
CENTRE FOR INTERNET & SOCIETY

# RANKING DIGITAL RIGHTS IN INDIA

DRAFT REPORT

## BACKGROUND

This report is a study of five Indian telecommunication companies (Tata Communications Ltd., Reliance Communications Limited, Aircel Limited, Vodafone India Private Limited and Reliance Jio Infocomm Limited) and three Indian online service providers (Hike Messenger, Shaadi.com and Rediff.com). The report is an attempt to evaluate the practices and policies of companies which provide internet infrastructure or internet services, and are integral intermediaries to the everyday experience of the internet in India. The report draws upon the methodology of Ranking Digital Rights project, which analysed 16 of the world's major internet companies, including internet services and telecommunications providers based on their commitment towards upholding human rights through their services – in particular towards their commitment to users' freedom of expression and privacy. The report comprehensively assessed the performance of companies on various indicators related to these human rights, as per information which was made publicly available by these companies or was otherwise in the public domain. This report follows the methodology of the proposed 2017 Ranking Digital Rights index, updated as of October 2016.[1]

This report studied Indian companies which have, or have had, a major impact on the use and experience of the Internet in India. The companies range from online social media and micro-blogging platforms to major telecommunications companies providing critical national communications infrastructure. While some of the companies have operations outside of India as well, our study was aimed at how these companies have impacted users in India. This allowed us to study the impact of the specific legal and social context in India upon the behaviour of these firms, and conversely also the impact of these companies on the Indian internet and its users.

[1] For more information about the detailed methodology followed, please see - *https://rankingdigitalrights.org/wp-content/uploads/2016/07/RDR-revised-methodology-clean-version.pdf.*

VSNL, the company later to be acquired by and merged into TATA Communications, was the first company to provide public Internet connections to India, in 1996. In 2015, India surpassed the United States of America, as the jurisdiction with the worlds second-largest internet user base, with an estimated 338 million users.[2] With the diminishing costs of wireless broadband internet and the proliferation of cheaper internet-enabled mobile devices, India is expected to house a significant number of the next billion internet users.

Concomitantly, the internet service industry in India has grown by leaps and bounds, particularly the telecommunications sector, a large part of whose growth can be attributed to the rising use of wireless internet across India. The telecom/ISP industry in India remains concentrated among a few firms. As of early 2016 just three of the last mile ISPs which are studied in this report, are responsible for providing end-user connectivity to close to 40% of mobile internet subscribers in India.[3] However, the market seems to be highly responsive to new entrants, as can be seem from the example of Reliance Jio, a new telecom provider, which has built its brand specifically around affordable broadband services, and is also one of the companies analysed in this report.[4] As the gateway service providers of the internet to millions of Indian users, these corporations remain the focal point of most regulatory concerns around the Internet in India, as well as the intermediaries whose policies and actions have the largest impact on internet freedoms and user experiences.

Besides the telecommunications companies, India has a thriving internet services industry – by some estimates, the Indian e-commerce industry will be worth 119 Billion USD by 2020.[5] While the major players in the e-commerce industry are shipping and food aggregation services, other companies have emerged which provide social networking services or mass-communication platforms including micro-

---

[2] Internet Users Per 100 People, WORLD BANK, *available at http://data.worldbank.org/indicator/IT.NET.USER.P2.*

[3] Telecommunications Indicator Report, TELECOM REGULATORY AUTHORITY OF INDIA, *available at* http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator_Reports.pdf.

[4] The upstaging of extant telecos did, however, lead to allegations of anti-competitive practices by both Jio as well as existing telecos such as Vodafone and Airtel. *See* http://thewire.in/64966/telecom-regulator-calls-time-out-as-reliance-jio-coai-battle-turns-anti-consumer/.

[5] *Get Ready for India's Internet Boom,* MORGAN STANLEY, *available at* http://www.morganstanley.com/ideas/rise-of-internet-in-india.

blogging platforms, matrimonial websites, messaging applications, social video streaming services, etc. While localised services, including major e-commerce websites (Flipkart, Snapdeal), payment gateways (Paytm, Freecharge) and taxi aggregators (Ola), remain the most widely utilized internet services among Indians, the services analysed in this report have been chosen for their potential impact they have upon the user rights analysed in this report – namely freedom of speech and privacy. These services provide important alternative spaces of localised social media and communication, as alternatives to the currently dominant services such as Facebook, Twitter and Google, as well as specialised services used mostly within the Indian social context, such as Shaadi.com, a matrimonial match-making website which is widely used in India. The online service providers in this report have been chosen on the basis of the potential impact that these services may have on online freedoms, based on the information they collect and the communications they make possible.

## LEGAL AND REGULATORY FRAMEWORK

### a. CORPORATE ACCOUNTABILITY IN INDIA

Corporate accountability and its intersection with human rights is a particularly relevant topic in India's post-liberalisation economy, where public functions are increasingly being taken upon by private corporations, although acting within the bounds of government regulation. While India has several pro-consumer laws and comprehensive corporate regulations, there are few government initiatives to measure the impact of various corporate actions upon human rights, and the structures for corporate accountability towards human rights remain rather lax. While corporate actions and accountability towards shareholders are monitored and comprehensively regulated, there is no well developed system for ensuring public accountability for corporate actions.

In the last decade, there has been a major push towards corporate social responsibility ("CSR") in policy. In 2009, the Securities Exchange Board of India mandated all listed public companies to publish 'Business Responsibility Reports' disclosing efforts taken

towards, among other things, human rights compliances by the company.[6] The new Indian Companies Act, 2013 introduced a 'mandatory' CSR policy which enjoins certain classes of corporations to maintain a CSR policy and to spend a minimum percentage of their net profits towards activities mentioned in the Act.[7] However, these provisions do not do much in terms of assessing the impact of corporate activities upon human rights or enforcing human rights compliance.

### b. PRIVACY AND DATA PROTECTION IN INDIA

There is no explicit right to privacy under the Constitution of India. However, such as right has been judicially recognized as being a component of the fundamental right to life and liberty under Article 21 of the Constitution of India.[8] However, there have been varying interpretations of the scope of such a right, including who and what it is meant to protect. The precise scope of the right to privacy, or whether a general right to privacy exists at all under the Indian Constitution, is currently being adjudicated by the Supreme Court.[9] Although the Indian Supreme Court has had the opportunity to adjudicate upon telephonic surveillance conducted by the Government,[10] there has been no determination of the constitutionality of government interception of online communications, or to carry out bulk surveillance.

As per Section 69 of the Information Technology Act, the primary legislation dealing with online communications in India, the government is empowered to monitor, surveil and decrypt information, *"in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence*

---

6 *Circular on Business Responsibility Reports*, SECURITES EXCHANGE BOARD OF INDIA, (August 13, 2012), available at http://www.sebi.gov.in/cms/sebi_data/attachdocs/1344915990072.pdf.

