but here is the catch', November 21, 2014, http://scroll.in/article/690755/free-wifi-in-delhi-is-good-news-but-here-is-the-catch

[8] LinkNYC, https://www.link.nyc/

Liberties Union, where the latter also issued a letter to the Mayor's office regarding this[9] as the collection of potentially sensitive personal, locational and behavioral data, without adequate safeguards could result in sharing of such data without the data subject's consent or knowledge. For example, one of the concerns raised has been regarding retention of user's data by CityBridge, the company behind the LinkNYC kiosks, often indefinitely, for building a massive database which carries a risk of security breaches and unwarranted surveillance by the police. [10] Also, users are concerned that their internet browsing history may reveal sensitive information about their political views, religious affiliations or medical issues[11], since registration is required to use LinkNYC by submitting their email addresses and by agreeing to allow CityBridge to collect information about the websites they visit, the duration for which they linger on certain information on a webpage and the links they click on. On the contrary, the privacy policy of CityBridge states that this massive amount of personally identifiable user information would be cleared only if there have been 12 months of user inactivity, raising an alarm in light of privacy concerns.[12]

In the year 2015, the Information Commissioner's Office (ICO) conducted a review of public Wi-Fi services on a UK high street, where it was found that the Wi-Fi networks requested for varying levels of personal data, which was also processed for marketing purposes. The results highlighted that while some networks did not request any personal data, others asked for varying amounts, including information regarding name, postal and email address, mobile number, gender, as well as asking for a date of birth as a mandatory requirement (except for gender). During the sign-up process, though some Wi-Fi networks provided users with the choice to opt-in or opt-out for receiving electronic newsletters and updates, others offered no choice at all.[13] As a result of the review process, the ICO notified Wi-Fi network providers that it had reviewed and advised them of improvements that they could make to their service and issued guidance[14] regarding the dangers of using public Wi-Fi[15]. ICO also recommended users to take time to read all the information given by providers of Wi-Fi services before connecting.

---

[9] See : http://www.nyclu.org/files/releases/city%20wifi%20letter.pdf

[10] The Huffingtonpost, 'Maybe You Shouldn't Use Public Wi-Fi In New York City', March 16, 2016, http://www.huffingtonpost.in/entry/public-wifi-nyc_us_56e96b1ce4b0b25c9183f74a

[11] NYCLU, 'City's Public Wi-Fi Raises Privacy Concerns', March 16, 2016, http://www.nyclu.org/news/citys-public-wi-fi-raises-privacy-concerns

[12] NYCLU, 'City's Public Wi-Fi Raises Privacy Concerns', March 16, 2016, http://www.nyclu.org/news/citys-public-wi-fi-raises-privacy-concerns

[13]Information Commissioner's Office Blog, 'Be wary of public Wi-Fi'September 25, 2015, https://iconewsblog.wordpress.com/2015/09/25/be-wary-of-public-Wi-Fi/

[14]Information Commissioner's Office Blog, 'Be wary of public Wi-Fi'September 25, 2015, https://iconewsblog.wordpress.com/2015/09/25/be-wary-of-public-Wi-Fi/

[15]Marketing Law, 'The ICO sounds a warning on public wi-fi and privacy', November 24, 2015, http://marketinglaw.osborneclarke.com/data-and-privacy/the-ico-sounds-a-warning-on-public-Wi-Fi-and-privacy/

In 2006, the European Data Retention Directive 2006/24/EC[16] was introduced for the retention of communications data by providers of public electronic communications services for national security. The Directive provides an obligation for providers of publicly available electronic communications services and public communications networks to retain traffic and location data for the purpose of the investigation, detection, and prosecution of serious crime.[17] Also, the Data Retention (EC Directive) Regulations 2009[18] were introduced to implement the Directive in the UK. However, this was challenged on grounds of insufficient safeguards for the privacy rights of individuals, given the substantial interference which it facilitated with those rights.[19]

To ensure protection of user's data and information, the Data Protection Act 1998[20] in UK obliges businesses retaining people's data to comply with the law, which involves informing people about what data is being collected and ensure that the data is stored securely.[21] . Therefore, in case of ISP's providing public Wi-Fi service, this would relate to the information people provide when they log on, such as their email address. Under the Act, the data protection principles must be complied with by the data controllers and it needs to be ensured that the information is used fairly and lawfully, for limited and stated purposes, used in a way that is adequate, relevant and not excessive, kept for no longer than is absolutely necessary, handled according to people's data protection rights, kept safe and secure and not transferred outside the European Economic Area without adequate protection.[22] This would soon be updated and synced with the European Union's General Data Protection Directive (GDPR).

