A Study of the Privacy Policies of Indian Service Providers and the 43A Rules

Contents

Executive Summary

India has one of the largest telecom subscriber base in the world, currently estimated at 898 Million users.[1] With over 164.8 Million people accessing the internet[2] in the subcontinent as well, technology has concurrently improved to facilitate such access on mobile devices. In fact, the high penetration rate of the internet in the market can be largely attributed to mobile phones, via which over 80% of the Indian population access the medium.[3]

While this is a positive change, concerns now loom over the expansive access that service providers have to the information of their subscribers. For the subscriber, a company's commitment to protect user information is most clearly defined via a privacy policy. Data protection in India is broadly governed by Rules notified under Section 43A of the Information Technology Act 2000.[4] Amongst other things, the Rules define requirements and safeguards that every Body Corporate is legally required to incorporate into a privacy policy.

The objective of this research is to understand what standards of protection service providers in India are committing to via organizational privacy policies. Furthermore, the research seeks to understand if the standards committed to via organizational privacy policies align with the safeguards mandated in the 43A Rules. Towards this, the research reviews the publicly available privacy policies from seven different service providers - Airtel, Aircel, Vodafone, MTNL, BSNL, ACT, and Tata Teleservices.

The research finds that only Airtel, Vodafone, and Tata Teleservices fully incorporate the safeguards defined in the 43A Rules. Aircel, and ACT incorporate a number of such safeguards though not all. On the other hand BSNL minimally incorporates the safeguards, while MTNL does not provide a privacy policy that is publicly available.

Introduction

The Indian Telecom Services Performance Indicators report by the Telecom Regulatory Authority of India (TRAI)[5] pegs the total number of internet subscribers in India at 164.81 million and the total number of telecom subscribers at 898.02 million, as of March 2013. As mobile phones are adopted more widely, by both rural and urban populations, there is an

1. Telecom Regulatory Authority of India, Press Release 143/2012,(<http://www.trai.gov.in/WriteReadData/PressRealease/Document/PR-TSD-May12.pdf>)
2. The Indian Telecom Service Performance Indicators, January-March 2013, Telecom Regulatory Authority of India,. (<http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Indicator%20Reports%20-01082013.pdf>)
3. 'India is now world's third largest Internet user after U.S., China', (The Hindu, 24 August 2013) <http://www.thehindu.com/sci-tech/technology/internet/india-is-now-worlds-third-largest-internet-user-after-us-china/article5053115.ece>
4. In addition, the Unified Access License Framework which allows for a single license for multiple services such as telecom, the internet and television, provides certain security guidelines. As per the model UIL Agreements, privacy of communications is to be maintained 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. For internet services, the Agreement stipulates the keeping an Internet Protocol Detail Record (IPDR) and copies of packets from customer premises equipment (CPE). Accessed at <http://www.dot.gov.in/sites/default/files/Unified%20Licence.pdf>
5. See >> http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Indicator%20Reports%20-01082013.pdf >>

amalgamation of telecommunications and internet users. Thus, in India, seven out of eight internet users gain access through mobiles phones.[6]

Though this rapid evolution of technology allows greater ease of access to digital communication, it also has led to an increase in the amount of personal information that is shared on the internet. Subsequently, a number of privacy concerns have been raised with respect to how service providers handle and protect and customer data as companies rely on this data not only to provide products and services, but also as a profitable commodity in and of itself. Individuals are thus forced to confront the possible violation of their personal information, which is collected as a *quid pro quo* by service providers for access to their services and products. In this context, protection of personal information, or data protection, is a core principle of the right to privacy.

In India, the right to privacy has been developed in a piecemeal manner through judicial intervention, and is recognized, to a limited extent, as falling under the larger ambit of the fundamental rights enshrined under Part III of the Constitution of India, specifically those under Article 21.[7] In contrast, historically in India there has been limited legislative interest expressed by the Government and the citizens towards establishing a statutory and comprehensive privacy regime. Following this trend, the Information Technology Act, 2000 (IT Act), as amended in 2008, provided for a limited data protection regime.

However, this changed in 2010 when, concerned about India's robust growth in the fields of IT industry and outsourcing business, an 'adequacy assessment' was commissioned by the European Union (EU), at the behest of India, which found that India did not have adequate personal data protection regime.[8] The main Indian legislation on the personal data security is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules), enacted under Section 43A of the IT Act, which extends the civil remedy by way of compensation in case wrongful loss or gain under Section 43A to cases where such loss or gain results from inadequate security practices and procedures while dealing with sensitive personal data or information. In 2012, the Justice AP Shah group of Experts was set up to review and comment on Privacy,[9] for the purpose of making recommendations which the government may consider while formulating the proposed framework for the Privacy Act.

Objective, Methodology, and Scope of the Study

6. 'India is now world's third largest Internet user after U.S., China', (The Hindu, 24 August 2013) <http://www.thehindu.com/sci-tech/technology/internet/india-is-now-worlds-third-largest-internet-user-after-us-china/article5053115.ece> Accessed..
7. Starting with *Kharak Singh* v. *State of UP* 1963 AIR SC 1295, the right to privacy has been further confirmed and commented on in other cases, like *Govind v.State of M.P* (1975) 2 SCC 148: 1975 SCC (Cri) 468. A full history of the development of the Right to Privacy can be found in B.D. Agarwala, *Right to Privacy: A Case-By-Case Development*, (1996) 3 SCC (Jour) 9, available at http://www.ebc-india.com/lawyer/articles/96v3a2.htm.
8. White Paper on EU Adequacy Assessment of India, 3, ("*Based on an overall analysis against the identifiable principles under Article 25, the 2010 Report concludes that India does not at present provide adequate protection to personal data in relation to any sector or to the whole of its private sector or to the whole of its public sector.*") available at <https://www.dsci.in/sites/default/files/WhitePaper%20EU_Adequacy%20Assessment%20of%20India.pdf>
9. Planning Commission, *Report of the Group of Experts on Privacy*, 2012, (<http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf>)

Objective of Research

This research aims to analyse the Privacy Policies of the selected Telecommunications (TSP) and Internet Service Providers (ISP) (collectively referred to as 'service providers' for the purposes of this research) in the context of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ('Rules') in order to gain perspective on the extent to which the privacy policies of different types of service providers in India, align with the Rules. Lastly, this research seeks to provide broad recommendations about changes that could be incorporated to harmonize the respective policies and to bring them in line with the aforementioned Rules.

Methodology

The Privacy Policies[10] of seven identified service providers are sought to be compared vis-a-vis – the requirements under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, (Rules) as notified by way of section 87(2) (ob) read with section 43A of the Information Technology Act, 2000.

Specifically, the Privacy Policies of each of the selected companies are compared against a template that is based on of the essential principles of the Rules respectively, and consists of a series of yes or no questions which are answered on the basis of the respective Privacy Policy. These responses are meant to fulfil the first aim of this research, i.e., provide a perspective into the extent to which these companies follow the Rules and the Principles, and thus the extent to which they respect the privacy of their customers. See Annex 1 for the survey template and the interpretation of the 43A Rules for the development of the survey.

Scope

Criteria for selection of companies being studied

For the purpose of the study the companies selected are limited to service providers – including Telecommunication Service Providers and Internet Service Providers. Four broad categories of companies have been selected, namely (i) State Owned Companies, (ii) Multinational Companies, (iii) Joint Venture companies where one party is an Indian company and the other party is a foreign based company and (iv) Domestic companies which have a localized user base. The companies have been selected on this basis of categorization to better understand if the quality of their respective privacy policies is determined by their market reach and user base.

The privacy policies of the following service providers have been analyzed:

1. State Owned Companies[11]

10. Though a company's Privacy Policy was the main document analysed for this research, when applicable a company's Terms of Service wavas also reviewed.
11. BSNL and MTNL are government companies as defined under section 617, Indian Companies Act, 1956, incorporated under the Indian Companies Act, 1956. Under section 43 A (i) of the Act, a 'body corporate' has been broadly defined as "any company…sole proprietorship or other association of individuals engaged in commercial or professional activities". Therefore, for the purpose of this survey, BSNL and MTNL are recognized as bodies corporate.

a. **BSNL[12]:** Bharat Sanchar Nigam Limited, better known as BSNL, is a state-owned telecommunications company that was incorporated by the Indian government in the year 2000, taking over the functions of Central Government departments of Telecommunications Services (DTS) and Telecom Operations (DTO). It provides, *inter alia*, landline, mobile, and broadband services, and is India's oldest and largest communication services provider.[13] It had a monopoly in India except for Mumbai and New Delhi till 1992.
b. **MTNL[14]:** Mahanagar Telephone Nigam Limited is a state-owned telecommunications company which provides its services in Mumbai and New-Delhi in India, and Mauritius in Africa. It was set up by the Indian Government in the year 1986, and just like BSNL, it had a monopoly in the sector till 1992, when it was opened up to other competitors by the Indian government. It provides, *inter alia*, Telephone, Mobile, 3G, and Broadband services.[15]

2. Multinational Companies

a. **Bharti Airtel Ltd:[16]** Bharti Airtel, more commonly referred to as Airtel, is the largest provider of mobile telephony and the second largest provider of fixed telephony in India. Its origins lie in the Bharti Group founded by Sunil Bharti Mittal in 1983, and the Bharti Telecom Group which was incorporated in 1986. It is a multinational company, providing services in South Asia, Africa, and the Channel Islands. Among other services, it offers fixed line, cellular, and broadband services.[17] The company also owns a submarine cable landing station in Chennai, connecting Chennai and Singapore.[18]
b. **Vodafone**[19]**:** Vodafone is a British multinational telecom company. Its origins lie in the establishment of Racal Telecom in 1982 which then became Racal Vodafone in 1984, which was a joint venture between Racal, Vodafone and Hambros Technology Trust. Racal Telecom was demerged from Racal Electronics in 1991, and became the Vodafone group. [20] The Vodafone group started its operations in India with its predecessor Hutchison Telecom, which was a joint venture of Hutchison Whampoa and the Max Group, acquiring the cellular license for Mumbai in 1994[21], and it bought out Essar's share in the same in the year 2007.[22] As of today, it has the second largest

---

12. Documents Reviewed*:* http://portal.bsnl.in/portal/privacypolicy.html
13. A full list of its services are available here: <http://bsnl.co.in/opencms/bsnl/BSNL/services/>
14. The MTNL website does not provide access to a privacy policy
15. A full list of its services are available here <<http://mtnldelhi.in>>
16. Documents Reviewed: http://www.airtel.in/forme/privacy-policy , http://www.airtel.in/applications/xm/FixedLineNodalOfficer.jsp, http://www.airtel.in/applications/xm/BroadbandInternet_AppellateAuth.jsp, http://www.airtel.in/about-bharti/about-bharti-airtel/ombuds-office
17. A full list of services provided by Bharti Airtel is available here: <www.airtel.in>
18. http://submarinenetworks.com/stations/asia/india/chennai-bharti
19. Documents Reviewed:http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html https://www.vodafone.in/pages/privacy_policy.aspx?cid=ker, http://www.vodafone.com/content/sustainability/operating_responsibly/privacy_and_security.html
20. See <http://historyofbusiness.blogspot.in/2013/11/history-of-vodafone.html.>
21. *Vodafone International Holdings v Union of India*, WP 1325/2010, Bombay High Court
22. 'Vodafone to Buy Additional Essar India Stake for $5 Billion',(*Bloomberg*, March 31, 2011) <http://www.bloomberg.com/news/2011-03-31/essar-exercises-option-to-sell-5-billion-stake-in-vodafone-essar-venture.html>Accessed 26 May 2014

subscriber base in India. After Airtel,[23] Vodafone is the largest provider of telecommunications and mobile internet services in India.[24]

3. Joint Ventures

a. **Tata Teleservices[25]** – Incorporated in 1996, Tata Teleservices Limited is an Indian telecommunications and broadband company, the origins of which lie in the Tata Group. A twenty-six percent equity stake was acquired by the Japanese company NTT Docomo in Tata Docomo, a subsidiary of Tata Teleservices, in 2008.[26] Tata Teleservices provides services under three brand names, Tata DoCoMo, Virgin Mobile, and T24 Mobile. As a whole, these brands under the head of Tata Teleservices provide cellular and mobile internet services, with the exception of the Tata Sky teleservices brand, which is a joint venture between and Tata Group and Sky. [27]

b. **Aircel[28]:** Aircel is an Indian mobile headquarter, which was started in Tamil Nadu in the year 1999, and has now expanded to Tamil Nadu, Assam, North-east India and Chennai. It was acquired by Maxis Communication Berhard in the year 2006, and is currently a joint venture with Sindya Securities & Investments Pvt. Ltd. [29] Aircel provides telecommunications and mobile internet services in the aforementioned regions.