7 *FAQ on Corporate Social Responsibility*, MINISTRY OF COPORATE AFFAIRS, available at https://www.mca.gov.in/Ministry/pdf/FAQ_CSR.pdf.

8 Govind vs. State of Madhya Pradesh, (1975) 2 SCC 148; R. Rajagopal vs. State of Tamil Nadu (1994) 6 S.C.C. 632; PUCL v. Union of India, AIR 1997 SC 568; Distt. Registrar & Collector vs Canara Bank, AIR 2005 SC 186.

9 Justice K.S. Puttaswamy (Retd.) & Another Versus Union of India & Others, *available at* http://judis.nic.in/supremecourt/imgs1.aspx?filename=42841

10 PUCL v Union of India, AIR 1997 SC 568.

*relating to above or for investigation of any offence."* Moreover, intermediaries, as defined under the act,[11] are required to provide facilities to enable the government to carry out such monitoring. The specific procedure to be followed during lawful interception of information is given under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, ("Interception Rules")[12] which provides a detailed procedure for government agencies to issue monitoring directions as well as the obligations of intermediaries to facilitate the same. The Interception Rules require intermediaries who are enlisted for facilitating monitoring of information to maintain strict confidentiality regarding such directions for lawful interception or decryption, as well as to destroy any records of such directions every six (6) months.[13] Intermediaries are required to designate specific authorities (the designated authority) to receive and handle any of the above government directions and also to maintain records and provide proper facilities to the government agencies.[14] The designated authority is also responsible for maintaining the security and confidentiality of all information which 'affects the privacy' of individuals. Further, the rules prescribe that no person may intercept any online communication or information, except the intermediary for the limited purposes specified in the rules, which include for tracing persons who may have contravened any provision of the IT Act or rules.[15]

With respect to decryption, besides the government's power to order decryption of content as described above, the statutory license between the telecommunications providers and the Department of Telecommunications ("DoT"), prescribes, among other things, that only encryption *"up to 40 bit key length in the symmetric algorithms or its equivalent in others"* may be utilized by any person, including an intermediary. In the case that any person utilizes encryption stronger than what is prescribed, the

---

11 According to Section 2(w) of the IT Act, *"Intermediary" with respect to any particular electronic records, means "…any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes."*

12 *See* http://cis-india.org/internet-governance/resources/it-procedure-and-safeguards-for-interception-monitoring-and-decryption-of-information-rules-2009

13 Rule 23, Interception Rules.

14 Rule 19 & 20, Interception Rules.

15 Rule 24, Interception Rules.

decryption key must be stored with the DoT.[16] At the same time, the license prescribes that ISP's must not utlilize any hardware or software which makes the network vulnerable to security breaches, placing intermediaries in a difficult position regarding communications privacy.. Moreover, the license (as well as the Unified Access Service License) prohibit the use of bulk encryption by the ISP for their network, effectively proscribing efforts towards user privacy by the ISP's own initiative.[17]

There is no statute in India generally governing data protection or for the protection of privacy. However, statutory rules address privacy concerns across different sectors, such as banking and healthcare. A more general regulation for data protection was enacted under Section 43A of the Information Technology Act, 2000 ("IT Act") and the rules made thereunder, in particular, the Information Technology (Reasonable Security Practices and Procedures and sensitive personal data or information) Rules, 2011 ("Rules").[18] Section 43A requires body corporates (defined as any company) handling sensitive personal information, (as defined under the IT Act and Rules), to maintain reasonable security practices regarding handling such information, and penalises failure to maintain such practices, in case it causes 'wrongful loss or wrongful gain to any person.' The Rules prescribed under Section 43A detail the general obligations of body corporates that handle sensitive personal information more comprehensively.

The Rules specify that all body corporates which *"collects, receives, possess, stores, deals or handle information"*, directly from the holder of such information through a lawful contract,[19] shall provide a privacy policy, which must – (a) be clearly accessible; (b) specify the data collected; (c) specify the purpose for collection and the disclosure of such information and; (d) specify the reasonable security practices for the protection of such data. There are also specific requirements for body corporates

---

16 *See* http://tikona.in/sites/default/files/pdf_using_mpdf/1-ISP%20Agreement%20Document.pdf.

17 Pranesh Prakash and Jarpreet Grewal, *How India Regulates Encryption*, CENTRE FOR INTERNET AND SOCIETY, (October 30, 2015) *available at* *http://cis-india.org/internet-governance/blog/how-india-regulates-encryption*.

18 *See* http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.

19 As clarified in a Central Governemnt Press Note, this does not apply to corporates collecting data from other corporations, but only those handling data directly from natural persons, *See* http://meity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf.

which handle sensitive personal information, which includes obtaining consent from the data subject, and permitting data collection for a specified and limited purpose as well as a limited time. The body corporate is also supposed to ensure the data subject is aware of: (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of he agency that is collecting the information as well as the agency that will retain the information. The rules also require the body corporate to provide an explicit option for users to opt-out of having their personal information collected, which permission can also be withdrawn at any time.

Apart from the above, the IT (Intermediary Guidelines) Rules, 2011, ("Guidelines) also contain a prescription for providing information to government agencies, although the rules have been enacted under the provisions of the safe-harbour conditions of the IT Act. Rule 3(7) of the Guidelines states that "…*When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance."* While this regulation outside the scope of the rule-making power under Section 79 of the IT Act, it continues to remain in force, although the extent to which it is utilized to obtain information is unknown.

### c. Content Restriction, Website blocking and Intermediary Liability in India

Section 79 of the IT Act contains the safe harbor provision for intermediaries, sheltering them from liability, under specific circumstances, against information, data, or communication links made available by any third party. For the safe harbor to apply, the role of the intermediaries must be limited to (a) providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) a platform which does not initiate

the transmission, modify it or select the receiver of the transmission. Moreover, the safe-harbour does not apply when the ISP has received actual knowledge, or been notified by the appropriate government agency, about potentially unlawful material which the intermediary has control over, fails to act on such knowledge by disabling access to the material.[20]

The Central Government has further prescribed guidelines under Section 79 of the IT Act, which intermediaries must comply with to have the shelter of the safe harbor provisions.[21] The guidelines contain prescriptions for all intermediaries to inform their users, through terms of service and user agreements, of information and content which is restricted, including vague prescriptions against content which is *"...grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise*

---

[20] *Section 79 – 'Exemption from liability of intermediary in certain cases - (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.*

*(2) The provisions of sub-section (1) shall apply if-*

*(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or*

*(b) the intermediary does not-*

*(i) initiate the transmission,*

*(ii) select the receiver of the transmission, and*

*(iii) select or modify the information contained in the transmission*

*(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf*

*(3) The provisions of sub-section (1) shall not apply if-*

*(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)*

*(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in orconnected to a computer resource controlled by the intermediary is being used to*

*commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.*

*Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.*

[21] Information Technology (Intermediaries guidelines) Rules, 2011, *available at* http://dispur.nic.in/itact/it-intermediaries-guidelines-rules-2011.pdf.