(III) Overview of public wifi in India

In India, the public Wi-Fi in some cases has been offered free for a limited duration, in several cities across the country. For example, in 2014, Bangalore became the first city in the country to establish free public Wi-Fi- Namma Wi-Fi (802.11N) to make Bangalore a smart and connected city. The service is offered at MG Road, Brigade Road and four other locations in Bangalore including Traffic and Transit Management Centres (TTMCs) at Shanthinagar, Yeshwanthpur,

[16] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0024

[17] Feiler, L., "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", European Journal of Law and Technology, Vol. 1, Issue 3, 2010, http://ejlt.org/article/view/29/75

[18] The Data Retention (EC Directive) Regulations 2009 http://www.legislation.gov.uk/ukdsi/2009/9780111473894/pdfs/ukdsi_9780111473894_en.pdf

[19] Purple, 'Update on the legal implications of offering public WiFi in the UK', September 10, 2014, http://purple.ai/update-legal-implications-offering-public-wifi-uk/

[20] Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents

[21] Wireless Social, http://www.wireless-social.com/how-it-works/legal-compliance/

[22] Data Protection Act 1998, https://www.gov.uk/data-protection/the-data-protection-act

Koramangala and CMH Road in Indiranagar.[23] The internet and Wi-Fi service provider for Namma Wi-Fi is D-VoiS Broadband Ltd,a city-based firm.[24] However, it seems the State Government plans to pull the plug on the project, funds, lack of awareness and difficulty in access as key constraints.[25] Tata Docomo has inked an agreement with GMR Airports to offer Wi-Fi services at several International Airports in the country, including the Bangalore International Airport. It offers access to access free Wi-Fi service for 45 minutes, following which they users are required to pay for the service online, to continue using the Wi-Fi service.[26]

Delhi has also introduced free Wi-Fi at its premier shopping hubs of Connaught Place and Khan Market in the year 2014, and BSNL launched a free WiFi service at Karnataka's Malpe beach in the year 2016 making it the first WiFi beach in the three coastal districts of the state.[27] The State Governments of Mumbai, Kolkata, Patna and Ahmedabad also offer free Wi-Fi services in limited areas.[28] As part of the flagship programme by Indian Government, Digital India, the Government announced the rollout of Wi-Fi services by June 2015 at select public places in 25 Indian cities with population of over 10 lakh and tourist destinations by December 2015.[29] Also, the Government has plans to digitise India by rolling out free Wi-Fi in 2500 towns and cities over a span of 3 years.[30] Google plans to deploy WiFi at 100 railway stations in partnership with Railtel. Under this scheme, Mumbai Central was the first station to get free Wi-Fi in the year 2016.[31] Also, Google's Project Loon aims to provide internet connectivity in remote and rural areas in India, which is currently being tested in other countries.[32].

---

[23]The Hindu, 'Free wifi on M.G. Road and Brigade Road from Friday', January 23, 2014, http://www.thehindu.com/news/cities/bangalore/free-wifi-on-mg-road-and-brigade-road-from-friday/article5606757.ece

[24]The Telegraph, 'Free Wi-fi on tech city streets- Bangalore offers five public hotspots', January 25, 2014, http://www.telegraphindia.com/1140125/jsp/nation/story_17863705.jsp#.VwIv_Zx97IU

[25]Economic Times, 'Karnataka Govt pulls the plug on public Wi-Fi spots in Bengaluru', March 15, 2016, http://tech.economictimes.indiatimes.com/news/internet/karnataka-govt-pulls-the-plug-on-public-Wi-Fi-spots-in-bengaluru/51404414

[26] Medianama, 'Why Don't Indian Airports Offer Free WiFi To Passengers?', May 22, 2013, http://www.medianama.com/2013/05/223-indian-airports-free-wifi/

[27]Hindustan Times, 'BSNL launches free public WiFi at Karnataka's Malpe beach', January 25, 2016, http://www.hindustantimes.com/tech/bsnl-launches-free-public-wifi-on-karnataka-s-malpe-beach/story-XVM06KQKIcoyqV8CLJoYzJ.html