4. India based Companies/Domestic Companies –

a. **Atria Convergence Technologies (ACT)[30]:** Atria Convergence Technologies Pvt. Ltd is an Indian cable television and broadband services company. Funded by the India Value Fund Advisor (IVFA), it is centered in Bangalore, but also provides services in Karnataka, Andhra Pradesh, and Madhya Pradesh.

Overview of Company Privacy Policy and Survey Results

This section lays out the ways in which each company's privacy policy aligns with the Rules found under section 43A of the Information Technology Act. The section is organized based on company and provides both a table with the survey questions and yes/no/partial ratings and summaries of each policy. The rationale and supporting documentation for each determination can be found in ANNEX II.

VODAFONE[31]: 43A Rules Survey

23. See <https://www.vodafone.in/pages/aboutus.aspx?cid=ker.>
24. Vodafone, *supra* note 13.
25. Documents Reviewed: http://www.tatadocomo.com/downloads/data-privacy-policy.pdf, http://www.tatateleservices.com/t-customercare.aspx, http://www.tatateleservices.com/download/aboutus/ttml/TTML-Annual-Report-2012-13.pdf
26. 'Japan's Docomo acquires 26% stake in Tata Tele'(The Hindu Business Line, November 13 2008) <http://www.thehindubusinessline.in/bline/2008/11/13/stories/2008111352410100.htm.>
27. Further details are available at: <http://www.tatateleservices.com/t-aboutus-ttsl-organization.aspx>
28. Documents Reviewed http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P26400194591312373872061, http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=customercare_consumergrievance_page, http://www.aircel.com/AircelWar/ShowProperty/UCMRepository/Contribution%20Folders/Global/PDF/Manual_Customer_Grievan.pdf
29. See <http://www.aircel.com/AircelWar/appmanager/aircel/ap?_nfpb=true&_pageLabel=aboutus_book.>
31. https://www.vodafone.in/pages/privacy_policy.aspx?cid=ker

Criteria	Yes/No
Clear and Accessible statements of its practices and policies	
Whether the privacy policy is accessible through the main website of the body corporate?	Yes
Whether the privacy policy is mentioned or included in the terms and conditions of publicly available documents of the body corporate that collect personal information?	No
Whether the privacy policy can be comprehended by persons without legal knowledge?	Yes
Collection of personal or sensitive personal data/information	
Type	
Whether the privacy policy mentions all categories of personal information including SPD/I being collected?	Partially
Whether the privacy policy explicitly specifies the type of SPD/I being collected?	Partially
Option	
Whether the Privacy Policy specifies that the user has the option to not provide information?	No
Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?	No
Grievance Officer	
Whether the privacy policy mentions the existence of a grievance officer?	Yes
Whether the privacy policy provides the contact information of the grievance officer	Yes
Purpose of Collection and usage of information	
Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?	Yes
Disclosure of Information	
Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties	Yes
Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?	Yes
Reasonable Security practices and procedures	
Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?	Yes

Vodafone

Vodafone's privacy policy partially incorporates the safeguards found in the Rules under 43A.

31. https://www.vodafone.in/pages/privacy_policy.aspx?cid=ker

Vodafone's privacy policy is accessible online, however, it does not include a copy of its policy with a customer application form. The policy merely lists the type of information collected with no categorization as to SPD/I. The information collected includes contact information, location based information, browsing activity and persistent cookies.

There is no provision for consent or choice within the policy. Disclosure of personal information to third parties extends to Vodafone's group companies, companies that provide services to Vodafone, credit reference agencies and directories.

The policy mentions an email address for grievance redressal. In addition, the policy does not lay down any mechanism for correcting personal information that is held with Vodafone.

Vodafone has a non-exhaustive list of purposes of information usage, though these primarily relate to subscriber services, personnel training, and legal or regulatory requirements.

With regard to security practices, Vodafone follows the ISO 27001 Certification as per its 2012 Sustainability Report, however this goes unmentioned under its privacy policy

Tata Teleservices Limited[32]: 43A Rules Survey	
Criteria	**Yes/No**
Clear and Accessible statements of its practices and policies	
Whether the privacy policy is accessible through the main website of the body corporate?	Yes
Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?	No
Whether the privacy policy can be comprehended by persons without legal knowledge?	Yes
Collection of personal or sensitive personal data/information	
Type	
Whether the privacy policy mentions all categories of personal information including SPD/I being collected?	Yes
Whether the privacy policy explicitly specifies the type of SPD/I being collected?	Yes
Option	
Whether the Privacy Policy specifies that the user has the option to not provide information?	No
Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?	No
Grievance Officer	
Whether the privacy policy mentions the existence of a grievance officer?	No
Whether the privacy policy provides the contact information of the grievance officer?	No
Purpose of Collection and usage of information	

32. http://www.tatadocomo.com/downloads/data-privacy-policy.pdf

Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?	Yes
Disclosure of Information	
Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties	Yes
Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?	Yes
Reasonable Security practices and procedures	
Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?	Yes

Tata Teleservices Limited

Tata Teleservices Limited's Privacy Policy fully incorporates the safeguards found in the Rules under 43A.
The Tata Teleservices Limited privacy policy is accessible on their website, though when applying for a subscription, the terms and conditions do not include the privacy policy. The privacy policy is easy to understand although there are several elements of the 2011 Rules that are unaddressed.

The policy does not make any distinction regarding sensitive personal data or information. As per the policy, TTL collects contact and billing information, information about the equipment the subscriber is using, and information and website usage from its customers.

The purposes of information collection are broadly for managing customer services and providing customized advertising. Information is also collected for security issues, illegal acts and acts that are violative of TTL's policy. TTL's directory services use a customer's name, address and phone number, however a customer may ask for his/her information to not be published on payment of a fee.

As per the policy, the disclosure of information to third parties is limited to purposes such as identity verification, bill payments, prevention of identity theft and the performance of TTL's services. Third parties are meant to follow the guidelines of TTL's privacy policy in the protection of its user information. The consent of subscribers is only required when third parties may use personal information for marketing purposes. Consent is precluded under the previous conditions. Disclosure of information to governmental agencies and credit bureaus is for complying with legally authorised requests such as subpoenas, court orders and the enforcement of certain rights or claims. The policy provides for a grievance officer and in addition, TTL, has a separate Appellate Authority to deal with consumer complaints.

TTL does not follow any particular security standard for the protection of subscriber information, however, it establishes other measures such as limited access to employees, and encryption and other security controls. Although TTL Maharashtra follows the ISO 27001 ISMS Certification, TTL does not seem to follow a security standard for data protection for other regions of its operations.

Airtel[33]: 43A Rules Survey	
Criteria	**Yes/No**
Clear and Accessible statements of its practices and policies	
Whether the privacy policy is accessible through the main website of the body corporate?	Yes
Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?	Yes
Whether the privacy policy can be comprehended by persons without legal knowledge?	Yes
Collection of personal or sensitive personal data/information	
Type	
Whether the privacy policy mentions all categories of personal information including SPD/I being collected?	Yes
Whether the privacy policy explicitly specifies the type of SPD/I being collected?	Yes
Option	
Whether the Privacy Policy specifies that the user has the option to not provide information?	Yes
Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?	Yes
Grievance Officer	
Whether the privacy policy mentions the existence of a grievance officer?	Yes
Whether the privacy policy provides the name and contact information of the grievance officer?	Yes
Purpose of Collection and usage of information	
Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?	Yes
Disclosure of Information	
Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties?	Yes
Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?	Yes
Reasonable Security practices and procedures	
Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?	Yes

Airtel

Airtel's Privacy Policy fully incorporates the safeguards found in the Rules under 43A.

33. http://www.airtel.in/forme/privacy-policy

Airtel's privacy policy incorporates a number of the requirements stipulated in the Rules. Airtel's privacy policy is easily accessible on its website and is clear and easy to understand. The policy defines sensitive personal information, and states that information collected will be used for specified regulatory and business purposes, though it adds that it may be used for other purposes as well. The policy does allow for the withdrawal of consent for providing information, in which case, certain services may be withheld. In addition, Airtel has provided for a grievance officer and abides by the IS/ISO/IEC 27001 security standards. While Airtel allows for the disclosure of information including sensitive personal information to third parties, its policy states that such third parties will follow reasonable security practices in this regard. Concerning disclosure to the government, Airtel shares user information only when it is legally authorised by a government agency. Airtel's policy also provides for an opt-out provision. Such choice remains after subscription of Airtel's services as well. However, withdrawal of consent gives Airtel the right to withdraw its services as well. In terms of disclosure, sharing of user information with third parties is regulated by its Airtel's guidelines on the secrecy of information.

While Airtel lists the purposes for information collection, it states that such collection may not be limited to these purposes alone. In addition, the policy states that user's personal information will be deleted, although it does not state when this will happen. Thus, the policy could be more transparent and specific on matters of regarding the purpose of collection of information as well as deletion of information.

Aircel[34]: 43A Rules Survey	
Criteria	Yes/No
Clear and Accessible statements of its practices and policies	
Whether the privacy policy is accessible through the main website of the body corporate?	yes
Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?	no
Whether the privacy policy can be comprehended by persons without legal knowledge?	Yes
Collection of personal or sensitive personal data/information	
Type	
Whether the privacy policy mentions all categories of personal information including SPD/I being collected?	Partially
Whether the privacy policy explicitly specifies the type of SPD/I being collected?	Partially
Option	
Whether the Privacy Policy specifies that the user has the option to not provide information?	Yes

34.http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P26400194591312373872061

Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?	Yes
Grievance Officer	
Whether the privacy policy mentions the existence of a grievance officer?	Yes
Whether the privacy policy provides the contact information of the grievance officer?	Yes
Purpose of Collection and usage of information	
Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?	Partially
Disclosure of Information	
Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties	Partially
Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?	Partially
Reasonable Security practices and procedures	
Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?	Yes

Aircel

Aircel's Privacy Policy partially complies with the safeguards in the Rules under 43A.
Aircel's privacy policy is accessible online through its website, though it is not included under the terms and conditions of its customer application. The privacy policy lists the kinds of information that is collected from subscribers, including relevant contact details, call records, browsing history, cookies, web beacons, server log files and location details. The policy does not demarcate information into SPD/I or personal information. Aircel provides subscribers with the right to withdraw consent from the provision of information before and after subscribing, while reserving the right to withdraw its services in this regard. The policy provides the name and contact details of a grievance officer.

In the privacy policy, the stated purposes for use of subscriber information is limited to customer services, credit requirements, market analyses, legal and regulatory requirements, and directory services by Aircel or an authorised third party.

In the policy, the provision on disclosure to governmental agencies is vague and does not mention the circumstances under which personal information would be disclosed to law enforcement. The policy provides for correction of information of a subscriber in case of error and deletion after the purpose of the information is served but does not specify when. Although Aircel follows the ISO 27001 standard, it does not mention this under its policy. It does however, provide for accountability in cases of breach or privacy.