*unlawful in any manner whatever;"* or that infringes any proprietary rights (including Intellectual Property rights).

Rule 3(4) is particularly important, and provides the procedure to be followed for content removal by intermediaries. This rule provides that any intermediary, who hosts, publishes or stores information belonging to the above specified categories, shall remove such information within 36 hours of receiving 'actual knowledge' about such information by any 'affected person'. Further, any such flagged content must be retained by the intermediary itself for a period of 90 days. The scope of this rule led to frequent misuse of the provision for removal of content. As non-compliance would make the intermediaries liable for potentially illegal conduct, intermediaries were found to be eager to remove any content which was flagged as objectionable by any individual. However, the scope of the rule received some clarification from the Supreme Court judgement in Shreya Singhal v Union of India.[22] While the Supreme Court upheld the validity of Section 79 and the Guidelines framed under that section, it interpreted the requirement of 'actual knowledge' to mean the knowledge obtained through the order of a court asking the intermediary to remove specific content. Further, the Supreme Court held that any such court order for removal of restriction must conform Article 19(2) of the Constitution of India, detailing permissible restrictions to the freedom of speech and expression.

For the enforcement of the above rules, Rule 11 directs intermediaries to appoint a Grievance Officer to redress any complaints for violation of Rule 3, which must be redressed within one month. However, there is no specific mention of any remedies against wrongful removal of content or mechanisms to address such concerns.

Apart from the above, there is a parallel mechanism for imposing liability on intermediaries under the Copyright Act, 1957. According to various High Courts in India, online intermediaries fall under the definition of Section 51(a)(ii), which includes as an infringer, *"…any person who permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no*

---

[22] AIR 2015 SC 1523.

*reasonable ground for believing that such communication to the public would be an infringement of copyright."*

Section 52(1) provides for exemptions from liability for infringement. The relevant part of S.52 states –

*"(1) The following acts shall not constitute an infringement of copyright, namely:*

*(b) the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public;*

*(c) transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy:*

*Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of twenty-one days or till he receives an order from the competent court refraining from facilitating access and in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access;"*

While Section 52 of the Act provides for safe harbour for certain kinds of online intermediaries, this does not apply where the intermediary has 'reasonable grounds for believing' that storage is an infringing copy, similar to language used in 51(a)(ii), which has been broadly interpreted by high courts. The procedure for notifying the intermediary for taking down infringing content is given in the Rules prescribed under the Copyright Act, which requires that the holder of the Copyright must give written notice to the intermediary, including details about the description of work for identification, proof of ownership of original work, proof of infringement by work sought to be removed, the location of the work, and details of the person who is responsible for uploading the potentially infringing work. Upon receipt of such a notice, the intermediary must disable access to such content within 36 hours. Further, intermediaries are required to display reasons for disabling access to anyone trying to access the content. However, the intermediary may restore the content after 21 days if no court order is received to endorse its removal, although this is not a requirement.

After this notice period, the intermediary may choose not to respond to further notices from the same complainant about the same content at the same location.

Besides the safe harbour provisions, which require intermediaries to meet certain conditions to avoid liability for content hosted by them, intermediaries are also required to comply with government blocking orders for removal of content, as per Section 69A of the IT Act. This section specifies that the government may, according to the prescribed procedure, order any intermediary to block access to any information "in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above." Failure to comply by the intermediary results in criminal penalties for the personnel of the intermediary.

The procedure for blocking has been prescribed in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.[23] The Rules under Section 69A allow any Central Government or State Government ministry or department to issue blocking requests, which may be made by any person to specific departmental representatives known as 'nodal officers', may request the blocking of access to content by any intermediary. The nodal officers forward such requests for blocking of access to the 'designated officer', who is an officer of the Central Government not below the rank of the joint secretary, as nominated by the Central Government. The blocking request is then considered by a committee which recommends whether the designated officer should approve such request or not. Once approved, the request is forwarded to the intermediary, who must nominate at least one person to handle all such requests. In case of non-compliance, the designated officer may initiate action under Section 69A against the intermediary.

The rules contain some safeguards to ensure due process before blocking orders are made. The designated officer is required to make 'reasonable efforts' to locate the user or intermediary who has hosted the content and allow for such person or intermediary to appear before the committee to submit their reply and clarifications. Rule 9 lays down the emergency procedure for blocking in which case the above detailed

[23] *See* http://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009.

procedural safeguards such as the committee deliberation or providing a hearing are dispensed with. However, Rule 16 requires the confidentiality of all such requests and actions taken under the rules, which defeats any attempts at the transparency or fairness of the process.

Finally, the ISP and Unified Services License (USL) issued by the DoT prescribe further obligations to block content.[24] Under Clause 38 of the USL, for example, ISP's must take measures to prevent the *"flow of obscene, objectionable, unauthorised or any other content infringing copy-rights, intellectual property right and international & domestic Cyber laws in any form"* over their network. Moreover, as per Clause 7 of the USL, the licensee is obliged to block subscribers as well as content, as identified by the Licensor (DoT). Failure to comply with license conditions can lead to the cancellation of the telecommunication operators license with the DoT, without which they are not permitted to operate in India.

[24] License Agreement For Unified License, *available at* http://www.dot.gov.in/sites/default/files/Amended%20UL%20Agreement_0_1.pdf?download=1.

## General

- ***Most companies' policies are only tailored towards minimum compliance with national regulations;***

1. As detailed in the above sections, companies are mandated by law to comply with certain procedures including data protection and content restriction policies. While compliance with these regulations also varies from company to company, there are barely any instances of companies taking initiative to ensure better privacy procedures than mandated by law, or to go beyond human rights reporting requirements as detailed in corporate social responsibility regulations. For example, Vodafone was the only company in this index to disclose (even in a limited manner) government requests for user information or for content restriction.
2. While compliance with regulations is an understandable threshold for companies to maintain, companies should make efforts to at least explain the import of the regulations to their users and explain how their policies are likely to affect their users' rights.

- ***Company policies are usually tailored towards regulations in specific regulations;***

3. Jurisdiction is a major issue in regulating internet services. Internet service providers may operate and have users in several jurisdictions, but their policies do not always meet the requirements of each jurisdiction in which they operate, where there services are accessed. Even in cases of large ISPs which operate across jurisdictions, the policies may be tailored to specific jurisdictions. Tata Communications Ltd. for example, specifically references the law of the United States of America in its policies, though the same policies may operate for users in other jurisdictions. This is problematic since most company policies have

accession to the terms as a condition of service, which means that restrictions (or protections, as the case may be) on user rights placed in one jurisdiction can be responsible for similar restrictions across the board in several jurisdictions.