[28]TechTree, 'Problems With Free City-Wide Wi-Fi Hotspots In India', September 28, 2015, http://www.techtree.com/content/features/9914/problems-free-city-wide-Wi-Fi-hotspots-india.html#sthash.2ZSf9kq7.dpuf

[29]India Today, '25 Indian cities to get free public Wi-Fi by June 2015', December 17, 2014, http://indiatoday.intoday.in/technology/story/25-indian-cities-to-get-free-public-Wi-Fi-by-june-2015/1/407214.html

[30]Business Insider, 'Modi Government To Roll Out Free Wi-Fi In 2,500 Towns And Cities To Make India Digital', January 23, 2015, http://www.businessinsider.in/Modi-Government-To-Roll-Out-Free-Wi-Fi-In-2500-Towns-And-Cities-To-Make-India-Digital/articleshow/45989339.cms

[31]RailTel launches free high-speed public Wi-Fi service with Google at Mumbai Central, http://www.railtelindia.com/images/Mumbai.pdf

[32]Economic Times, 'Google may get government nod to conduct pilot for Project Loon in India', May 24, 2016, http://economictimes.indiatimes.com/tech/internet/google-may-get-government-nod-to-conduct-pilot-for-project-loon-in-india/articleshow/52408455.cms

(IV) Indian policy and legal conundrum

In light of national security concerns around the misuse of public Wi-Fi, the Department of Telecommunication, GoI, published a regulation[33] dated February 2009, defining procedures for the establishment and use of public Wi-Fi to prevent misuse of public Wi-Fi and to be able to track the perpetrator in case of abuse. Indeed, the DOT has stated that "Insecure Wi-Fi networks are capable of being misused without any trail of user at later date".[34]

As per the 2009 Regulations, DoT has instructed ISPs to enforce centralized authentication using Login ID and Password for each user to ensure that the identity of the user can be traced.[35] Regarding Wi-Fi services provided at public places, the Regulations state that bulk login IDs shall be created for controlled distribution, with authentication done at a centralized server. The subscribers are required to use public Wi-Fi by registering with temporary user ID and password, in the following methods:

- Obtaining copy of photo identity of the subscriber, to be maintained by Licensee for one year; or
- Providing details of user ID and password via SMS on subscriber's mobile phone , to be used as his/her identity by keeping the mobile number for one year.

Additionally, the data protection regime in India is governed by section 43A of the Information Technology Act, 2000 and the Rules[36] notified under it. It obliges corporate bodies which possess, deal or handle any sensitive personal data to implement and maintain reasonable security practices, failing which they would be held liable to compensate those affected by any negligence attributable to this failure. The said Rules also define requirements and safeguards that every Body Corporate is legally required to incorporate into the company's privacy policy. The Rules put restrictions on body corporates on collecting sensitive personal information, and also states that it must obtain prior consent from the "provider of information" regarding "purpose, means and modes of use of the information, along with limiting disclosure of such information.[37] Most of the ISPs in India being a private company, like D-VoiS and Tata

[33]Department of Telecommunications, Ministry of Communications & IT, Government of India, February 23, 2009, http://www.dot.gov.in/sites/default/files/Wi-%20fi%20Direction%20to%20UASL-CMTS-BASIC%2023%20Feb%2009.pdf

[34] Scroll, 'Free wifi in Delhi is good news but here is the catch' November 21, 2014, http://scroll.in/article/690755/free-wifi-in-delhi-is-good-news-but-here-is-the-catch

[35]MojoNetworks, 'Complying with DoT Regulation on Secure Use of WiFi: Less in Letter, More in Spirit', http://www.mojonetworks.com/fileadmin/pdf/Implementing_DoT_Regulation_on_WiFi_Security.pdf

[36] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[37]The Centre for Internet & Society, 'Privacy and the Information Technology Act — Do we have the Safeguards for Electronic Privacy?', April 7, 2011, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

Docomo, are obliged to comply with these provisions. Also, under the model License Agreement for Unified License[38] by Ministry of Communication & IT, Department of Telecommunications, Government of India, where the Unified Access License Framework allows for a single license for multiple services such as telecom, the internet and television and provides certain security guidelines, privacy of communications is to be maintained by the Licensee (the ISPs in this case) and network security practices and audits are mandated along with penalties for contravention in addition to what is prescribed under the Information Technology Act,2000. It also provides for ensuring unauthorized interception of messages does not take place. Therefore, the ISPs providing public Wi-Fi services in various cities across India would be governed by the data protection regime and could be held liable under these provisions in case of non-compliance with the security measures so stated.