Atria Convergence Technologies[35]: 43A Rules Survey

35. http://www.acttv.in/index.php/privacy-policy

Criteria	Yes/No
Clear and Accessible statements of its practices and policies	
Whether the privacy policy is accessible through the main website of the body corporate?	Yes
Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?	information not available
Whether the privacy policy can be comprehended by persons without legal knowledge?	Yes
Collection of personal or sensitive personal data/information	
Type	
Whether the privacy policy mentions all categories of personal information including SPD/I being collected?	Partially
Whether the privacy policy explicitly specifies the type of SPD/I being collected?	Partially
Option	
Whether the Privacy Policy specifies that the user has the option to not provide information?	No
Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?	No
Grievance Officer	
Whether the privacy policy mentions the existence of a grievance officer?	No
Whether the privacy policy provides the contact information of the grievance officer?	No
Purpose of Collection and usage of information	
Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?	Yes
Disclosure of Information	
Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties	Yes
Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?	Partially
Reasonable Security practices and procedures	
Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?	No

Atria Convergence Technologies

Though Atria Convergence Technologies provides a privacy policy on its website, it does not broadly incorporate the safeguards in the Rules under 43A. ACT's privacy policy is easily accessible online and is easy to understand as well. The information collected from subscribers is limited to contact details along with information on whether a subscriber has transacted with

any of ACT's business partners. Though the privacy policies refers to disclosing information for the purpose of assisting with investigating, preventing, or take action on illegal behaviour - there is no specific provision concerning disclosure to government and regulatory agencies. The policy does not provide information on any security practices and procedures followed. Provisions for withdrawal of consent or correction of personal information are absent from the

BSNL: 43A Rules Survey	
Criteria	Yes/No
Clear and Accessible statements of its practices and policies	
Whether the privacy policy is accessible through the main website of the body corporate?	No
Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?	No
Whether the privacy policy can be comprehended by persons without legal knowledge?	Yes
Collection of personal or sensitive personal data/information	
Type	
Whether the privacy policy mentions all categories of personal information including SPD/I being collected?	No
Whether the privacy policy explicitly states that it is collecting SPD/I?	No
Option	
Whether the Privacy Policy specifies that the user has the option to not provide information?	No
Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?	No
Grievance Officer	
Whether the privacy policy mentions the existence of a grievance officer?	Yes
Whether the privacy policy provides the contact information of the grievance officer?	Yes
Purpose of Collection and usage of information	
Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?	Partially
Disclosure of Information	
Whether contractual provisions exist in the privacy policy or ToS addressing the disclosure of personal information with third parties	Yes
Whether personal information is disclosed to government agencies/LEA/IA only when legally mandated?	Yes
Reasonable Security practices and procedures	
Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure personal information?	No

policy as well.

BSNL

BSNL's Privacy Policy broadly does not incorporate the safeguards in the Rules under 43A.

BSNL's privacy is accessible online, though not on the website, and is easy to understand. The policy does not however, categorize SPD/I but defines personal information vaguely as information that helps BSNL identify its customers. As per its policy, subscriber information is used for subscriber services such as identification, assistance etc., credit-worthiness and marketing communications. The policy does not contain any provision on consent and with respect to marketing communications and a customer implicitly agrees to third party usage of personal information. Third parties under the policy are those that provide services on behalf of BSNL, which extend mailing and billing services and market research services.

As per its policy, BSNL may disclose personal information on the basis of legal requirements to credit organisations, BSNL's consultants, government agencies.

With respect to access and correction, BSNL reserves the right to modify its privacy policy without notice to its customers. What is presumably a grievance officer email address has been provided for queries and corrections on personal information, however no further contact details are given.

MTNL

MTNL does not provide a publicly available Privacy Policy.

Observations

This section highlights key trends observed across the privacy policies studied in this research by contrasting the applicable Rule against the applicable provision in the policy.

1. Access and Location of Privacy Policy

Applicable Rule and Principle: According to Rule 4 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, a Body Corporate must provide a privacy policy on their website. Under Rule 5, all bodies corporate have to convey the purpose(s) for which SPD/I are collected prior to the collection and they can, under certain circumstances, move forward with the collection regardless of consent. While this does not entirely violate the Notice Principle of the National Privacy Principles, it does not meet the rather higher standards of the Principle, which recommends that notice must be provided prior to any form of collection of personal information. In addition, the Rules do not contain provisions regulating bodies corporate, regarding changes to their privacy policies.[36]

36. In 2012, the Minister of State for Communications & Information Technology informed the Rajya Sabha that "*(a)ny change in the privacy policy is not within the purview of amended Information Technology Act, 2000*",, while discussing changes to Google's privacy policy. Even though the Minister noted that the EU has reported its dissatisfaction with the changed policy, finding that the policy "*makes it impossible to understand which purposes, personal data, recipients or access rights are relevant to the use of a specific service*", he argued that the Act and Rules therein merely stipulate the publication of a privacy policy which provide "*information to the end users as to how their personal information is collected, for which it is collected, processed and secure*". Further, when asked how changes to privacy policy affect end users the Minister shifted the responsibility on end users, stating that "*(t)he end users… need to fully understand the privacy policy of Google, the consequences of sharing their personal information and their privacy rights before they start using online services*".(<http://rsdebate.nic.in/bitstream/123456789/609109/2/PQ_225_30032012_U1929_p129_p130.pdf#search=%22google%22>).

Observation: In the survey, it was found that the location and accessibility of a service provider's privacy policy varied. For example:

a. **Privacy Policy on main website:** Airtel, Aircel, and Vodafone provide a privacy policy that is accessible through the main website of each respective company.
b. **Privacy Policy not on website**: MTNL does not provide a Privacy Policy on the main website of each of its respective branches across India.
c. **Privacy Policy not accessible through main website**: TTL and BSNL have a Privacy Policy, but it is not accessible through the main website. For example, The Privacy Policy found on TTL's website is only accessible through the "terms and services" link on the homepage. Similarly, the BSNL privacy policy can only be found through its portal website.[37]
d. **Privacy Policy not included in Customer Application form**: Almost all of the Service Providers do not include/refer to their Privacy Policy in the Customer Application Form, and some do not display their privacy policy or a link to it on its website's homepage. For example, Airtel is the only Service Provider that refers to their privacy policy in the Customer Application Form for an Airtel service.
e. **Collection of personal information before Privacy Policy:** In some cases it appears that service providers collect private information before the privacy policy is made accessible to the user. For example, before the homepage of ACT's website is shown, a smaller window appears with a form asking for personal information such as name, mobile and email Id. Although the submission of this information is not mandatory, there is no link provided to the privacy policy at this level of collection of information.

2. Sharing of information with Government

Applicable Rule and Principle: Rule 6, specifically the proviso to Rule 6, and the Disclosure of Information Principle respectively govern the disclosure of information to third parties. Yet, while the proviso to Rule 6 directly concerns the power of the government to access information with or without consent for investigative purposes, the Disclosure of Information Principle only says that disclosure for law enforcement purposes should be in accordance with the laws currently in force.

Observation: Though all service providers did include statements addressing the potential of sharing information with law enforcement or governmental agencies, how this was communicated varied. For example:

a.) **Listing circumstances for disclosure to law enforcement**: The Privacy Policy of ACT states *"We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person".*[38] The Privacy Policy of Airtel on the other hand states *"Government Agencies: We may also share your personal information with Government agencies or other authorized law enforcement agencies (LEAs) mandated under law to obtain such information for the purpose of verification of identity or for prevention, detection, investigation including but not*

37. Available at http://portal.bsnl.in/portal/privacypolicy.htm, the privacy policy was found through a search engine and not through a link from the website. An RTI request was submitted to BSNL for a copy of its privacy policy as applicable to all its products, services and websites. BSNL responded by submitting a copy of this privacy policy even though the text of the policy does not clarify the scope.
38. See, <http://www.acttv.in/index.php/privacy-policy>

limited to cyber incidents, prosecution, and punishment of offences."[39] Lastly, TTL states "*To investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person" or "To notify or respond to a responsible governmental entity if we reasonably believe that an emergency involving immediate danger of death or serious physical injury to any person requires or justifies disclosure without delay".*[40]

b.) Listing authorities to whom information will be disclosed to: The privacy policy of Aircel states *"There may be times when we need to disclose your personal information to third parties. If we do this, we will only disclose your information to: …8. Persons to whom we may be required to pass your information by reason of legal, governmental or regulatory authority including law enforcement agencies and emergency services".*[41] Similarly, Vodafone states *"There may be times when we need to disclose your personal information to third parties. If we do this, we will only disclose your information to persons to whom we may be required to pass your information by reason of legal, governmental or regulatory authority including law enforcement agencies and emergency services and any person or organisation as authorised by laws and regulations applicable in India."*[42] While BSNL states *"Apart from the above, BSNL may divulge your personal information to: Government bodies, Regulatory Authorities, and other organizations in accordance with the law or as authorised by law…".*[43]

3. Readability of Privacy Policies

Applicable Rule and Principle: In subsection (i) of Rule 4 body corporate must provide a privacy policy that is "*clear and accessible*". Similarly, the Notice Principle requires that the data controller give a "*simple-to-understand notice of its information practices to all individuals, in clear and concise language*".

Observation: It was found that, particularly with respect to clauses on the collection and disclosure of information, most Privacy Policies use:

a. **Vague terminology:** For example, in the Privacy Policy of ACT, it states as a purpose of collection *"conduct research"* while for the collection and disclosure of information it states*,"The Company may combine information about you that we have, with information we obtain from business partners or other companies. The Company shall have the right to pass on the same to its business associates, franchisees without referring the same to you."*[44] Similarly, with regards to the collection of information, Vodafone's Privacy Policy states that it may collect *"any other information collected in relation to your use of our products and services".*[45]

---

39. See <http://www.airtel.in/forme/privacy-policy>
40. See <www.tataindicom.com/Download/data-privacy-policy.pdf>
41. See <<www.aircel.com/AircelWar/appmanager/aircel/delhi?_nfpb=true&_pageLabel=P264001945913123 73872061>>
42. See <https://www.vodafone.in/pages/privacy_policy.aspx?cid=kar>
43. See<< http://portal.bsnl.in/portal/privacypolicy.htm>>
44. See <http://www.acttv.in/index.php/privacy-policy>
45. See <https://www.vodafone.in/pages/privacy_policy.aspx?cid=kar>

b. **Undefined terminology:** On disclosure of information TTL's privacy policy states disclosure is *"Subject to applicable legal restrictions, such as those that exist for Customer Proprietary Network Information (CPNI)"*[46] Confusingly, although TTL defines CPNI it does not mention what legal restriction it is referring to, and CPNI is in fact an American term and similar legal restrictions could not be found in India.

4. Information about security practices

Applicable Rule and Principle: The parameter for 'reasonable security practices and procedures' has been detailed comprehensively under Rule 8 of the Rules. The same is also covered in detail under the Openness Principle read with Security Principle. While the Security Principle recommends that the data controller protect the information they collect through reasonable security safeguards, the Openness Principle recommends that information regarding these should be made available to all individuals in clear and plain language.

Observation: With the exception of Airtel, no service provider has comprehensively followed the legal requirements for the purpose of their privacy policy. Thus, while most service providers do mention security practices, many do not provide specific or comprehensive details about their security practices and procedures for data protection, and instead assure users that 'reasonable security' procedures are in place. For example:

a. **Comprehensive information about security practices in privacy policy**: Airtel and Aircel have provided comprehensive information about their security practices in the companies Privacy Policy.
b. **Information about security practice, but not in privacy policy**: Vodafone has specified its security standards only in its latest 'Sustainability Report' available on its website. In the case of TTL, the specific security standard it follows is available only for its Maharashtra branch (TTLM) through its annual report.
c. **Broad reference to security practices**: Many service providers broadly reference security practices, but do not provide specifics. For example, TTL states only *"we have implemented appropriate security controls to protect Personal Information when stored or transmitted by TTL*."[47]
d. **No information about security practices:** Some service providers do not mention any details about their security practices and procedures, or whether they even follow any security practices and procedures or not. An example of this would be ACT, which does not mention any security practices or procedures in its Policy.

5. Grievance mechanisms

Applicable Rule and Principle: Rule 5 of the Rules mandates that applicable bodies corporate must designate a 'Grievance Officer' for redressing grievances of users regarding processing of their personal information, and the same is also recommended by the Ninth Principle, i.e., Accountability.

Observation: It was found that adherence with this requirement varied depending on service provider. For example:

a. **No Grievance Officer:** ACT and MTNL do not provide details of a grievance officer on their websites.

46. See <http://www.tataindicom.com/Download/data-privacy-policy.pdf>
47. Ibid

b. **Grievance Officer, but no process details**: Airtel, TTL, and Vodafone provide details of the Grievance Officer, but no further information about the grievance process is provided.
c. **Grievance Officer and details of process:** Aircel provides details of the grievance officer and grievance process.

As a note: All service providers with the exception of ACT have a general grievance redressal mechanism in place as documented on TRAI's website.[48] It is unclear whether these mechanisms are functional, and furthermore it is also unclear if these mechanisms can be used for complaints under the IT Act or the Rules, or complaints on the basis of the Principles. It should be further noted that the multiplicity of grievance redressal officers is a cause for concern, as it may lead to confusion.

6. Consent Mechanism

Applicable Rule and Principle: Rules 5 and 6 of the Rules[49] on Collection and Disclosure of information, respectively, require applicable bodies corporate to obtain consent/permission before collecting and disclosing personal information. The Choice and Consent Principle of the National Privacy Principles, as enumerated in the A.P. Shah Report, deals exclusively with choice and consent.[50] Withdrawal of consent is an important facet of the choice and consent principle as evidenced by the Rules[51] and the National Privacy Principles[52].