- ***Companies do not seek meaningful consent from their users before subjecting them to their policies;***

4. The study highlights the importance of company policies to users rights. These policies define the relationship between the service provider and the user, including delimiting the rights available to users and their control over the information collected from them (often automatically). However, most companies take very little effort in obtaining meaningful user consent towards their policies, including efforts towards educating users about the import of their policies. In many cases, mere use of the service is mentioned as a sufficient condition for making the policies binding upon the users. Even in other cases, where notice of policies is more prominent, few efforts are made to ensure that users fully understand the scope and effect of the policies.

5. Further, while most companies have committed to informing users of changes to their policies in some form, only Reliance Jio disclosed that it directly informed users of changes to policies, subject to its discretion; while others did not maintain any clear standard for notice to changes to policies. None of the companies provided access to any archives where changes to the company policies could be reviewed.

6. It is apparent that most companies do not take much effort in maintaining robust or meaningful terms and conditions or privacy policies, which include an explanation of how the service could potentially affect a user's privacy or freedom of expression. Nor do most companies attempt to take safeguards for protecting such freedoms beyond complying with regulations. Only Shaadi.com commits to informing users about data protection and how to take reasonable steps for ensuring their online privacy, above and beyond the regulations.

*7.* Finally, a study of TCL's policy indicates that in some cases, the actions or policies of upstream providers (backbone internet providers such as TCL), can affect users' experience of the internet without their consent or even notice, since these terms must be complied with by the last-mile provider to whom the users may connect.

*8.* The formalistic manner in which these policies are framed and worded effectively prevents many users from understanding their import upon online freedoms. Companies which are serious about committing to human rights should take steps towards making their policies easily accessible, and to clearly explain the scope of their policies and their impact on users' online human rights in an easy and understandable manner instead of a formalistic, legal statement which is not accessible to lay users. Companies should also take steps towards educating users about how to protect their online freedoms while utilizing the services of the company.

- ***Indian regulations hinder transparency and prevent companies from being accountable to their users;***

*9.* The regulations outlined in Part – I of this report are telling in the broad restrictions they place on company transparency, in particular for disclosing any information about government requests for user information, or government or third party requests for content restriction. The policies are vaguely worded and broad in their confidentiality requirements, which potentially causes a chilling effect around the release of even aggregate or depersonalized information by companies.

***10.*** Government regulations often provide the framework around which company policies operate. Regulators must include principles for safeguarding online freedom of expression and privacy as a fundamental part of their regulations. This includes clearly specifying the scope of confidentiality requirements as a response to government requests and to enable some form of transparency and oversight.

**Commitment**

- ***Most companies do not adequately disclose efforts towards assessing their impact on online freedoms or compliance with the same;***

*11.* Except Vodafone India (through Vodafone plc, its parent company), none of the companies surveyed in this report have disclosed any assessments of the impact of their services on online freedom of speech or privacy. The lack of such disclosures indicates companies' lack of concern over ensuring transparency in such issues.

*12.* Although no legal framework exists for such assessment, companies must independently assess the impact of their services upon basic online freedoms as the first step towards committing to protecting those freedoms, possibly through a third party such as the Global Network Initiative. The findings from these assessments should, to the extent possible, be made public.

- ***Some companies have implemented internal policies for training on and to monitor compliance with online freedoms;***

*13.* Some companies have disclosed internal mechanisms which emphasise on protecting online freedoms, for example, through employee training on such issues. These internal policies are an important aspect of accountability for company processes which are generally outside of public oversight. Four of the eight companies surveyed, for example, have whistle-blower policies protecting the internal reporting of violations of 'ethical conduct'. In addition, some companies, for example Tata Communications and Aircel disclose an internal code of ethics and measures for ensuring compliance with the same. Similarly, Vodafone discloses the existence of a Privacy Management System for training employees on the importance of customer privacy.

*14.* While some companies have robust internal processes for accountability, companies should also specify that these processes explicitly deal with concerns about user privacy or censorship, above and beyond general requirements for ethical conduct.

- ***Companies do not disclose direct efforts to lobby against regulatory policies which negatively impact online freedoms;***

*15.* None of the companies disclosed efforts towards directly lobbying for clearer regulations on government censorship of online privacy. However, the lack of transparency could possibly be attributed to the nature of the public consultancy process by Indian regulators. In fact, where the consultancy process is made public and transparent, companies have shown efforts at engaging with regulators. For example, several of the companies studied in this report have responded to the TRAI's call for public comments on the network neutrality framework for the Indian internet, including TCL, Airtel, Aircel and Vodafone India.

***16.*** The obvious implication for regulators is to improve the public consultancy process and attempt to engage stakeholders in a more transparent manner. Companies should also put regulatory pressure against regulations which stifle free speech or user privacy, if not through legal challenges, through public statements against regulatory overreach or oversight in these areas.

- ***However, companies are making efforts towards better regulation through industry groups, particularly for privacy and data protection;***

*17.* Most telecommunication companies surveyed in this report are members of some industry body which advocates in favour of protecting online freedoms. In particular, the companies are members of associations such as the Data Security Council of India or the Internet Service Providers Association of India, which commit to protecting different aspects of users rights. The DSCI, for example, is an influential industry association which lobbies for better regulations for data protection. However, there are few such associations actively committed towards tackling private or governmental censorship online.

*18.* While industry bodies are a growing voice in lobbying efforts towards better regulation, companies should also participate in civil society forums which advocate for protecting online freedoms.

- ***All companies disclose some forum for grievance redressal, however, none of these specifically address freedom of speech and privacy issues;***

*19.* All the companies surveyed have disclosed some forum for grievance redressal. As indicated above, this forum is also a statutory requirement under both the Reasonable Security Practices Rules and the Intermediaries Guidelines Rules under the IT Act. In most cases, however, these policies do not specify whether and to what extent the grievance redressal forum addresses issues of online censorship or privacy concerns, although some companies, such as Vodafone, have specifically designated Privacy Officers. Only Aircel, TCL and RCL disclosed an appellate process or timelines for resolution of complaints. Further, Aircel is the only company in this report which disclosed aggregate data of complaints received and dealt with.

*20.* Companies must take steps towards improving customer protection, particularly in cases involving violations of online freedoms. Grievance redressal by the company is generally the first step towards addressing rights violations and can also prevent future legal problems which the company may face. Further, companies should be transparent in their approach towards resolving customer grievances, and should publish aggregate data including complaints received and resolved, and to the extent possible, classifying the nature of the complaints received.

**Freedom of Speech**

- ***Most companies do not disclose processes or safeguards in case of content restriction requests by private third parties or by the government;***

*21.* Few of the companies surveyed have any form of checking misuse by government or third parties of blocking procedures prescribed under their terms and conditions. Some policies, such as TCL's acceptable use policy, specifies that the company shall attempt to contact the owner of the content upon notice of private requests for content restriction, however, this requirement is entirely discretionary.

*22.* Some companies, such are Rediff, have a well-defined procedure for content restriction on intellectual property claims, but not in case of general content restriction measures.

*23.* However, there is evidence that at least some of the companies do provide some notice to users when the information they attempt to access has been removed or blocked by court order. TCL, for example, redirects users to a notice stating that

the information has been blocked as per the provisions of a specific law. However, this does not reflect in its policies.