In July 2016, the Telecom Regulatory Authority of India (hereinafter referred as "TRAI") floated a Consultation paper on Proliferation of Broadband through Public Wi-Fi Networks[39] with an objective to examine the need of encouraging public Wi-Fi networks in the country from a public policy point of view and discuss the issues as well as solutions in its proliferation. The paper recognises the fact that India is still in a green field deployment phase in terms of adoption of public Wi-Fi services and requires solutions for resolving the challenges and risks being faced in the process and lay a strong foundation to evolve towards a meaningful position in the advancement of initiatives related to Internet of Things, Smart Cities, etc.[40] This is an important step towards fulfilment of the Digital India scheme of the Indian Government to ensure better connectivity. In the paper, TRAI has advocated development of a payment platform which allows easy access to Wi-Fi services across internet service providers (ISPs) and through any payment instrument.[41] Besides that, the paper raises issues of various regulatory, licensing or policy measures required to encourage ubiquitous city-wide Wi-Fi networks as well as expansion of Wi-Fi networks in remote or rural areas, along with the issue of encouraging interoperability between the Wi-Fi networks of different service providers, both within the country and internationally, as well as between cellular and Wi-Fi networks.[42]

---

[38] License Agreement for Unified License, http://www.dot.gov.in/sites/default/files/Unified%20Licence.pdf

[39] Telecom Regulatory Authority of India, 'Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks' July 13, 2016, https://www.mygov.in/sites/default/files/mygov_1468492162190667.pdf

[40] Telecom Regulatory Authority of India, 'Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks' July 13, 2016, https://www.mygov.in/sites/default/files/mygov_1468492162190667.pdf

[41] The Economic Times, 'Trai floats consultation paper to boost broadband through Wi-Fi in public places', July 14, 2016, http://economictimes.indiatimes.com/articleshow/53195586.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[42] Telecom Regulatory Authority of India, 'Consultation Paper on Proliferation of Broadband through Public Wi-Fi Networks' July 13, 2016, https://www.mygov.in/sites/default/files/mygov_1468492162190667.pdf

(V) Public Wi-Fi and Privacy concerns

Since proliferation of public Wi-Fi in India is happening at a moderate pace, the paper discusses key issues towards this, one of them being the logistics of deploying this service. This section briefly states and acknowledges privacy and security concerns as an important factor that may be posing issues in the adoption of public Wi-Fi services in the country. Since there have been numerous cases of security vulnerabilities in public Wi-Fi networks worldwide, security of networks and cyber crimes is a key issue for consideration.[43]

Deployment of public wireless access points has made it more convenient for people to access the Internet outside of their offices or homes. Despite advantages like ease of accessibility, connectivity and convenience, public Wi-Fi connection pose serious concerns as well. "The proliferation of public Wi-Fi is one of the biggest threats to consumer data", says David Kennedy, founder of TrustedSec, a specialised information security consulting company based in the United States of America.[44] Also, the networks become an easier target with little public awareness about the existence of such threats wherein users expose valuable personal data over Wi-Fi hotspots. The recently released Norton Cyber Security Report 2016[45] shows how the benefit of constant connectivity is often outweighed by consumer complacency, leaving consumers and their Wi-Fi networks at risk. For the purpose of this report, Norton surveyed 20,000 people (over a 1,000 from India) which reflects that though users in India may be increasingly becoming aware of the cyber threats they face due to use of public Wi-Fi, they don't fully understand the accompanying risks and their online behaviour is often contradictory.[46] Also, it is important to consider that the services which claim to be free, actually generate revenue by advertisements, where the model works by providing free access to internet in exchange for user's' personal and behavioral data, which is subsequently used to target ads to them.[47]

Some of the privacy harms stemming from use of public Wi-Fi are listed below :