Observation: Methods of obtaining consent and for what consent was obtained for varied across service providers. For example:

a. Obtaining consent: Some service providers give data subjects with the choice of submitting their personal information (with some exceptions such as for legal requirements) and obtaining their consent for its collection and processing. For example, the policies of Airtel, Aircel, and TTL are the only ones which provide information on the mechanisms used to obtain consent. ACT provides for targeted advertisements based on the personal information of the user. The viewing or interaction of the user of such targeted advertisements is however, considered an affirmation to this third party source, that the user is the targeted criteria. Thus, there appears to be lack of consent in this regard.
b. No Consent or choice offered: Some service providers do not mention consent. For example, Vodafone, and BSNL do not make any mention of choice or consent in their respective privacy policies.
c. Consent for limited circumstances: Some service providers only provide consent in limited circumstances. For example, ACT mentions consent only in relation to targeted advertising. However, this information is potentially misleading, as discussed earlier in the survey.

There is also a certain degree of assumption in all the policies regarding consent, as noted in the survey. Thus, if you employ the services of the company in question, you are implicitly agreeing to their terms even if you have not actually been notified of them. And the vague terminology used by most of the policies leaves quite a lot of wiggle room for the companies

48. The complaint center details are available here: <http://www.tccms.gov.in/Queries.aspx?cid=1>
49. Rules 5 and 6
50. Principle 2, Principle 3, Personal Information Protection and Electronic Documents Act 2000. Available at: << http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>>
51. Rule 5(7),
52. Principle 2

in question, allowing them to thereby collect more information than the data subject has been notified of without obtaining his or her consent.

7. Transparency mechanism:

Applicable Rule and Principle: The Openness Principle specifically recommends transparency in all activities of the data controller.[53] The Rules provide a limited transparency mechanism under Rule 8 which require bodies corporate to document their security practices and procedures and Rule 4 which requires them to provide such information via a privacy policy. As a note, these fall short of the level of 'transparency' espoused by the Openness Principle of the National Privacy Principles.

Observation: All service providers fail in implementing adequate mechanisms for transparency.

8. Scope:

Applicable Rule and Principle: Though the Openness Principle does not directly speak of the scope of the policies in question, it implies that policies regarding all data collection or processing should be made publically available. The same is also necessary under Rule 4, which mandates that any body corporate which "*collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract.*"

Observation: Though most of the companies mention the scope of their Privacy Policy and include the information collected through the websites, WAP Services, and use of the company's products and services, some companies do not do so. For instance, the scope of the policy is given rather vaguely in the Airtel's Policy, and the scope of ACT's policy is restricted to the information collected during the usage of their products and services, and not their website. BSNL's privacy policy is worrisome as it seems to restrict its scope to the information collected through the website only, but does not at the same time state that it does not apply to other methods of data collection and processing.

International Best Practices

Canada

The privacy regulation regime in Canada is a mixture of the federal regulations and the provincial regulations. Of the former, the Privacy Act is applicable to the public sector, while the Personal Information Protection and Electronic Documents Act ('PIPEDA') applies to the private sector. There are also federal level sectoral regulations, of which the Telecommunications Act is relevant here. The PIPEDA covers the activities of all businesses and federally regulated industries regarding their collection, use, disclosure, safeguarding and provision of access to their customers' personal information. Further, in 2009, the Canadian Radio-television and Telecommunications Commission ('CRTC'), by virtue of the 'Telecom Regulatory Policy CRTC 2009-657'[54] made ISPs subject to privacy standards higher than the

53. P. 21
54. Telecom Regulatory Policy CRTC 2009-657, Review of the Internet traffic management practices of Internet service providers << www.crtc.gc.ca/eng/archive/2009/2009-657.htm>>

standards given under the PIPEDA, while at the same time allowing them to use Internet Traffic Management Practices ('ITMPs').[55]

The 2009 policy is progressive as it balances the economic needs of Internet Traffic Management Providers vis-à-vis the privacy concerns of consumers. The need to identify ITMP's is integral in the protection of online privacy, as ITMP's most commonly employ methods such as deep packet inspection which can be used to burrow into personal information of consumers as well.

Recognising that this may not be the current practice, but a possibility in the future, the policy makes certain guidelines for ITMPs. It permits ITMP's that block bad traffic such as spam and malicious software. Nearly all other ITMPs however, require the prior notice of 30 days or more before initialising the ITMP.[56]

ITMP's are to be used only for the defined need of the ISP and not beyond this, and must not be used for behavioural advertising. Secondary ISPs in their contracts with Primary ISPs must agree to the same duties of the latter, that is the personal information entrusted to them is meant for its purpose alone and is not to be disclosed further.

Australia

The central privacy regulation in Australia is the Privacy Act, 1988. The Act defines two sets of privacy principles, the Information Privacy Principles which apply to the public sector, and the National Privacy Principles which apply to the private sector.[57] These principles govern the following: collection,[58] use and disclosure,[59] data quality,[60] security,[61] openness,[62] access and correction,[63] identifiers,[64] anonymity,[65] trans-border data flows,[66] and sensitive information.[67] The Telecommunications Act, 1997, is also relevant here, as it also governs the use or disclosure of information by telecommunication services providers,[68] but such information is only protected by the Telecommunications Act if it comes to a person's knowledge or

55. Alex Cameron,*CRTC Imposes Super-PIPEDA Privacy Protections for Personal Information Collected by ISPs*, Privacy and Information Protection Bulletin, Fasken Martineau, <<http://www.fasken.com/files/Publication/4317fd62-0827-4d1d-b836-5b932b3b21db/Presentation/PublicationAttachment/bafbf01e-365c-47f8-86a5-5cf7d7e43787/Bulletin_-_November_2009_-_Cameron.pdf. >> Accessed 21 May 2014
56. Bram D. Abramson, Grant Buchanan, Hank Intven, *CRTC Shapes Canadian "Net Neutrality" Rules*, McCarthy Tetrault. < http://www.mccarthy.ca/article_detail.aspx?id=4720 > Accessed 21 May 2014
57. The Privacy Act, 1988, Part III, *available at* << http://www.comlaw.gov.au/Series/C2004A03712.>>
58. *Id*, note 28, Schedule 3, 1.
59. *Id*, schedule 3, 2.
60. *Id*, schedule 3, 3.
61. *Id*, schedule 3, 4.
62. *Id*, schedule 3, 5.
63. *Id*, schedule 3, 6.
64. *Id*, schedule 3, 7.
65. *Id*, schedule 3, 8.
66. *Id*, schedule 3, 9.
67. *Id*, schedule 3, 10.
68. Telecommunications Act, Part 13 (Information or a document protected under Part 13 could relate to many forms of communications, including fixed and mobile telephone services, internet browsing, email and voice over internet telephone services. For telephone-based communications, this would include subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet-based applications, the information protected under Part 13 would include the Internet Protocol (IP) address used for the session, and the start and finish time of each session.)

possession in certain circumstances. An example of this is Section 276 of the same, which providers that the information protected by that section will be protected only if the person collecting the information is a current or former carrier, carriages service provider or telecommunications contractor, in connection with the person's business as such a carrier, provider or contractor; or if the person is an employee of a carrier, carriage service provider, telecommunications contractor, because the person is employed by the carrier or provider in connection with its business as such a carrier, provider or contractor.

European Union

The most important source of law in the European Union ('EU') regarding Data Privacy in general is the Data Protection Directive ('Directive').[69] The Directive has a broad ambit, covering all forms of personal data collection and processing, and mandating that such collection or processing follow the Data Protection Principles it sets out.[70] The Directive differentiates between Personal Data and Sensitive Personal Data,[71] with the collection and processing of the latter being subject to more stringent rules. The telecommunications service providers and internet service providers are included in the definition of 'Controller' as set out in the Directive, and are hence subject to the regulations enforced by the member states of the EU under the same.[72] The Directive will soon be superseded by the General Data Protection directive, which is scheduled to come into force in late 2014, with a two-year transition period after that.[73]

In addition to the above, ISPs are also subject to the Directive on Privacy and Electronic Communications[74] and the Data Retention Directive.[75] The Directive on Privacy and Electronic Communications ('E-Privacy Directive') sets out rules regarding processing security, confidentiality of communications, data retention, unsolicited communications, cookies, and a system of penalties set up by the member states under the title of 'Control'. The E-Privacy Directive supplements the original Data Privacy Directive, and replaces a 1997 Telecommunications Privacy directive. The Data Retention Directive does not directly concern the collection and processing of data by a service provider, but only concerns itself with the retention of collected data. It was an amendment to the E-Privacy Directive, which required the member states to store the telecommunications data of their citizens for six to twenty-four months, and give police and security agencies access to details such as IP addresses and time of use of e-mails.

---

69. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
70. *Id*, article 3.
71. *Id*, article 8.
72. *Id*, article 2, (d). ("*(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;*")
73. European Commission-IP-12/46, 25 January 2012, <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.>
74. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
75. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The established practices considered above have the following principles, relevant to the study at hand, in common:

1. Notice
2. Collection Limitation
3. Use Limitation
4. Access and Corrections
5. Security
6. Data Quality and Accuracy
7. Consent
8. Transparency

And the following principles are common between two of the three regimes discussed above:

1. The PIPEDA and the Privacy Act both mention rules regarding Disclosure of collecting information, but the Data Protection Directive does not directly govern disclosure of collected information.
2. The Principles of Accountability is covered by the Data Protection Directive and the PIPEDA, but is not directly dealt with by the Privacy Act
3. The PIPEDA and the Data Protection Directive directly mention the principle of Enforcement, but it is not directly covered by the Privacy Act.

Recommendations

Broadly, service providers across India could take cognizance of the following recommendations to ensure alignment with the Rules found under section 43A and to maximize the amount of protection afforded to customer data.

1. **Access and location of privacy policy:** Service providers should ensure that the privacy policy is easily accessible through the main page of the company's website. Furthermore, the Privacy Policy should be accessible to users prior to the collection of personal information. All 'User Agreement' forms should include a written Privacy Policy or a reference to the Privacy Policy on the service provider's website.
2. **Scope of privacy policy:** The privacy policy should address all practices and services offered by the service provider. If a service requires a different or additional privacy policy, a link to the same should be included in the privacy policy on the main website of the service provider.
3. **Defining consent**: The Privacy Policy should clearly define what constitutes 'consent'. If the form of consent changes for different types of service, this should be clearly indicated.
4. **Clear language:** The language in the Privacy Policy should be clear and specific, leaving no doubt or ambiguity with regards to the provisions.
5. **Transparent security practices:** The Privacy Policy should include comprehensive information about a company's security practices should be included in the Privacy Policy. Information pertaining to audits of these procedures should be made public.
6. **Defined and specified third parties:** The Privacy Policy should define 'third party' as it pertains to the company's practices and specify which third parties information will be shared with.
7. **Comprehensive grievance mechanism:** The Privacy Policy should include relevant details for users to easily use established grievance mechanisms. This includes contact details of the grievance officers, procedure of submitting a grievance, expected response of the grievance officer (recognition of the grievance, time period for resolution etc.), and method of appealing decision of the grievance officer.

8. **Specify laws governing disclosure to governmental agencies and law enforcement:** The Privacy Policy should specify under what laws and service providers are required disclose personal information to.
9. **Inclusion of data retention practices:** The Privacy Policy should include provisions defining the retention practices of the company.

Annexure 1

Explanation and Interpretation of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Section 43A under the Information Technology Act 2000 addresses the protection of sensitive personal data or information and the implementation of an information security management system, and the Rules framed under section 43A attempt establish a holistic data security regime for the private sector.

The following section is a description of the requirements found under section 43A and subsequent Rules with respect to information that must be included in the privacy policy of a 'body corporate' and procedures that must be followed by 'body corporate' with respect to the publishing and notice of a privacy policy. This section also includes an explanation of how each relevant provision has been interpreted for the purpose of this research.

Relevant provisions that pertain to the privacy policy of body corporate

Rule 3: This section defines the term 'Sensitive Personal Data or Information', setting out the six types of information that are considered 'sensitive personal data' including:

i. Password – Defined under the Rules as "a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information"[76].
ii. Financial information – "such as Bank account or credit card or debit card or other payment instrument details"[77]
iii. Physical, physiological and mental health condition
iv. Sexual orientation
v. Medical records and history
vi. Biometric information

The two other broad categories of Sensitive Personal Data or Information that are included in the Rule are – any related details provided to the body corporate, and any information received by the body corporate in relation to the categories listed above.[78]

The proviso to this section excludes any information available in the public domain or which may be provided under the Right to Information Act, 2005 from the ambit of SPD/I.