*24.* Companies must have internal procedural safeguards to ensure the authenticity of content restriction claims and their compliance with regulations. Companies must commit to objecting against overbroad requests for restriction. One important step in this regard is to clarify the scope of companies liabilities as intermediaries, for actions taken in good faith.

*25.* Companies must also provide clear and detailed notice to both users attempting to access blocked content as well as to the person whose content has been restricted. Such notice must specify whether the removal was due to a judicial, executive or privacy order, and to the extent possible, should specify the law, regulation or company policy under which the content has been restricted.

- ***Companies do not disclose internal processes on content restriction or termination of services taken independently of third party requests;***

*26.* None of the companies disclosed their process for removal of content independently of third party requests, for the enforcement of their terms. None of the company policies disclose processes for identification or investigation of any violation of their terms. In fact, many companies, including Rediff, Hike Messenger and Vodafone expressly state that services may be terminated without notice and entirely at the discretion of the service provider.

*27.* Further, none of the companies surveyed disclose their network management principles or make any public commitments against throttling of blocking of specific content or differential pricing, although, some of the telecommunications companies did vouch for some form of network neutrality, in their response to the TRAI's public consultation on network neutrality regulations. As an outcome of those consultations, regulations now effectively prevent telecoms from discriminatory tariffs based on the nature of content.[25]

---

*25* http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf.

*28.* Company processes for enforcement of their terms of use must be disclosed. Further, companies should commit to transparency in the enforcement of the terms of use, to the extent possible.

**Privacy**

- ***Company practices on data protection vary widely – most companies show some commitment towards users' privacy, but fall short on many grounds***

*29.* Despite the existence of a privacy regulation (the Reasonable Security Practices Rules), company practices on data collection vary. Some companies, such as TCL, have robust commitments towards important privacy principles including user consent and collection limitation, however, on the other end of the spectrum, RCL does not have a publicly available privacy policy governing the use of its internet services. In fact, none of the companies have data collection policies which contain the minimum safeguards as expected from such policies, such as compliance with the OECD Privacy Principles, or the National Privacy Principles as laid out in the A.P. Shah Committee Report on Privacy.[26]

*30.* Most of the companies surveyed make some form of commitment to notifying users of the collection and use of their data, including specifying the purposes for which information would be used and specifying the third parties with whom such information may be shared, and the option to opt-out of sharing their data with third parties. However, none of the policies explicitly commit to limiting collection of data to that which is necessary for the service. Further, while companies generally specify that data may be shared with 'third parties', usually for commercial purposes, theses parties are usually not explicitly mentioned in the policies.

*31.* Some of the companies, including TCL and Reliance Jio also explicitly allow individual participation to access, amend or delete the information companies have stored about them. However, in other cases, users can only delete specific information upon account termination. Moreover, other companies do not specify if they continue to hold user information beyond the period for which services are

---

[26] OECD Privacy Principles, *available at* http://oecdprivacy.org/; Report of the Group of Experts on Privacy, PLANNING COMMISSION OF INDIA, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

provided. In fact, none of the companies except Hike Messenger disclose that they limit the storage of information to a specified time period.

*32.* Companies must follow acceptable standards for data protection and user privacy, which, at the very least, require them to commit to collection and use limitations, specify time periods for retaining the data, allowing users to access, amend and delete data and to ensure that data stored is not out-dated or wrong. These policies must clearly specify the third parties with whom information may be shared, and should specify whether and how user consent is to be obtained before sharing of this information.

- ***Companies' processes for sharing of user information upon request by private third parties or governments are not transparent***

*33.* With the exception of the Vodafone Transparency Report (undertaken by Vodafone India's holding company), none of the companies studied attempt to disclose any information about their processes for sharing user information with governments. Even in the case of private third parties, only some companies expressly commit to user notification before sharing of information.

*34.* Companies should be more transparent about third-party requests for user data. While regulations regarding confidentiality could be clearer, companies should at least indicate that governments have requested user data and present this information in aggregate form.

- ***Some companies disclose specific measures taken to secure information collected through the use of their services, including the use of encryption***

*35.* While all companies collecting sensitive personal information are requested to comply with the reasonable security standards laid down under the Rules, companies' disclosures about measures taken to secure data are generally vague. Rediff, for example, merely specifies that it uses the SSL encryption standard for securing financial data and 'accepted industry standards' for securing other data and Vodafone discloses that it takes 'reasonable steps' to secure data.

*36.* None of the companies surveyed disclose the existence of security audits by independent professionals, or the procedure followed in case of a breach of security. Further none of the companies commit to encrypting communications with or between the users end-to-end.

*37.* Companies should specify the safety standards utilized for the handling, transmission and storage of personal information. They must specify that the security used is in compliance with acceptable industry standards or legally prescribed standards. Further, they should ensure, wherever possible, that end-to-end encryption is used to secure the information of their users.

## RDR Company Reports

### 1. Tata Communications Limited

**www.tatacommunications.com**

**Industry**: Telecommunications

**Services evaluated**: Tier-1 Internet Backbone Services, VSNL Mail

**Market Capitalization**: INR 194 Billion

TATA Communications Ltd. (TCL) is a global telecommunications company, headquartered in Mumbai and Singapore. A part of the TATA group of companies, TCL was founded as Videsh Sanchar Nigam Limited (VSNL), which was the first public-access gateway internet provider in India. VSNL was later acquired by the TATA group, and entirely merged with TATA Communications in 2008. TATA continues to retain the VSNL domain for its personal and enterprise email service.

According to its latest annual report, TCL provides backbone connectivity to over 240 countries and territories and carries close to 24% of the world's Internet routes.[27] TCL also owns three of the ten submarine cable landing stations in India, responsible for India's connectivity to the global internet.[28]

A. **Commitment**

TCL scores averagely on disclosure of its commitment to human rights on the internet, including on disclosures relating to freedom of expression and privacy. Although TCL maintains a corporate social responsibility policy as well as business responsibility report, which include policy commitments to protecting human rights, (which are mandated by Indian law),[29] none of its publicly available policies make a reference to its commitments to freedom of expression of its users.

---

[27] TATA Communications Annual Report 2016, *available at* https://www.tatacommunications.com/sites/default/files/FIN-AnnualReport2015-16-AR-20160711.pdf.

[28] Submarine Cable Networks Data, *available at* http://www.submarinenetworks.com/stations/asia/india.

[29] *National Voluntary Guidelines on Social, Environmental and Economic Responsibilities of Business*, MINISTRY OF CORPORATE AFFAIRS, GOVERNMENT OF INDIA; SEBI Amendment to Listing Agreement, (August 13, 2012) *available at* *http://www.sebi.gov.in/cms/sebi_data/attachdocs/1344915990072.pdf*.