1. Data Theft

[43]Mint, 'Trai issues paper on public Wi-Fi networks' July 14, 2016, http://www.livemint.com/Industry/1jVgso2R2Lz4NR5IYFaCtN/Trai-issues-paper-on-public-WiFi-networks.html
[44]Forbes,'How To Avoid Data Theft When Using Public Wi-Fi', March 4, 2014, http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers-love-public-wi-fi-but-you-can-make-it-safe/#373c75e32476
[45]Symantec, 'Norton Cyber Security Insights Report', 2016, https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf
[46]The Indian Express, 'Indian cybercrime victims don't learn from past experience: Norton Report', November 18, 2016, http://indianexpress.com/article/technology/tech-news-technology/indian-users-complacent-when-it-comes-to-cyber-security-norton-report/
[47]Mashable, 'This is the real price you pay for 'free' public Wi-Fi', January 26, 2016, http://mashable.com/2016/01/25/actual-cost-free-Wi-Fi/?utm_cid=mash-com-Tw-main-link#WmAJGJ_COiq5

With hackers finding it easy to access personal information of the data subjects, data can be hijacked by unauthorized internet access by spoofing the MAC and IP addresses of the authenticated user's device or by use of default settings (saved passwords or IPs).[48] The following kinds of data is at a risk of being stolen and further misused:

- demographic and locational data[49]
- forms of personal information acting as identifiers like financial information, social and personal information[50]
- private information like passwords to social networking sites, email accounts and banking websites[51]
- historical data from the devices[52]

2. Tracking an individual

Like cell phones, Wi-Fi devices have unique identifiers that can be used for tracking purposes which can cause potential security issues. Tracking by using a Wi-Fi hotspot can also lead to third party harms like stalking.[53] To receive or use a service, often websites require the user to share their personal information such as name, age, ZIP code, or personal preferences, which is many times shared with advertisers and other third parties, without the knowledge or consent of the users.[54]

3. Makes the electronic devices prone to hacking and setting up fake networks

A recent experiment conducted by the chief scientist at mobile security firm Appknox at the Bengaluru International Airport, India, found that the wireless devices could be easily hacked over the airport's free Wi-Fi network due to the easily exploitable security holes in the software made by Apple, Google, and Microsoft.[55] A similar experiment was backed by the European law

[48]MojoNetworks, 'Complying with DoT Regulation on Secure Use of WiFi: Less in Letter, More in Spirit', http://www.mojonetworks.com/fileadmin/pdf/Implementing_DoT_Regulation_on_WiFi_Security.pdf
[49]Network Computing, 'Public WiFi, Location Data & Privacy Anxiety', July 4, 2015, http://www.networkcomputing.com/wireless/public-wifi-location-data-privacy-anxiety/1496375374
[50]Network Computing, 'Public WiFi, Location Data & Privacy Anxiety', July 4, 2015, http://www.networkcomputing.com/wireless/public-wifi-location-data-privacy-anxiety/1496375374
[51]The Indian Express, 'Public Wifi can be used to steal private information: IT Security Expert', May 19, 2015, http://indianexpress.com/article/technology/technology-others/public-wifi-can-be-used-to-steal-private-information-it-security-expert/#sthash.xiuWtL6v.dpuf
[52]Medium, 'Maybe Better If You Don't Read This Story on Public WiFi', October 14, 2014, https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6#.3061h6lsv
[53]Network Computing, 'Public WiFi, Location Data & Privacy Anxiety', July 4, 2015, http://www.networkcomputing.com/wireless/public-wifi-location-data-privacy-anxiety/1496375374
[54]University of Washington, Computer Science and Engineering, 'When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use', https://djw.cs.washington.edu/papers/wifi-CHI09.pdf
[55]Breitbart, 'Fre Public Wi-Fi poses security risks', May 19, 2015, http://www.breitbart.com/big-government/2015/05/19/free-public-wifi-poses-security-risk/

enforcement agency, Europol, where a mobile hotspot was created in central London[56] and the hacker was able to gain access to passwords, apps, and even credit card and banking information with ease.[57] Lack of secure softwares and prevalence of open, unprotected Wi-Fi has made it fairly easy for hackers to set up fake twin access points that give them access to data histories and personal information.[58] This makes is easy to track data histories of users. Even if certain softwares use encryption codes, a simple decryption software can be used to obtain the information.[59]