Under the Rules, Sensitive Personal Data is considered to be a subset of Personal Information – which has been defined by Section 2 (1) (i) as "*any information that relates to a natural*

76. Rule 2 (h)
77. Rule 3 (ii)
78. Rule 3 (vii) and (viii)

person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person"[79]

Interpretation: While the Rules are clearly limited to personal and sensitive personal data or information, the use of these terms throughout the Rules is not consistent. For example, some provisions under the Rules ambiguously use the term 'information' in place of the terms 'personal information' and/or 'sensitive personal information'.[80] While 'information' has been defined non-exhaustively as any 'data, message, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated microfiche' in the Act, this definition appears to be overbroad and cannot be applied in that form for the purpose of provisions on privacy policy.[81] Hence, 'information', when used in the Rules, is construed to mean 'personal information' including 'sensitive personal information' for the purpose of this survey.

As per Rule 3, information in the public domain isn't classified as sensitive personal data. This exception may require a relook considering that 'providers' of information' may not want their data to be disclosed beyond its initial disclosure, or in certain cases, they may not even know of its existence in the public domain. Since the notice of collection, purpose and use of information is limited to SPD alone under Rule 5, information in the public domain should be seen together with whether the provider of information has provided the latter directly or to service provider that requires the information. If the source is the information provider directly, it need not be classified as SPD.

On a positive note, the addition of the term "in combination with other information available or likely to be available", gives recognition to the phenomenon of convergence of data. Parts of information that seem of negligible importance, when combined, provide a fuller personal profile of an individual, the recognition of this, in effect, gives a far wider scope to personal information under the Rules.

In the specific context of Privacy Policies, the Rules do not stipulate whether the mandated privacy policy has to explicitly mention SPD/I that is collected or used.{This is mentioned under Rule 4(ii) and (iii)} Since Rules do require that a privacy policy must be clear, it is construed that the privacy policy should explicitly recognize the type of PI and SPD/I being collected by the company.

Rule 4: This rule mandates that a "*body corporate that collects, receives possess, stores, deals or handles information of the provider of information*". For the purposes of this research, this entity will be referred to as a 'data controller'. According to Rule 4, every data controller must provide a privacy policy on its website for handling of or dealing in personal information including sensitive personal information.
The following details have to be included in the privacy policy –
"(i) Clear and easily accessible statements of its practices and policies;
(ii) Type of personal or sensitive personal data or information collected under rule 3;
(iii) Purpose of collection and usage of such information;
(iv) Disclosure of information including sensitive personal data or information as provided in rule 6;

79. Rule 2 (i)
80. Rule 4(iii), (iv)
81. Section 2(v) of the Act defines 'information'

(v) Reasonable security practices and procedures as provided under rule 8."[82]
Interpretation: The Rules do not provide an adequate understanding of the terms 'clear' and 'accessible', and the terms 'practices' and 'policies' are not defined. For the purpose of this research, 'practices' will be construed to mean the privacy policy of the company. It is deemed to be clear and accessible if it is available either directly or through a link on the main website of the body corporate. To meet the standards set by this Rule, the policy or policies should disclose information about the company's services, products and websites, whenever personal information is collected.

Rule 5: This Rule establishes limits for collection of information. It states that prior informed consent has to be obtained by means of letter, fax or email from the user regarding the purpose of usage for the sensitive personal information sought to be collected. It limits the purpose for collection of SPD/I to collection for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf and only if it is considered necessary for that purpose. Thus, the information collected can only be used for the stated purpose for which it has been collected.[83]

Further, Rule 5 (3) provides that consent has to be obtained and knowledge provided to a person from whom personal information is being directly collected – which for service providers – is understood to be through the customer application form. This rule will be deemed to have been complied with when the following information is provided –

a. The fact that the information is being collected.
b. The purpose of such collection.
c. Intended recipients of the collected information.
d. Names and addresses of the agency or agencies collecting and retaining information.

Moreover, it provides that the user has to be given the option of not providing information prior to its collection. In case the user chooses this option or subsequently withdraws consent the body corporate has the option to withhold its services.

This section also provides under Section 5 (2) (a) that the type of information that this Rule concerns itself with can only be collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf and if it is considered necessary for that purpose.

It also requires that a Grievance Officer be instated to redress the grievance "*expeditiously but within one month from the date of receipt of grievance.*" The Grievance Redressal process has been discussed in more detail later.

Interpretation: Even though Rule 5 incorporates various major data protection principles and mandates the establishment of a Grievance Redressal Mechanism, neither Rule 5 nor Rule 4 (3) makes a reference to the other. [Rule 4(3) uses the term "such information", and the fact that it follows Rule 4(2) which clearly refers to personal information as well as SPD/I, means that Rule 4(3) also refers to the same]

Prima facie, the scope of Rule 5 is limited to collection of SPD/I. However, Rule 4 (3) ostensibly covers the broad ambit of 'information' which includes SPD/I. Construing these two

82. Rule 4 (1).
83. Rule 5 (5)

provisions together using the 'Harmonious Construction' principle[84], Rule 5 could be interpreted to cover personal information for privacy policies under Rule 4.
In addition, Rule 5(3) doesn't expand on the reasonable steps to be taken for intimating the information provider on the extent of disclosure and purpose of collection. This appears as a rather large loophole considering the wide interpretation that can be given to 'reasonable' practices of service providers.

Rule 6: This rule lays down the conditions and procedure for disclosure of information.[85] Under it, the following conditions apply before any disclosure of information by the 'body corporate' to any third party –

a. The body corporate is required to obtain prior permission from the provider of the information, or
b. Permission to disclose has to be agreed on in the contract between the company and the data subject, or
c. Disclosure is necessary for the compliance of a legal obligation.

An exception is made in case the disclosure is made to an authorized and legally mandated Government agency upon request for the purposes of verification of identity, for prevention, detection, and investigation of incidents, specifically including cyber incidents, prosecution, and punishment of offences, in which case no consent from the data subject will be required. Thus, the company does not need user consent to disclose information to authorized law enforcement or intelligence agencies when presented with an authorized request.

Interpretation:

The guidelines for disclosure limit themselves to SPD under Rule 6 leaving a vacuum with respect to information that doesn't fall within the definition of SPD/I. However, Rule 4 (iv)'s applies to 'information including SPD'. Reading the two together, in accordance with the 'Harmonious Construction' principle, the scope of SPD/I in Rule 6 is construed to extend to the same personal information and SPD/I as is covered by Rule 4 (iv), for the limited purpose of the privacy policies under Rule 4.

Rule 7: This Rule requires that when the data controller transfers SPD/I to another body corporate or person, such a third party must adhere to the same standards of data protection that the body corporate collecting the information in the first instance follows.

Interpretation: Although the privacy policy is not required to provide details of the transfer of information, the fourth sub-section of Rule 4, which concerns itself with the obligation of the body corporate to provide a policy for privacy including information about the disclosure of information to its consumers, incorporates this Rule as it deals with disclosure of information to third parties. Thus, the Policy of the body corporate must include details of the way the data is handled or dealt by the third party, which is shared by the body corporate in question.

84. Defined by Venkatarama Aiyar, J as: "The rule of construction is well settled that when there are in an enactment two provisions which cannot be reconciled with each other, they should be so interpreted that, if possible, effect could be given to both" in *Venkataramana Devaru v. State of Mysore*, AIR 1958 SC 255, p. 268: G. P. Singh, Principles of Statutory Interpretation, 1th ed. 2010, Lexisnexis Butterworths Wadhwa Nagpur. The principle was applied to interpret statutory Rules in A. N. Sehgal v. Raje Ram Sheoram, AIR 1991 SC 1406.
85. Rule 6

Rule 8: This Rule details the criteria for reasonable security practices and procedures.[86] It provides that not only must the body corporate have implemented standard security practices and procedures, but it should also have documented the information security program and policies containing appropriate "*managerial, technical, operational and physical security control measures*". The Rule specifically uses the example of IS/ISO/IEC 27001 as an international standard that would fulfill the requirements under this provision. The security standards or codes of best practices adopted by the company are required to be certified/audited by a Government approved independent auditor annually and after modification or alteration of the existing practice and procedure. Sub-section (1) of the Rule also gives the body corporate the option of creating its own security procedures and practices for dealing with managerial, technical, operational, and physical security control, and have comprehensive documentation of their information security programme and information security policies. These norms should be as strict as the type of information collected and processed requires. In the event of a breach, the body corporate can be called to demonstrate that these norms were suitably implemented by it.

Interpretation: It is unclear whether the empanelled IT security auditing organizations recognized by CERT-In discussed later are qualified for the purpose of this Rule, but from publicly available information the Data Security Council of India and CERT-In's empanelled Security Auditors seem to be the agencies given this task[87]. With regards to the Privacy Policy or Policies of a company, it is only necessary that the company include as many details as possible regarding the steps taken to ensure the security and confidentiality of the collected information in the Privacy Policy and Policies, and notify them to the consumer.

Other Relevant Policies:

Empanelled Information Technology Security Auditors - CERT-In has created a panel of 'IT Security Auditors' for auditing networks & applications of various organizations of the Government, critical infrastructure organizations and private organizations including bodies corporate.[88] The empanelled IT security auditing organization is required to, *inter alia*, conduct a "*Review of Auditee's existing IT Security Policy and controls for their adequacy as per the best practices vis-à-vis the IT Security frameworks outlined in standards such as COBIT, COSO, ITIL, BS7799 / ISO17799, ISO27001, ISO15150, etc.*"[89] and conduct and document various assessments and tests. Some typical reviews and tests that include privacy reviews are – Information Security Testing, Internet Technology Security Testing and Wireless Security Testing.[90] For this purpose CERT-In maintains a list of IT Security Auditing Organizations[91].

Criteria for analysis of company policies based on the 43A Rules

86. Rule 8
87. 52nd Report, Standing Committee on Information Technology, 24, available at <http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf .>
88. Panel Of Information Security Auditing Organisations, CERT-IN <http://www.cert-in.org.in/PDF/background.pdf>
89. Section 1, Guidelines for applying to CERT-In for Empanelment of IT Security Audition Organisation, <http://www.cert-in.org.in/PDF/InfoSecAuditorsEmpGuidelines.pdf>
90. Section 2.0, Guidelines for auditee organizations, Version 2.0, IT Security Auditing Assignment, http://www.cert-in.org.in/PDF/guideline_auditee.pdf
91. See <http://www.cert-in.org.in/PDF/Empanel_org.pdf>

1. Clear and Accessible statements of its practices and policies[92] –

i. Whether the privacy policy is accessible through the main website of the body corporate?
ii. Whether the privacy policy is mentioned or included in the terms and conditions of all document of the body corporate that collects personal information?
iii. Whether the privacy policy can be comprehended by persons without legal knowledge?

2. Type and acknowledgment of personal or sensitive personal data/information collected[93]-

i. Whether the privacy policy explicitly states that personal and sensitive personal information will be collected.
ii. Whether the privacy policy mentions all categories of personal information including SPD/I being collected?

3. Option to not provide information and withdrawal of consent[94] –

i. Whether the Privacy Policy specifies that the user has the option to not provide information?
ii. Whether the Privacy Policy specifies that the user has the option to subsequently withdraw consent?

4. Existence of Grievance Officer –

i. Whether the privacy policy mentions the existence of a grievance officer?
ii. Whether the privacy policy provides details of the grievance redressal mechanism?
iii. Whether the privacy policy provides the names and contact information of the grievance officer?

5. Purpose of Collection and usage of information –

i. Whether the privacy policy enumerates the purpose(s) for which information is collected exhaustively?

6. Disclosure of Information –

i. Whether personal information is shared with third parties (except authorized government agencies/LEA/IA) only with user consent?
ii. Whether the policy specifies that personal information is disclosed to Government agencies/LEA/IA only when legally mandated as per the circumstances laid out in 43A?

7. Reasonable Security practices and procedures –

i. Whether the privacy policy provides adequate details of the reasonable security practices and procedures followed by the body corporate to secure information?

92. Rule 4
93. Rule 4
94. Rule 5 (7)

Annexure 2

Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules) 2011 and Company SURVEY

1. Bharti Airtel Ltd.

1. **Clear and Accessible statements of its practices and policies: Yes**

a. **Rationale:** Airtel's Privacy Policy[95] is available through the main page of the website and it is mentioned in the Airtel Terms and Conditions and is applicable for Airtel's websites as well as its services and products, such as its telecommunications services. It was determined that the policy can be comprehended by individuals without legal knowledge.