The TATA group maintains a code of conduct, applicable to all of its group companies, including TCL.[30] The code makes an explicit reference to data security and privacy of TATA's customers. As per that code, the Managing Director and Group CEO is the Chief Ethics Officer, responsible for the implementation of the Code of Conduct.[31]

TCL's internal policies concerning internal implementation of human rights, as well as grievance redressal, are more robust than their public policy commitments to the same. As per in the TATA group code of conduct, which is applicable to its group companies, TCL provides employee training and conducts ethics awareness workshops at frequent intervals, and also takes other initiatives to ensure compliance with the code of conduct, which includes a commitment to customer privacy and data protection.[32] Further, TCL has a well articulated whistleblower policy which states the processes to be followed in case any employee observes any unethical conduct within the company, including violations of the TATA code of conduct.[33] The whistleblower policy commits to protecting any employee who reports unethical conduct under the policy, but contains no explicit references to freedom of speech or censorship issues, or issues of user privacy.

Concerning stakeholder engagement, TCL seems to be somewhat involved in engaging with issues of privacy, but makes no commitments on issues of freedom of expression. TCL is a member of the Data Security Council of India, an industry body which makes public commitments towards user privacy and data security, which includes guiding the Indian IT industry on self-regulation on issues of privacy and data security.[34]

---

[30] Employee Code of Conduct, TATA GROUP, *available at* http://www.tata.com/pdf/tcoc-booklet-2015.pdf.

[31] TATA Communications Busines Responsibility Policies, *available at* http://www.tatacommunications.com/sites/default/files/Business_Responsibility_Policies.pdf.

[32] *Supra* Note 4 , at page 18.

[33] TATA Communications Whistleblower Policy, *available at* https://www.tatacommunications.com/sites/default/files/Whistleblower%20Policy%20-%20Designed%20Version.pdf.

[34] Kamlesh Bajaj, *DSCI: A self-regulatory organization*, *available at* https://www.dsci.in/sites/default/files/DSCI%20Privacy%20SRO.pdf.

TCL maintains various grievance redressal forums, evidenced through different policies. For example, their consumer charter provides a general forum for addressing grievances, which include complaints regarding service outages.[35] However, this does not refer specifically to complaints about censorship or privacy-related concerns. TCL's Acceptable Use Policy and privacy policy also guide users to specific grievance redressal forums, for complaints under those policies.[36] Besides this, there are recorded instances where TCL has advertised grievance redressal mechanisms relating to cases of private or judicial requests for blocking of content.[37] However, TCL does not make any public disclosures about the inputs to or outcomes of its grievance redressal mechanisms.

### B. Freedom of Expression

**General**

TCL's Acceptable Use Policy ("**AUP**") governs the use of TCL services by its customers, which includes downstream providers, which TCL is responsible for interconnection with, as a backbone internet provider.[38] VSNL mail maintains its own terms and conditions for users, which are available on its website.[39] Both TCL's AUP and VSNL's terms and conditions are easily locatable through their websites, are presented in a clear and understandable manner and are available in English.

TCL does not commit to notifying users of important changes to their terms of use, stating that it *may* chose to notify its customers of changes to the AUP, either directly, or by posting such modifications on its website. VSNLs policy states that the terms

---

[35] Customer Charter, TATA COMMUNICATIONS, *available at* https://www.tatacommunications.com/legal/customer-charter.

[36] AUP Violations Grievances Portal, *available at* http://www.tatacommunications.com/reporting-aup-violations; Privacy Policy, TATA COMMUNICATIONS, *available at* https://www.tatacommunications.com/policies/privacy-policy.

[37] Shamnad Basheer, *Busting a Baloney: Merely Viewing Blocked Websites Will Not Land You in Jail*, SPICY IP, (August 23, 2016), *available at* http://spicyip.com/2016/08/busting-a-baloney-merely-viewing-blocked-websites-will-not-land-you-in-jail.html.

[38] Acceptable Use Policy, TATA COMMUNICATIONS, *available at* https://www.tatacommunications.com/policies.

[39] *See* http://login.vsnl.com/terms_n_conditions.html.

and conditions of the use of the webmail service may change without any notice to users.

Although TCL is an Indian company and its terms are applicable to its customers worldwide, the AUP contains several references are to laws and procedures of the United States of America, such as the US PATRIOT Act, ostensibly due to TATA's heavy presence in the US market coupled with stricter disclosure requirements in that jurisdiction.

**Content Restrictions and Termination of Services**

The AUP does not place any obligations on TCL to ensure a fair judgement before sanctions such as removal of content, termination or suspension for violations of terms of use. Although the AUP identifies categories of content which is prohibited by the service,[40] the AUP also states that TCL may suspend or terminate a users account, for any action they may deem to be inappropriate or abusive, whether or not stated in their policies. The AUP clearly states that TCL may remove of edit content in violation of the AUP or content which is harmful or offensive. Although it states that TCL shall attempt to first contact a user who is suspected of violations, they may suspend or terminate the services of the customer at their sole discretion. There is evidence, although not stated explicitly in its policies, that TCL provides general notice when content is taken down on its network through judicial order. However, there is no disclosure of any requirement to contact the relevant user, in case of takedown of user-generated content in compliance with judicial order.[41]

Although TCL has voiced its opinion on network neutrality, for example, by issuing public comments to the Telecom Regulatory Authority of India,[42] it does not disclose its policies regarding throttling or degrading of content over its network, or its network management principles.

---

[40] This includes inappropriate content, which may be threatening, hateful or abusive content; content that infringes any intellectual property right; transfer of viruses or harmful content, fraudulent content (such as credit card fraud) and spam or unsolicited email.

[41] Basheer, *Supra* note 11.

[42] Response to Consultation Paper on Regulatory Framework for Over-the-top (OTT) Services, TATA COMMUNICATIONS, *available at* http://trai.gov.in/Comments/Service-Providers/TCL.pdf.

As a backbone connection provider, TCL's major customers include downstream ISP's who connect through TCL's network. Therefore, the AUP states that the downstream provider shall ensure that its customers comply with the AUP, failing which TCL may terminate the services of the downstream provider. Further, importantly, TCL treats violations of the AUP by the end-user as violations by the downstream ISP, making them directly liable for the violations of the terms and subject to any actions TCL may take in that regard. The AUP further expressly states that TCL shall co-operate with appropriate law enforcement agencies and other parties investigating claims of illegal or inappropriate conduct, but does not mention whether this involves taking down content or disconnecting users.

Technical observations on TCL's blocking practices in 2015 showed that TCL appeared to be using a proxy server to inspect and modify traffic to certain IP addresses.[43]

### C. Privacy

**General**

TCL has one privacy policy which covers all services provided by the company with the exception of VSNL mail, which has its own privacy policy.[44] The policy is easily accessible and available in English. The policy partially discloses that users are updated of any changes to the policy, however, any notification of the changes is only on the website and not done directly. In addition to the above, TCL also has a separate cookie policy, which contains information about its use of cookies for the collection of user information on its websites. Use of TCL's services entails acceptance of its privacy policy.