4. Illegal use of data

- By authorities - the authorities have easier access to people's browsing details and habits, and with justification in the name of national security, could be used to monitor the people without their consent.[60]
- Wi-Fi provider - can sell the user's demographic and location information. [61] Also, it was revealed in a study that the personal information of users is often transmitted by service providers without encryption. Anyone along the path between the user and the service's data center can then intercept this information, opening users to grave privacy and security risks.[62]
- By hackers - steal information and hack into unsuspecting victim's bank accounts and misuse corporate financial information and secrets[63]

(VI) Ranking Digital Rights project

The "Ranking Digital Rights" project, an ongoing international non-profit research initiative, aims to promote greater respect for freedom of expression and privacy by focusing on the policies and practices of companies in the information communications technology (ICT)

[56]The Guardian, 'Londoners give up eldest children in public Wi-Fi security horror show', September 29, 2014, https://www.theguardian.com/technology/2014/sep/29/londoners-Wi-Fi-security-herod-clause
[57] Medium, 'Maybe Better If You Don't Read This Story on Public WiFi', October 14, 2014, https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6#.3061h6lsv
[58]ABC13, 'Hackers set up fake Wi-Fi hotspots to steal your information, July 10, 2015, http://abc13.com/technology/hackers-set-up-fake-Wi-Fi-hotspots-to-steal-your-information/835223/
[59]Medium, 'Maybe Better If You Don't Read This Story on Public WiFi', October 14, 2014, https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6#.3061h6lsv
[60] Scroll, 'Free wifi in Delhi is good news but here is the catch' November 21, 2014, http://scroll.in/article/690755/free-wifi-in-delhi-is-good-news-but-here-is-the-catch
[61] Scroll, 'Free wifi in Delhi is good news but here is the catch' November 21, 2014, http://scroll.in/article/690755/free-wifi-in-delhi-is-good-news-but-here-is-the-catch
[62]University of Washington, Computer Science and Engineering, 'When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use', https://djw.cs.washington.edu/papers/wifi-CHI09.pdf
[63] Breitbart, 'Fre Public Wi-Fi poses security risks', May 19, 2015, http://www.breitbart.com/big-government/2015/05/19/free-public-wifi-poses-security-risk/

sector[64], rank such companies in this light, and undertake research to develop the ranking methodology.[65]

In November 2015, the Ranking Digital Rights project launched the Corporate Accountability Index. Since several actors like the Internet and telecommunications companies, software producers, and device and networking equipment manufacturers exert growing influence over the political and civil lives of people all over the world, it is important to state that these organisations share a responsibility to respect human rights. For this purpose, 16 Internet and telecommunications companies were evaluated according to 31 indicators, which focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy.[66]

The data produced by the index can help companies improve their policies, practices and help them identify challenges faced by companies in meeting their corporate obligations to respect human rights like Freedom of Expression and Privacy in the digital space.[67] Some of the key corporate practices which affect these rights are :

- How companies handle government requests to hand over user data or restrict content;
- How companies enforce their own terms of service;
- What information companies collect about users and how long they retain it; and
- To whom they share or sell user information.[68]

The 2015 Corporate Accountability Index assesses transparency levels of the World's most powerful Internet and telecommunications companies regarding their commitments, policies and practices that affect users' freedom of expression and privacy and evaluates what companies share about these practices and offers recommendations for improvement. The methodology adopted relies on publicly available information so that advocates, researchers, journalists, policy makers, investors, and users can understand the extent to which different companies respect freedom of expression and privacy, and make appropriate policy, investment, and advocacy decisions. Also, public disclosures would enable researchers and journalists to investigate and verify the accuracy of company statements.[69]

For the purpose of this research, we would apply this index and the indicators to the internet service provider of public Wi-Fi in Bangalore-D-VoiS Ltd. and Tata Docomo to understand how comprehensive their privacy policies are when compared to global standards and make informed recommendations. Analysing policies against the index can help these companies identify best

[64] Ranking Digital Rights, https://rankingdigitalrights.org/who/frequently-asked-questions/
[65] Business & Human Rights Resource Centre, 'Ranking Digital Rights Project', http://business-humanrights.org/en/documents/ranking-digital-rights-project
[66] Ranking Digital Rights, https://rankingdigitalrights.org/about/
[67] Ranking Digital Rights, https://rankingdigitalrights.org/about/
[68] Ranking Digital Rights, https://rankingdigitalrights.org/who/frequently-asked-questions/
[69] Ranking Digital Rights, https://rankingdigitalrights.org/who/frequently-asked-questions/

practices, as well as the obstacles they face in meeting their corporate obligations to respect human rights in the very digital spheres they helped to create.[70] The information has been gathered and analysed on the basis of publicly available information, and this can help companies empower users to make informed decisions about how they use technology, which would help build trust between users and companies in the long run.[71]

- **D-VoIS, Bangalore[72]**

For the purpose of this case study, the Privacy Policies of D-VoIS have been analysed on the basis of the Corporate Accountability index, and the answers can be accessed in Annex 1.