2. **Type and acknowledgement of personal or sensitive personal data/information collected: Yes**

b. **Rationale:** Airtel's Privacy Policy indicates that sensitive personal and personal information will be collected, defines sensitive personal information[96], and specifies specific types of personal[97] and sensitive personal information[98] that will be collected.

3. **Option to not provide data or information and subsequent withdrawal of consent: Yes**

c. **Rationale:** The Airtel Privacy Policy states that individuals have the right to choose not to provide consent or information and have the right to withdraw consent. The policy notes that if consent/information is not provided, Airtel reserves the right to not provide or to withdraw the services.[99]

4. **Existence of Grievance Officer: Yes**

---

95. See << http://www.airtel.in/forme/privacy-policy>>
96. *'Information that can be used by itself to uniquely identify, contact or locate a person, or can be used with information available from other sources to uniquely identify an individual. For the purpose of this policy, sensitive personal data or information has been considered as a part of personal information.'* Accessed at << http://www.airtel.in/forme/privacy-policy/collection+of+personal+info?contentIDR=53535f55-b787-4cb8-b399-d11d97f80c26&useDefaultText=0&useDefaultDesc=0>>
97. Subscriber's name, father's name, mother's name, spouse's name, date of birth, current and previous addresses, telephone number, mobile phone number, email address, occupation and information contained in the documents used as proof of identity and proof of address. Information related to your utilization of our services which may include your call details, your browsing history on our website, location details and additional information provided by you while using our services. We may keep a log of the activities performed by you on our network and websites by using various internet techniques such as web cookies, web beacons, server log files, etc.
98. Password**,** Financial information –details of Bank account, credit card, debit card, or other payment instrument detail**s,** Physical, physiological and mental health condition**.**
99. Airtel states that if a customer does not provide information or consent for usage of personal information or subsequently withdraws consent, Airtel reserves the right to not provide the services or to withdraw the services for which the said information was sought, Avaliable at: <http://www.airtel.in/forme/privacy-policy/collection+of+personal+info?contentIDR=53535f55-b787-4cb8-b399-d11d97f80c26&useDefaultText=0&useDefaultDesc=0>

a. **Rationale:** Airtel provides for the contact details of nodal officers[100] and appellate authorities[101] on its website. Additionally the website provides for the 'Office of the Ombudsperson'[102], which is an independent forum for employees and external stakeholders[103] of the company to raise concerns and complaints about improper practices which are in breach of the Bharti Code of Conduct. Additionally, details of the Airtel Grievance Redressal Officers can also be found in the TRAI website.[104]

5. Comprehensive disclosure of purpose of collection and usage of information: Partial

Rationale: Airtel's Privacy Policy indicates eight purposes[105] that information will be collected and used for, but notes that the use and collection is not limited to the defined purposes.

6. Disclosure of Information[106]: Yes

a. **Rationale:** Airtel has a dedicated section explaining the company's practices around the disclosure and sharing of collected information, including ways in which consent will be collected for the sharing of personal information[107], how collected personal information may be collected internally[108], the disclosure of information to third parties and that the third party will be held accountable for protecting the information through contract[109], the possible transfer of personal information and its purposes[110], and the

100. See <www.airtel.in/applications/xm/FixedLineNodalOfficer.jsp>
101. See << http://www.airtel.in/applications/xm/BroadbandInternet_AppellateAuth.jsp>
102. See << http://www.airtel.in/about-bharti/about-bharti-airtel/ombuds-office>>
103. Stakeholders are defined as: employee, associate, strategic partner, vendor
104. See <<http://www.trai.gov.in/WriteReadData/ConsumerGroup/Document/201307233124780556 6Bharti_Airtel_CC_AA-23072013.pdf>>
105. Verification of customer's identity; Complete transactions effectively and bill for products and service; Respond to customer requests for service or assistance; Perform market analysis, market research, business and operational analysis; Provide, maintain and improve Airtel products and services; Anticipate and resolve issues and concerns with Airtel products and services; Promote and market Airtel products and services which it may consider of interest and benefit to customers; and, Ensure adherence to legal and regulatory requirements for prevention and detection of frauds and crimes.
106. See << http://www.airtel.in/forme/privacy-policy/disclosure+and+transfer?contentIDR=745792ad-d6af-4684-85d4-d85773e77356&useDefaultText=0&useDefaultDesc=0>>
107. "Airtel may obtain a customer's consent for sharing personal information in several ways, such as in writing, online, through "click-through" agreements; orally, including through interactive voice response; or when a customer's consent is part of the terms and conditions pursuant to which Airtel provides a service."
108. Airtel and its employees may utilize some or all available personal information for internal assessments, measures, operations and related activities…"
109. Airtel may at its discretion employ, contract or include third parties external to itself for strategic, tactical and operational purposes. Such agencies though external to Airtel, will always be entities which are covered by contractual agreements. These agreements in turn include Airtel's guidelines to the management, treatment and secrecy of personal information
110. Airtel may transfer subscriber's personal information or other information collected, stored, processed by it to any other entity or organization located in India or outside India only in case it is necessary for providing services to a subscriber or if the subscriber has consented (at the time of collection of information) to the same. This may also include sharing of aggregated information with them in order for them to understand Airtel's environment and consequently, provide the subscriber with better services. While sharing personal information with third parties, adequate measures shall be taken to ensure that reasonable security practices are followed at the third party."

circumstances under which information will be disclosed to governmental agencies (which reflect the circumstances defined by the Rules.)[111]

7. Existence of reasonable security practices and procedures[112]: Yes

a. **Rationale:** Airtel's privacy policy has a dedicated section that explains the company's security practices and procedures in place. The policy notes that Airtel's practices and procedures are IS/ISO/IEC 27001 compliant[113], that access is restricted to a need to know basis and that employees are bound by codes of confidentiality[114], and that Airtel works to ensure that third parties also have strong security procedures in place.[115] The policy also provides details on the retention[116] and destruction[117] procedures for personal information, and notes that reasonable steps are taken to protect against hacking and virus attacks.[118]

1. Tata Telecommunication Services (DoCoMo and Virgin Mobile)

1. Clear and Accessible statements of its practices and policies: Partial

a. **Rationale**: Though Tata DoCoMo has a comprehensive Data Privacy Policy[119] that is applicable to Tata Teleservices Limited's ("**TTL**") products and services and the TTL website, it is not accessible to the user through the main website. In the Frequently Asked Questions Section of TTL, it is clarified under what circumstances information that you provide is not covered by the TTL privacy policy.[120]

---

111. Airtel may share subscribers' personal information with Government agencies or other authorized law enforcement agencies (LEAs) mandated under law to obtain such information for the purpose of verification of identity or for prevention, detection, investigation including but not limited to cyber incidents, prosecution, and punishment of offences.
112. See<< http://www.airtel.in/forme/privacy-policy/security+practices+and+procedures?contentIDR=9346516c-c1a1-4bd7-bce0-6945236dceaa&useDefaultText=0&useDefaultDesc=0>>
113. Airtel adopts reasonable security practices and procedures, in line with international standard IS/ISO/IEC 27001, to include, technical, operational, managerial and physical security controls in order to protect a customer's personal information from unauthorized access, or disclosure while it is under our control.
114. Airtel's security practices and procedures limit access to personal information on need-only basis. Further, its employees are bound by Code of Conduct and Confidentiality Policies which obligate them to protect the confidentiality of personal information.
115. Airtel takes adequate steps to ensure that its third parties adopt reasonable level of security practices and procedures to ensure security of personal information.
116. Airtel may retain a subscriber's personal information for as long as required to provide him/her with services or if otherwise required under any law.
117. When Airtel disposes of its customers' personal information, it uses reasonable procedures to erase it or render it unreadable (for example, shredding documents and wiping electronic media)."
118. Airtel maintains the security of its internet connections, however for reasons outside of its control, security risks may still arise. Any personal information transmitted to Airtel or from its online products or services will therefore be at a customer's own risk. It observes reasonable security measures to protect a customer's personal information against hacking and virus dissemination.
119. See <<http://www.tatadocomo.com/downloads/data-privacy-policy.pdf
120. Information that customers provide to non-TTL companies is not covered by TTL's Policy. For example: When customers download applications or make an online purchase from a non-TTL company while using TTL's Internet or wireless services, the information collected by the non-TTL company is not subject to this Policy. When you navigate to a non-TTL company from TTL websites or applications (by clicking on a link or an advertisement, for example), information collected by the non-TTL company is governed by its privacy policy and not TTL's Privacy Policy. If one uses public forums — such as social networking services, Internet bulletin boards, chat rooms, or blogs on TTL or non-TTL websites, any Personal Information disclosed publicly can be read, collected, or used by others. Once one chooses to

2. **Type of personal or sensitive personal data/information collected: Partial**

a. **Rational:** TTL defines personal information[121] but only provides general examples of types of personal information[122] (and not sensitive personal) collected, rather than a comprehensive list. The definitions and examples of information collected are clarified in the FAQs and the Privacy Policy, rather than in the Privacy Policy alone. As a strength, the Privacy Policy clarifies the ways in which TTL will collect information from the user – including the fact that they receive information from third parties like credit agencies.[123]

3. **Option to not provide information and withdrawal of consent: N/A**

a. **Rationale:** The TTL Privacy Policy does not address the right of the individual to provide consent/information and to withdraw information/consent.

4. **Existence of Grievance Officer: Yes**

a. **Rationale:** TTL has various methods to lodge complaints and provides for an appellate authority.[124] Additionally, details of the Grievance Redressal Officers are provided via the TRAI website.[125]

5. **Purpose of Collection and usage of information: Yes**

---

reveal Personal Information on such a site, the information is publicly available, and TTL cannot prevent distribution and use of that information by other parties. Information on a wireless Customer 's location, usage and numbers dialed, which is roaming on the network of a non-TTL company will be subject to the privacy policy of the non-TTL company, and not TTL's Policy.

121. "Personal Information" is any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

122. Personal Information – Some general examples -TTL may collect Confidential Data in different forms such as Personal and other Information based on a customer's use of its products and services. Some examples include, Contact Information that allows us to communicate with you -- including your name, address, telephone number, and e-mail address; Billing information-- including payment data, credit history, credit card number, security codes, and service history.Equipment, Performance, TTL Website Usage, Viewing and other Technical Information about use of TTL's network, services, products or websites.
Technical & Usage Information is clarified in the FAQ's as information related to the services provided, use of TTL's network, services, products or websites. Examples of the Technical & Usage Information collected include: **Equipment Information** that identifies the equipment used on TTL's network, such as equipment type, IDs, serial numbers, settings, configuration, and software. **Performance Information** about the operation of the equipment, services and applications used on TTL's network, such as IP addresses, URLs, data transmission rates and latencies, location information, security characteristics, and information about the amount of bandwidth and other network resources used in connection with uploading, downloading or streaming data to and from the Internet. **TTL Website Usage Information** about the use of TTL websites, including the pages visited, the length of time spent, the links or advertisements followed and the search terms entered on TTL sites, and the websites visited immediately before and immediately after visiting one of TTL's sites.TTL also may collect similar information about a customer's use of its applications on wireless devices. **Viewing Information** about the programs watched and recorded and similar choices under Value added TTL services and products.

123. Ways in which TTL collects information: On the purchase or interaction about a TTL product or service provided; Automatically collected when one visits TTL's websites or use its products and services; Other sources, such as credit agencies.