**Disclosure of Collection, Use and Sharing of Personal Information**

---

[43] Kaustabh Srikanth, *Technical Observations about Recent Internet Censorship in India*, HUFFINGTON POST, (January 6, 2015) *available at* http://www.huffingtonpost.in/kaustubh-srikanth/technical-observations-about-recent-internet-censorship-in-india/

[44] *See* https://www.tatacommunications.com/policies/privacy-policy; http://login.vsnl.com/privacy_policy.html (VSNL); However, there are other documents available on the TCL website purporting to be the Privacy Policy. Since the policies are not dated, it is not entirely clear which is applicable. (*See* http://www.tatacommunications.com/downloads/Privacy-Policy-for-TCL-and-Indian-Subs.pdf).

TCL, as well as VSNL mail, discloses that it collects users' personal information, based on the service utilized by them, both as solicited information and as automatically collected information through the use of technologies such as cookies, or through third parties. TCL's privacy policy states the various purposes to which such personal collection might be used, including for the investigation of fraud or unlawful activity, and for the provision of services, including for marketing. TCL discloses that it may combine this information prior to use. VSNL does not clearly state the purpose for which information may be collected, nor how it is shared.

TCL discloses that it may share personal information with affiliates, marketing partners, service providers as well as in response to legal processes including court orders or subpoena's or in any other case which TCL deems necessary or appropriate. Where personal information is shared with third parties, TCL commits to ensure that third parties (which include third party downstream carriers) also have appropriate data protection policies. TCL does not disclose its process for responding to orders for interception or for user information from private parties or from governmental agencies, nor does it provide any specific or aggregate data regarding the same.

**User control over information**

The policy discloses that TCL explicitly seeks user consent before it transfers data across legal jurisdictions. Although the policy states that TCL may share user information with law enforcement agencies in compliance with legal requests, it does not disclose any process for vetting such requests, nor does it disclose any data (specific or aggregate) about any such requests received.[45] With the exception of California, USA, TCL does not permit users to access data about any requests for their personal information which may have been received or granted by TCL to private third parties. Further, in contrast to most companies studied in this index, TCL discloses that it permits users to access, amend or delete information which the company stores about them. VSNL does not disclose that it allows users to access, amend or delete their personal information collected by VSNL.

**Security**

[45] The disclosure of governmental requests may be affected by laws which require such information to remain confidential, as explained in detail in Section I of this report.

TCL does not disclose that it uses or permits the use of encryption for any communications transmitted through its network, nor does it provide users any training or disclaimers to consumers on data protection.

2. **Rediff.com India Ltd.**

**www.rediff.com**

**Industry**: Internet Software Services and Media

**Services evaluated**: Rediff.com, Rediff Mail, Rediff iShare, Rediff Shopping

**Market Capitalization**: USD 6.07 Million

Rediff.com is a company, operating several internet services, including personal and enterprise email services, news services, a media-sharing platform and a shopping platform. It has its headquarters in Mumbai, India.

According to the Alexa Index, Rediff.com is the 47th most visited website in India, and the 407th overall. Approximately 87% of its traffic originates from Indian users.[46]

A. **Commitment**

Of the companies studied in this survey, Rediff.com ("**Rediff**") received the lowest scores on commitment indicators. None of Rediff's publicly available policies, including government mandated filings, disclose efforts towards protecting online freedoms. Rediff also does not disclose that it maintains a whistleblower policy or a company ethics policy. As a major online media and internet services provider in India, Rediff makes no public commitment towards freedom of speech and user privacy, and has not disclosed any efforts at engaging with stakeholders in this regard. Although the terms of use for various services provided by Rediff disclose the existence of a grievance redressal mechanism, it is only within the bounds of Rule 3 of

[46] *See* http://www.alexa.com/siteinfo/rediff.com.

the Intermediary Guidelines Rules, 2011.[47] The terms of use do not explicitly make mention of grievances related to online freedoms, nor is any specific or aggregate data about the complaints mechanism released by the company. Rediff does not disclose that it undertakes any impact assessment of how its services may impact online freedoms.

B. **Freedom of expression**

**General**

Rediff has an umbrella policy covering the use of all services offered by Rediff.com,[48] as well as separate policies governing the use of its video sharing platform,[49] its blogging platform[50] and messaging boards.[51] The use of any Rediff services is construed as acceptance of their terms of use. Rediff discloses that it may change any of its terms of use without prior notification to its users. Rediff's services are accessible through a Rediffmail account, which does not require verification through any government issued license to link online users to their offline identity. The existence of various disparate policies and the manner and format of the policies somewhat decrease their accessibility.

**Content Restriction and Termination of Services**

Rediff's General Terms of Use specify content which is prohibited on its various services, which is materially similar to the content prohibited under the guidelines issued under the Information Technology Act. Further, Rediff's messaging board policy lists a number of vague and broad categories which are prohibited and may be restricted on the forums, including *"negatively affecting other participants, disrupt the normal flow of the posting."*

As per the General Terms of Use, Rediff reserves the right to remove any content posted by users, solely at its own discretion. Rediff's General Terms of Use do not

---

47 *See* http://www.rediff.com/terms.html.

48 *Id.*

49 *See* http://ishare.rediff.com/templates/tc.html.

50 *See* http://blogs.rediff.com/terms/.

51 *See* http://www.rediff.com/news/disclaim.htm.

disclose any process for responding to requests by law enforcement or judicial or other government bodies for the takedown of content. However, the terms of Rediff's video sharing platform specifies that written substantiation of any complaint from the complaining party is required. Rediff's process for responding to complaints regarding intellectual property infringement are well detailed in this policy, although it does not substantiate the process for responding to other requests for restriction of content from private parties or law enforcement agencies.

Rediff further reserves the right to terminate the services offered to its users, with or without cause and without notice of the same. Similar to most companies surveyed, Rediff does not disclose its process for responding to requests for restriction of content or services by private parties or by government agencies, nor does it publish specific or aggregate data about restriction of content, the number of requests for takedown received or the number complied with.

C. **Privacy**

**General**

Rediff's performance on privacy indicators is marginally better than those on freedom of expression. A single privacy policy is applicable to all of Rediff's services, which is easily accessible through its various websites, including on its homepage. Rediff discloses that any material changes of its privacy policy will be notified prominently.[52] Use of Rediff's services entails acceptance of its privacy policy.

**Disclosure of Collection, Use and Sharing of Personal Information**

Rediff specifies that it collects both anonymous and personally identifiable information, automatically as well as what is solicited through their services, including financial information and 'user preferences and interests'. Rediff does not disclose if any information so collected is combined for any purpose. It also specifies the purpose to which such information may be used, which includes its use 'to preserve social history as governed by existing law or policy', or to investigate violations of Rediff's terms of use. The policy further specifies that Rediff may share information with third

[52] *See* http://blogs.rediff.com/terms/.

parties including law enforcement agencies or in compliance of court orders or legal process. Rediff discloses that it notifies users in case any personal information is being used for commercial purposes, and gives users the option to opt-out of such use. Rediff does not disclose its process for responding to orders for interception or for user information from private parties or from governmental agencies, nor does it provide any specific or aggregate data regarding the same.