Summary : On the basis of the indicators and the information available, it can be ascertained that:

- The Company has a freely available and understandable Privacy Policy and Terms of Use, though only in the English language.
- The company does not commit to notify users in case of changes in the privacy policy of the company.
- The company states circumstances in which it would restrict use of its services, along with reasons for content restriction.
- The Company commits to the principle of data minimization, discloses circumstances when it shares information with third parties, and provides users with options to control the company's collection and sharing of their information
- Deploys industry standards for security of products and services

Analysis-

Commitment

D-VoIS fares low on Commitment since it has made no overarching public commitments to protect users' freedom of expression or privacy in a manner that meets the Index's criteria. The Company lacks adequate top-level policy commitments to users' freedom of expression and privacy, establishing executive and management oversight over these issues, creating a process for human rights impact assessment, and lacks stakeholder engagement and a grievance mechanism.

Freedom of Expression

[70] Ranking Digital Rights, https://rankingdigitalrights.org/about/
[71] Ranking Digital Rights, https://rankingdigitalrights.org/who/frequently-asked-questions/
[72] D-VoIS Communication Pvt. Ltd. http://www.dvois.com/

The Company also fares low on Freedom of Expression as the terms of services, though easily available, are only in English language. Also, it does not commit to notify users about changes to the terms of service. While the company discloses what content and activities it prohibits , it provides no information about how the company notifies these restrictions to the users.
Regarding transparency about content restriction requests, since the Indian law prevents the company from disclosing government requests for content removal[73], but it does not prevent the company from publishing more information about private requests for content restriction. D-VoIS does not provide any information with respect to this.

Privacy
D-VoIS is required by law to have a privacy policy available on its website, this policy is available in English, but not in other languages spoken in India. Also, D-VoIS does not disclose what user information is collected, how and why, nor does it offer users meaningful access to their information. D-VoIS does not disclose any information regarding retention of user information, and the company could improve its disclosures about what user information it collects and how long it is retained.
Though the company discloses information about its security practices, it does not disclose any information regarding its efforts to educate users about security threats. It also does not disclose information regarding requests by non-governmental entities for user data.

- **Tata Docomo, Bangalore[74]**

The Privacy Policy and Terms & Conditions of Tata Docomo have been analysed on the basis of the Corporate Accountability index, and the answers can be accessed in Annex 2.
Summary : On the basis of the indicators and the information available, it can be ascertained that:

- The Company has a freely available and understandable Data Privacy Policy and Terms of Use, though only in English language.
- The Company has established electronic and administrative safeguards designed to secure the information collected to prevent unauthorized access to or disclosure of that information and to ensure it is used appropriately.
- The company states circumstances in which it would restrict use of its services, along with reasons for content restriction. The company's disclosed policies and practices demonstrate how it works to avoid contributing to actions that may interfere with the right to freedom of expression, except where such actions are lawful, proportionate and for a justifiable purpose.

[73]Section 16 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 states that all request and complaints must be kept confidential.
[74] Tata Docomo, http://www.tatadocomo.com/

- The Company clearly states the kind of information collected, ways of collection and the reasons for collection as well as sharing.
- Deploys industry standards for security of products and services

Analysis-

Commitment

Tata Docomo fares low on Commitment since it has made no overarching public commitments to protect users' freedom of expression or privacy in a manner that meets the Index's criteria. Though the Company has established electronic and administrative safeguards designed to secure the information collected, it lacks adequate top-level policy commitments to users' freedom of expression and privacy, establishing executive and management oversight over these issues, creating a process for human rights impact assessment, and lack of stakeholder engagement.

Freedom of Expression

The Company fares low on Freedom of Expression as the terms of services, though easily available, are only in English language. Also, it does not commit to notify users about changes to the terms of service. While the company discloses what content and activities it prohibits , it provides no information about how the company notifies these restrictions to the users.