124. See <http://www.tatateleservices.com/t-customercare.aspx>

125.See<http://www.trai.gov.in/WriteReadData/ConsumerGroup/Document/20130723412184636 21Tata_CC_AA_1-23072013.pdf>

a. **Rationale:** In its' Privacy Policy, TTL describes the way in which collected information is used.[126] The TTL FAQs further clarify the use of cookies by the company, the use of provided information for advertising purposes, [127] and the use of aggregate and anonymized data.[128]

6. Disclosure of Information: Yes

a. **Rationale:** In the Privacy Policy and the FAQs page, TTL is transparent about the circumstances on which they will share/disclose personal information with third parties[129], with law enforcement/governmental agencies[130], and with other TTL companies.[131] Interestingly, the TTL FAQ's clarify to the customer that their personal information might be processed in different jurisdictions, and thus would be accessible by law enforcement in that jurisdiction.[132]

---

126. To provide the best customer experience possible; Provide the services a customer purchases, respond to customer questions; Communicate with customers regarding service updates, offers, and promotions; Deliver customized content and advertising that may be of interest to customers; Address network integrity and security issues; Investigate, prevent or take action regarding illegal activities, violations of TTL's Terms of Service or Acceptable Use Policies
127. **Site functionality** -Cookies and other tracking tools are used to help TTL analyze, manage and improve websites and storing customer preferences. **Advertising** TTL and its advertising partners, including Yahoo! and other advertising networks, use anonymous information gathered through cookies and other similar technologies, as well as other information TTL or its advertising networks may have, to help tailor the ads a customer sees on its sites.
128. TTL collects some Information on an anonymous basis. TTL also may anonymize the Personal Information it collects about customers. It may obtain aggregate data by combining anonymous data that meet certain criteria into groups.
129. In Other Circumstances: TTL may provide Personal Information to non-TTL companies or other third parties for purposes such as: To assist with identity verification, and to prevent fraud and identity theft; Enforcing its agreements and property rights; Obtaining payment for products and services that appear on customers' TTL billing statements, including the transfer or sale of delinquent accounts to third parties for collection; and to comply to legal and regulatory requirements. TTL shares customer Personal Information only with non-TTL companies that perform services on its behalf, and only as necessary for them to perform those services. TTL requires those non-TTL companies to protect any Personal Information they may receive in a manner consistent with this policy. TTL does not provide Personal Information to non-TTL companies for the marketing of their own products and services without a customer's consent. TTL may share aggregate or anonymous Information in various formats with trusted non-TTL entities, and may work with those entities to do research and provide products and services.
130. TTL provides Personal Information to non-TTL companies or other third parties (for example, to government agencies, credit bureaus and collection agencies) without consent for certain purposes, such as: To comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements, and to enforce our legal rights or defend against legal claims, To obtain payment for products and services that appear on customer TTL billing statements, including the transfer or sale of delinquent accounts to third parties for collection; To enforce its agreements, and protect our rights or property; To assist with identity verification, and to prevent fraud and identity theft; To prevent unlawful use of TTL's services and to assist in repairing network outages; To provide information regarding the caller's location to a public safety entity when a call is made to police/investigation agencies, and to notify the public of wide-spread emergencies; To notify or respond to a responsible governmental entity if we reasonably believe that an emergency involving immediate danger of death or serious physical injury to any person requires or justifies disclosure without delay; To display name and telephone number on a Caller ID device;
131. Subject to applicable legal restrictions, such as those that exist for Customer Proprietary Network Information (CPNI), the TTL companies may share your Personal Information with each other to make sure your experience is as seamless as possible, and you have the benefit of what TTL has to offer.
132. Customers and Users should be aware that TTL affiliates and non-TTL companies that perform services on behalf of TTL may be located outside the country where customers access TTL's services. As a result,

7. **Reasonable Security practices and procedures: Partial**

a. **Rationale:** TTL's Privacy Policy broadly references that security practices are in place to protect user information, but the policy does not make reference to a specific security standard, or provide detail as to what these practices and procedures are.[133] Although TTL's Privacy Policy does not make mention of any specific security standard, Tata Teleservices (Maharashtra) Limited claims to have been awarded with ISO 27001 ISMS (Information Security Management Systems) Certification in May 2011, and completed its first Surveillance Audit in June 2012[134]. Information on IT security standards adopted by other circles could not be found on the internet.

2. **Vodafone**

1. **Clear and Accessible statements of its practices and policies: Yes**

Rationale: Vodafone's Privacy Policy[135] is easily accessible from its website from a link at the bottom, directly from the home page and from all other pages of the website.[136]

2. **Collection of personal or sensitive personal data/information: No**

Rationale: Type –

a. Personal Information – The amount of details given by the Privacy Policy with regards to the personal information being collected is insufficient, as it does not include a number of relevant facts, and uses is vague language – such as '*amongst other things*', implying that information other than that which is notified is being collected.[137]

---

when customer Personal Information is shared with or processed by such entities, it may be accessible to government authorities according to the laws of those jurisdictions.

133. TTL has implemented appropriate security controls to protect Personal Information when stored or transmitted by TTL. It has established electronic and administrative safeguards designed to secure the information it collects, to prevent unauthorized access to or disclosure of that information and to ensure it is used appropriately. Some examples of those safeguards include: All TTL employees are subject to the internal Code of Business Conduct. The TTL Code requires all employees to follow the laws, rules, regulations, court and/or commission orders that apply to TTL's business such as legal requirements and company policies on the privacy of communications and the security and privacy of Customer records. Employees who fail to meet the standards embodied in the Code of Business Conduct are subject to disciplinary action, up to and including dismissal. TTL has implemented technology and security features and strict policy guidelines to safeguard the privacy of customer Personal Information. TTL has implemented encryption or other appropriate security controls to protect Personal Information when stored or transmitted by it; TTL limits access to Personal Information to those employees, contractors, and agents who need access to such information to operate, develop, or improve its services and products; TTL requires caller/online authentication before providing Account Information so that only the customer or someone who knows the customer's account Information will be able to access or change the information.
134. See << http://www.tatateleservices.com/download/aboutus/ttml/TTML-Annual-Report-2012-13.pdf>>
135. See << https://www.vodafone.in/pages/privacy_policy.aspx?cid=ker>>
136. "We have created this Privacy Policy to help you understand how we collect, use and protect your information when you visit our web and WAP sites and use our products and services."
137. Vodafone may hold information relating to customers that have been provided (such as on an application or registration form) or that it may has obtained from another source (such as its suppliers or from marketing organisations and credit agencies).
This information may include, amongst other things, a customer's name, address, telephone numbers, information on how a customer uses Vodafone's products and services (such as the type, date, time, location and duration of calls or messages, the numbers called and how much a customer spends, and information on his/her browsing activity when visiting one of Vodafone's group companies' websites), the location of a customer's mobile phone from time to time, lifestyle information and any other information collected in relation to his/her use of Vodafone's products and services ("information").

b. Sensitive Personal Data or Information – The Privacy Policy does not mention the categories or types of SPD/I, as defined under Rule 3, being collected by the service provider explicitly, only gives a general overview of the information that is collected.

3. Option to not provide information and withdrawal of consent: No

a. **Rationale:** The privacy policy does not mention the consent of data subject anywhere, nor does it mention his or her right to withdraw it at any point of time. It also does not mention whether or not the provision of services by Vodafone is contingent on the provision of such information.

4. Existence of Grievance Officer: Yes

a. **Rationale:** The Privacy Policy explicitly mentions and gives the email address of a grievance redressal officer, though further details about the other offices are given in a separate section of the website.[138]

5. Purpose of Collection and usage of information: Partial

a. Rationale:

The Privacy Policy gives an exhaustive list of purposes for which the collected information can be used by Vodafone,[139] but at the same time the framing of the opening sentence and the usage of the term 'may include' could imply that it can be used for other purposes as well.

It may use cookies and other interactive techniques such as web beacons to collect non-personal information about how a customer interacts with its website, and web-related products and services.
It may use a persistent cookie to record details such as a unique user identity and general registration details on your PC. Vodafone states that most browser technology (such as Internet Explorer, Netscape etc) allows one to choose whether to accept cookies or not – a customer can either refuse all cookies or set their browser to alert them each time that a website tries to set a cookie.

138. In case of any concerns the privacy officer can be contacted at privacyofficer@vodafone.com. Additionally details of the Grievance Redressal Officers is provided via the TRAI website. (TRAI website: http://www.trai.gov.in/WriteReadData/ConsumerGroup/Document/20130723415678511 24Vodafone_CC_AA-23072013.pdf

139. The information that Vodafone collects from customers is held in accordance with applicable laws and regulations in India. It may be used by us for a number of purposes connected with its business operations and functions, which include:
2.1 Processing customer orders or applications;
2.2 Carrying out credit checking and scoring (unless Vodafone have agreed otherwise);
2.3 Providing the customer with products and/or services requested (including the presentation or elimination of calling or connected line identification) or administering his/her account;
2.4 Billing
2.5 Settling accounts with those who provide related services to Vodafone;
2.6 Dealing with requests, enquiries or complaints and other customer care related activities; and all other general administrative and business purposes;
2.7 Carrying out market and product analysis and marketing Vodafone and its group companies' products and services generally;
2.8 Contacting a customer (including by post, email, fax, short text message (SMS), pager or telephone) about Vodafone and its group companies' products and services and the products and services of carefully selected third parties which it think may be of interest to customers (unless a customer asks us in writing not to). Electronic marketing messages may not include a marketing facility.
2.9 Registering customer details and allocating or offering rewards, discounts or other benefits and fulfilling any requests that a customer may have in respect of our and our group companies' schemes.
2.10 inclusion in any telephone or similar directory or directory enquiry service provided or operated by us or by a third party (subject to any objection or preference a customer may have indicated to us in writing);

6. **Disclosure of Information: Yes**

a. Rationale:

The Privacy Policy mentions that Vodafone might share the collected information with certain third parties and the terms and conditions which would apply to such a third party.[140] The phrasing does not imply that there are other conditions that have not been mentioned in the policy, under which the information would be shared with a third party. At the same time, the Privacy Policy does not explicitly say that the third party will necessarily follow the privacy and data security procedures and rules laid down in the Privacy Policy.

7. **Reasonable Security practices and procedures: Yes**

a. Rationale:

The Privacy Policy mentions in reasonably clear detail the security practices and procedures followed by Vodafone, and also mentions the circumstances in which the data subject should take care to protect his or her own information, wherein Vodafone will not be liable.[141]

2.11 carrying out any activity in connection with a legal, governmental or regulatory requirement on Vodafone or in connection with legal proceedings, crime or fraud prevention, detection or prosecution;
2.12 carrying out activities connected with the running of Vodafone's business such as personnel training, quality control, network monitoring, testing and maintenance of computer and other systems and in connection with the transfer of any part of Vodafone's business with respect to a customer or a potential customer.

140. In the need for disclosure to third parties, the personal information will only be disclosed to the third parties below:
3.1 Vodafone's group companies who may in India use and disclose your information for the same purposes as us;
3.2 those who provide to Vodafone or its group companies products or services that support the services that we provide, such as our dealers and suppliers;
3.3 credit reference agencies (unless Vodafone has agreed otherwise) who may share your information with other organisations and who may keep a record of the searches Vodafone makes against a customer's name;
3.4 if someone else pays a customer's bill, such as a customer's employer, that person;
3.5 those providing telephone and similar directories or directory enquiry services
3.6 anyone Vodafone transfers business to in respect of which a person is a customer or a potential customer;
3.7 anyone who assists Vodafone in protecting the operation of the Vodafone India networks and systems, including the use of monitoring and detection in order to identify potential threats, such as hacking and virus dissemination and other security vulnerabilities;
3.8 persons to whom Vodafone may be required to pass customer information by reason of legal, governmental or regulatory authority including law enforcement agencies and emergency services;
3.9 any person or organisation as authorised by laws and regulations applicable in India.
If a customer has opted in to receiving marketing material from Vodafone, it may also provide customer's personal information to carefully selected third parties who we reasonably believe provide products or services that may be of interest to customers and who have contracted with Vodafone India to keep the information confidential, or who are subject to obligations to protect your personal information.
To opt-out of receiving Vodafone marketing materials,customers can send a 'Do Not Disturb' message to Vodafone. If a customer wishes to use Vodafone products or services abroad, his/her information may be transferred outside India to that country. Vodafone's websites and those of its group companies may also be based on servers located outside of India.

141. Vodafone takes reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete, up-to-date and stored in a secure environment protected from unauthorized access, modification or disclosure.
Vodafone makes every effort to maintain the security of our internet connections; however for reasons outside of our control, security risks may still arise. Any personal information transmitted to it or from its online products or services will be at a customer's own risk, however, it will use its best efforts to ensure that any such information remains secure. Vodafone cannot protect any information that a customer makes available to the general public – for example, on message boards or in chat rooms.

Although Vodafone India's Privacy Policy does not specify what their IT Security standard is, its 2012/2013 Sustainability Report available through its international website[142] states that it follows industry practices in line with the ISO 27001 standard and its core data centre in India follows this standard[143].

3. Aircel

1. Clear and Accessible statements of its practices and policies: Yes

Rationale:

The Privacy Policy is accessible from every page of the Aircel website, with a link at the bottom of each page after the specific circle has been chosen. It is reasonably free of legalese and is intelligible.[144]

2. Type of personal or sensitive personal data/information collected: Partial

Rationale: Type –

a. Personal Information

In the Privacy Policy, the repeated usage of the term 'may' creates some doubt about the actual extent of the data collected, and leaves the Privacy Policy quite unclear in this regard. At the same time, the Privacy Policy does include a fairly comprehensive list of personal information that could be collected. [145] The wording in the Privacy Policy thus requires further clarification and specification in order to make a determination on whether or not it provides complete details on the personal information that will be collected.

a. Sensitive Personal Data or Information

The Privacy Policy does not mention SPDI explicitly, which adds to the lack of concrete details as noted earlier.

3. Option to not provide information and withdrawal of consent – Yes

---

Vodafone may use cookies and other interactive techniques such as web beacons to collect non-personal information about how a customer interacts.

142. See <http://www.vodafone.com>

143. See <http://www.vodafone.com/content/sustainability/operating_responsibly/privacy_and_security.html>

144. http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P26400194591312373872061 (Scope - This Privacy Policy has been created to help customer's understand how Aircel collects, uses and protects customer information when one visits its web and WAP sites and use its products and services.)

145. This information may include, amongst other things, customer's name, father's name, mother's name, spouse's name, date of birth, address, telephone numbers, mobile phone number, email address, occupation and information contained in the documents used as proof of identity and proof of address. Aircel may also hold information related to utilization of its services. This may include customer call records, browsing history while surfing Aircel's website, location details and additional information provided by customer while using our services.
Aircel may keep a log of the activities performed by a customer on its websites by using various internet techniques such as web cookies, web beacons, server log files, etc.
Aircel may use cookies and other interactive techniques such as web beacons to collect non-personal information about how customers interact with Aircel's website, and web-related products and services
Aircel may use a persistent cookie to record details such as a unique user identity and general registration details on customer's Personal Computers.

Rationale: The Privacy Policy mentions that users do have the right to refuse to provide or the withdrawal of consent to collect personal information. In such cases, Aircel can respectively refuse or discontinue the provision of its services.[146]

4. **Existence of Grievance Officer: Yes**

a. Rationale:

Though not directly mentioned in the Privacy Policy, a separate, easily noticeable link at the bottom of each webpage links to the Customer Grievance section. There are different officers in charge of each node, called the Nodal Officers.[147]

5. **Purpose of Collection and usage of information: Partial**

a. **Rationale:** The usage of the term 'may' in the section of the Privacy Policy regarding the purpose of collection and usage of information again leaves it ambiguous in this regard, implying that it can just as easily be used for purposes that have not been notified to the data subject.[148]

---

146. In case a customer does not provide information or consent for usage of personal information or later on withdraw consent for usage of the personal information so collected, Aircel reserves the right to discontinue the services for which the said information was sought.
147. In case of any feedback or concern regarding protection of personal information, customers can contact Aircel's **Circle Care ID.** Alternatively, one may also direct your privacy-related feedback or concerns to the **Circle Nodal Officer.** (e.g. – Delhi Circle Nodal details are as mentioned below):

1. Name: Moushumi De
Contact Number: 9716199209
E-mail: nodalofficer.delhi@aircel.co.in
Further it provides for a general customer grievance redressal mechanism
Additionally details of the Grievance Redressal Officers is provided via the TRAI website.
To resolve all concerns, Aircel has established a 2-tier complaint handling mechanism. Level I: Our Customer Touch Points As an Aircel customer you have the convenience to contact at Customer Interface Points via email, post or telephone.**Level II - Appellate Authority**Despite the best efforts put by Aircel's executive, if a customer is still not satisfied with the resolution provided then he/she may submit his/her concern to the Appellate Authority of the circle. Comments - However this information contradicts the mechanism provided under Aircel's Manual of Practice for handling Consumer Complaints which provides for a 3-tier complaint handling mechanism.
[According to the DoT – The **earlier three-tier complaint redressal mechanism – Call center, Nodal Center and Appellate Authority, has been replaced by a two-tier** one by doing away with the level of Nodal Officer. This is because the Complaint Centres are essentially registration and response centres and do not deal with the resolution of complaints. They only facilitate registration of consumer complaint and the level at which a problem is resolved within a company depends upon the complexity of the issue involved.]

148. It may be used by us for a number of purposes connected with our business operations and functions, which include:
1. Processing customer orders or applications.
2. Carrying out credit checking and scoring (unless agreed otherwise).
3. Providing customers with products and/or services requested (including the presentation or elimination of calling or connected line identification) or administering a customer's account.
4. Billing (unless there exists another agreed method).
5. Settling accounts with those who provide related services to Aircel.
6. Dealing with requests, enquiries or complaints and other customer care related activities; and all other general administrative and business purposes.
7. Carrying out market and product analysis and marketing our and our group companies' products and services generally.
8. Contacting customers (including by post, email, fax, short text message (SMS), pager or telephone) about Aircel and its group companies' products and services and the products and services of carefully selected third parties which it think may be of interest to a customer (unless a customer says 'no' in writing). Electronic messages need not have an unsubscribe facility.

6. **Disclosure of Information: Yes**

a. **Rationale:** Though the Privacy Policy does not specify all the circumstances under which Aircel would share the collected information with a third party, it specifies the terms and conditions that would apply in the cases that it does.[149]

7. **Reasonable Security practices and procedures: Yes**

a. Rationale:

The Policy gives a reasonable amount of detail about the steps taken by Aircel to ensure the security of the information collected by it, but leaves certain holes uncovered.[150]

---

9. Registering customer details and allocating or offering rewards, discounts or other benefits and fulfilling any requests that customers may have in respect of Aircel and its group companies' loyalty or reward programmes and other similar schemes.
10. Inclusion in any telephone or similar directory or directory enquiry service provided or operated by Aircel or by a third party (subject to any objection or preference a customer may have indicated in writing).
11. Carrying out any activity in connection with a legal, governmental or regulatory requirement on Aircel or in connection with legal proceedings, crime or fraud prevention, detection or prosecution.
12. Carrying out activities connected with the running of business such as personnel training, quality control, network monitoring, testing and maintenance of computer and other systems and in connection with the transfer of any part of Aircel's business with respect to a customer or potential customer. Aircel may use cookies and other interactive techniques such as web beacons to collect non-personal information about how customers interact with our website, and web-related products and services, to:

- Understand what a customer likes and uses about Aircel's website.
- Provide a more enjoyable, customised service and experience

Aircel may use a persistent cookie to record details such as a unique user identity and general registration details on your Personal Computer.

149. Where Aircel needs to disclose your information to third parties, such third parties will be:

1. Group companies who may use and disclose your information for the same purposes as us.
2. Those who provide to Aircel or its group companies products or services that support the services that we provide, such as our dealers and suppliers.
3. Credit reference agencies (unless we have agreed otherwise) who may share your information with other organisations and who may keep a record of the searches Aircel make against your name.
4. If someone else pays a customer's bill, such as an employer.
5. Those providing telephone and similar directories or directory enquiry services.
6. Anyone Aircel transfers its business to in respect of which you are a customer or a potential customer.
7. Anyone who assists Aircel in protecting the operation of the Aircel networks and systems, including the use of monitoring and detection in order to identify potential threats, such as hacking and virus dissemination and other security vulnerabilities.
8. Persons to whom Aircel may be required to pass customer information by reason of legal, governmental or regulatory authority including law enforcement agencies and emergency services. If a customer has opted in to receiving marketing material from Aircel, it may also provide personal information to carefully selected third parties who it reasonably believes to provide products or services that may be of interest to customers and who have contracted with Aircel to keep the information confidential, or who are subject to obligations to protect customer personal information.

150. We adopt reasonable security practices and procedures to include, technical, operational, managerial and physical security control measures in order to protect your personal information from unauthorized access, or disclosure while it is under our control.Our security practices and procedures limit access to personal information on need to know basis. Further, our employees, to the extent they may have limited access to your personal information on need to know basis, are bound by Code of Conduct and Confidentiality Policies which obligate them to protect the confidentiality of personal informationWe take adequate steps to ensure that our third parties adopt reasonable level of security practices and procedures to ensure security of personal information

We may retain your personal information for as long as required to provide you with services or if otherwise required under any law. We, however assure you that Aircel does not disclose your personal information to unaffiliated third parties (parties outside Aircel corporate network and its Strategic and Business Partners) which could lead to invasion of your privacy

4. **Atria Convergence Technologies Private Limited (ACT)**
    1. **Clear and Accessible statements of its practices and policies: Yes**

    a. **Rationale:** The Policy is intelligible, and is easily accessible from all the webpages of the company's website from a link at the bottom of all pages.[151]
    2. **Type of personal or sensitive personal data/information collected: Partial**

    a. Rationale:
        Type –

    a. Personal Information – Yes –

The Policy mentions the different types of Personal Information which will be collected by ACT if the customer registers with the Company.[152]

    a. Sensitive Personal Data or Information –

The categories of SPD/I collected by ACT are not specifically mentioned in the policy, though they are mentioned as part of the general declarations.

    3. **Option to not provide information and withdrawal of consent: No**

    a. **Rationale**: The option of the data subject not providing or withdrawing consent has not been mentioned in the Policy.
    4. **Existence of Grievance Officer: No**

    a. **Rationale:** No Grievance Officer has been mentioned in the Privacy Policy or on the ACT website, nor has any other grievance redressal process been specified.[153]
    5. **Purpose of Collection and usage of information: Yes**

When we dispose off your personal information, we use reasonable procedures to erase it or render it unreadable (for example, shredding documents and wiping electronic media).
We will take reasonable steps to ensure that the personal information we collect, use or disclose is accurate, complete, up-to-date and stored in a secure environment protected from unauthorised access, modification or disclosure. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the personal information you provide on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol. If a password is used to help protect your accounts and personal information, it is your responsibility to keep your password confidential. Do not share this information with anyone. If you are sharing a computer with anyone you should always log out before leaving a site or service to protect access to your information from subsequent users.
We make every effort to maintain the security of our internet connections; however for reasons outside of our control, security risks may still arise. Any personal information transmitted to us or from our online products or services will therefore be your own risk, however we will use our best efforts to ensure that any such information remains secure.

151. http://www.acttv.in/index.php/privacy-policy
152. "When you register, we ask for information such as your name, email address, birth date, gender, zip code, occupation, industry, and personal interests.
The Company collects information about your transactions with us and with some of our business partners, including information about your use of products and services that we offer."
153. Not provided for on the TRAI website as ACT is not a telecom.

a. **Rationale:** The Policy mentions the various ways ACT might use the information it collects, though the use of the term 'general' is a cause for concern.[154] The list of purposes for collection given in the Privacy Policy is a very general list.

6. Disclosure of Information: Yes

a. **Rationale:** The Policy mentions the circumstances in which ACT might share the collected information with a third party, and also mentions that such parties will either be subject to confidentiality agreements, or that the data subject will be notified before his or her information becomes subject to a different privacy policy. It also mentions the exception to above, that being when the information is shared for investigative purposes.[155] At the same time, the intended recipients of the information are not mentioned, and the name and address of agency/agencies collecting and retaining information is not mentioned.

7. Reasonable Security practices and procedures: No

a. **Rationale:** – The security practices and procedures followed by ACT to protect the information of its customers are not mentioned in the Policy, which is a critical weak point, keeping in mind the requirements of the Rules.[156]

154. The Company can use information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.
The Company collects personal information when you register with the Company, when you use the Company products or services, when you visit the Company pages or the pages of certain partners of the Company. The Company may combine information about you that we have, with information we obtain from business partners or other companies. The Company shall have the right to pass on the same to its business associates, franchisees without referring the same to you.

155. Aircel provide the information to trusted partners who work on behalf of or with the Company under confidentiality agreements. These companies may use customer personal information to help the Company communicate about offers from the Company and marketing partners.
Aircel believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of the Company's terms of use, or as otherwise required by law.
Aircel transfer information about a customer if the Company is acquired by or merged with another company under a different management. In this event, the Company will notify a customer before information about a customer is transferred and becomes subject to a different privacy policy.
The Company plans to display targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click on targeted ads meet the targeting criteria - for example, women ages 18-24 from a particular geographic area.
The Company will not provide any personal information to the advertiser when customers interact with or view a targeted ad. However, by interacting with or viewing an ad a customer consents to the possibility that the advertiser will make the assumption that he/she meets the targeting criteria used to display the ad.

156. Rule 8.