Regarding transparency about content restriction requests, since the Indian law prevents the company from disclosing government requests for content removal, it does not prevent the company from publishing more information about private requests for content restriction. Tata Docomo does not provide any information with respect to that.

Privacy

Tata Docomo is required by law to have a privacy policy available on its website, this policy is available in English, but not in other languages spoken in India. No information is publically available regarding users option to control company's collection of information. Tata Docomo discloses that user information shall be retained as long as required and does not mention a specific duration for the same. Though the company discloses information about its security practices, it does not disclose any information regarding its efforts to educate users about security threats. It also does not disclose information regarding requests by non-governmental entities for user data.

(VII) Compliance of Privacy Policies with Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

The Privacy Policy and Terms & Conditions of D-VoIS and Tata Docomo have been analysed on the basis of the security measures and procedures stated under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 to ascertain how sound and compliant the framework is with the existing data protection regime in India. The comparison can be accessed in Annex 3.

Comparing the requirements listed under the Rules with the policies of both the companies, it can be said that though the websites of both companies provide privacy policies and are easily accessible, they lack crucial information regarding consent of the user before collection as well as sharing of information. Also, though the policies state the purpose of sharing such data with third parties, it does not state the purpose of collection of the information. The policies are also silent regarding the requirements to be complied with before transferring personal data into another jurisdiction . There is also no information about the companies having a grievance officer. Additionally, though the terms of services of D-VoIS state that the customer may choose to restrict the collection or use of their personal information, both companies do not specifically provide for an opt out mechanism to its users.

(VIII) Conclusion and Recommendations:

To allay the numerous concerns regarding privacy and security with respect to public Wi-Fi's, the ISPs must have a sound Privacy Policy in place. For this purpose, adherence to the indicators as listed under the Corporate Accountability Index, along with requirements for security of personal information stated under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and improving the policies accordingly shall greatly contribute to protection of Freedom of Expression and ensure Privacy of user information. Ensuring compliance with the existing data protection regime in the country becomes more important in light of the growing privacy and security concerns due to proliferation of free and public Wi-Fi service in India. Adequate measures like acquiring consent for collection and sharing of user data, commitment by company executives to ensure protection of rights of individuals, adoption of security standards, creating awareness about security concerns, etc. by such corporate must be considered to ensure protection of personal information and reduce the likelihood of a data breach. Both D-VoIS and Tata Docomo must consider the following recommendations in order to meet the criteria set by the Ranking Digital Rights project, ensuring commitment towards protection of right to freedom of expression and privacy of the users:

- Commitment

- Set in place an oversight mechanism to monitor how the company's policies and practices affect freedom of expression and privacy. In case the Company already has that in place, information regarding the same must be made publically available for greater transparency.
- Also, they must conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of their business impact freedom of expression and privacy.
- In addition to that, they must Provide for a remedy or grievance mechanism. The Telecom Regulatory Authority of India also requires that all service providers have redress mechanisms. In case the Company already has that in place, information regarding the same must be made publically available for greater transparency.

- Freedom of Expression

- The Companies must make an effort to make the Terms of Service available in the most commonly spoken languages by its users, besides English.
- Also, it is recommended that the Companies must ensure to provide meaningful notice to users regarding change in terms of service.
- Besides disclosing what content and activities the companies prohibit, they must disclose information regarding how it enforces these prohibitions and should provide examples regarding the circumstances under which it may suspend service to individuals or areas to help users understand such policies.
- The Companies must also disclose information regarding the process for evaluating and responding to requests from third parties to restrict content or service. Additionally, it must disclose how long it retains user information, publish process for evaluating and responding to requests from government and other third parties for stored user data and/or real-time communications.

- Privacy

- Though both the Companies disclose that the user information shall be shared with third parties, and Tata Docomo discloses what information is collected and how, yet there should be no legal impediment for the companies to improve its disclosures about what user information it collects, with whom it is shared, and how long it is retained to protect the privacy of the users.
- Though Tata Docomo allows the users to review and correct their Personal Information collected by the Company, D-VoIS must release information regarding whether the users are able to view, download or otherwise obtain all of the information about them that the company holds. In case it does not allow, the Company must duly change its policy regarding the same.
- The Companies must also publish information to help users defend against cyber threats.