**User Control over Information**

Rediff discloses that its users may chose to correct, update or delete their information stored with Rediff if they chose to discontinue the use of its services. However, unless users specifically chose to do so, Rediff continues to store user information even after termination of their account.

**Security**

Rediff discloses that it encrypts sensitive information (including financial information) through SSL encryption, and uses 'accepted industry standards' to protect other personal information submitted by users, although it does not define what these standards are.

### 3. Vodafone India Limited

***www.vodafone.in***

**Industry**: Telecommunications

**Services evaluated**: Broadband and Narrowband mobile internet services

Vodafone India Limited is a wholly owned subsidiary of the Vodafone Group Plc., the world's second largest telecommunications provider. As of March 2016, Vodafone India was the second largest telecommunications provider in India, with a market

share of 19.71% of internet subscribers (broadband and narrowband).[53] Vodafone entered the Indian market after acquiring Hutchison Telecom in 2007.

This survey has only examined the policies of Vodafone India and those policies of Vodafone plc. which may be applicable specifically to Vodafone India.

### A. Commitment

Vodafone India Limited ("**Vodafone**") scores the highest on the commitment indicators of the companies examined in this survey. While the Vodafone Group, (the Group/holding company) examined as part of the global Ranking Digital Rights Index, discloses its compliance with the UN Guiding Principles on Business and Human Rights,[54] Vodafone India does not specifically make any such disclosures independently. The companies annual report, corporate responsibility policies or business responsibility reports do not disclose any commitments towards online freedoms. However, Vodafone India does disclose the existence of a Privacy Management Framework, under which employees are provided training regarding data privacy of users.[55] Moreover, Vodafone's public statements disclose the existence of a privacy impact assessment procedure to ensure 'data minimisation' and reduce the risk of breach of privacy. Vodafone is also a member of the Data Security Council of India, an industry body which makes public commitments towards user privacy and data security, which includes guiding the Indian IT industry on self-regulation on issues of privacy and data security,[56] as well as the Cellular Operators Association of India, another industry organization which also commits to protecting consumer rights, including consumers right to privacy.[57]

---

[53] *Performance Indicator Report*, TELECOM REGULATORY AUTHORITY OF INDIA, (August, 2016) *available at* (http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator_Report_05_August_2016.pdf.

[54] *See* https://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/human-rights.html.

[55] Vodafone Sustainability Report, *See* http://static.globalreporting.org/report-pdfs/2015/ffaa6e1f645aa009c2af71ab9505b6b0.pdf.

[56] Amit Pradhan, CISO, on Data Privacy at Vodafone, DSCI BLOG, (July 15, 2015), *available at* https://blogs.dsci.in/interview-amit-pradhan-vodafone-india-on-privacy/.

[57] *See* http://www.coai.com/about-us/members/core-members.

Vodafone also discloses a multi-tiered grievance redressal mechanism, which includes an appellate authority as well as a timeline of 39 days for the resolution of the complaint. However, the mechanism does not specify if grievances related to online freedoms may be reported or resolved.[58] In addition, Vodafone has designated a Privacy Officer for redressing concerns under its privacy policy.

### B. Freedom of Expression

**General**

Vodafone scored the lowest on disclosures under this head of the companies surveyed. The terms of use for Vodafone India's services are not available on their homepage or site-map nor are they presented in a clear or easily accessible manner. They may be accessed through the Vodafone Telecom Consumers Charter, with different terms of use for pre-paid and post-paid customers. There is no policy specific to the use of internet services through the use of the Vodafone network, nor do these policies make reference to the use of internet services by Vodafone users. Vodafone does not disclose that it provides any notification of changes to the policies to its users.

**Content Restriction and Termination of Services**

While the Terms of Use do not specifically refer to online content, Vodafone's Terms of Use prohibit users from "sending messages" under various categories, which include messages which infringe upon or affect "national or social interest". Vodafone reserves the right to terminate, suspend or limit the service upon any breach of its Terms of Use or for any reason which Vodafone believes warrants such termination, suspension or limitation. Vodafone does not disclose its process for responding to violations of its terms of use.

Vodafone does not disclose its process for responding to requests for restriction of content or services by private parties or by government agencies, nor does it publish specific or aggregate data about restriction of content, the number of requests for takedown received or the number complied with. Although the Vodafone group internationally publishes a comprehensive law enforcement disclosure report (making

[58] *Process for registration of a complaint,* Vodafone India Telecom Consumers' Charter, *available at* https://www.vodafone.in/documents/pdfs/IndiaCitizensCharter.pdf.

it one of few major internet companies to do so), the report does not contain information on orders for blocking or restricting services or content.

Vodafone has made public statements of its commitment to network neutrality and against any kind of blocking or throttling of traffic, although it does not have any policies in place for the same.[59]

As with all telecommunications companies in India, users must be authenticated by a valid government issued identification in order to use Vodafone's telecommunication services.

### C. Privacy

**General**

Vodafone India's privacy policy which is applicable to all users of its services is not as comprehensive as some other policies surveyed. It is accessibly through the Vodafone India website, and available in English. Vodafone merely discloses that the policy may change from time to time and does not disclose that it provides users any notice of these changes.[60] Use of Vodafone's services entails acceptance of its privacy policy.

**Collection, Use and Sharing of Personal Information**

Vodafone's policy discloses the personal information collected, as well as the purpose and use of such information, and the purpose for which such information may be shared with third parties, including law enforcement agencies. However, Vodafone does not disclose how such information may be collected or for what duration.

Vodafone India's privacy policy does not disclose its process for responding to government requests for user information, including for monitoring or surveillance. However, the Vodafone law enforcement disclosure report elaborates upon the same,

---

[59] *Vodafone India: We are Pro Ne Neutrality*, GADGETS NOW, (May 20, 2015), *available at* http://www.gadgetsnow.com/tech-news/vodafone-wont-toe-zero-rating-plan-of-airtel/articleshow/47349710.cms; *Vodafone Response to TRAI Consultation Paper on Regulatory Framework for Over-the-Top (OTT) services*, VODAFONE INDIA, (March 27, 2015) *available at* http://trai.gov.in/Comments/Service-Providers/Vodafone.pdf.

[60] *See* http://www.vodafone.in/privacy-policy.

including the principles followed by Vodafone upon requests for user information or for monitoring their network in compliance with legal orders. However, as per the applicable laws in India, Vodafone does not publish any aggregate or specific data about such requests, although it states that the Indian government has made such requests.[61]

**User Control over Personal Information**

Vodafone does not disclose that it allows users to access, amend, correct or delete any information it stores about its users. It does not disclose if user information is automatically deleted after account termination.

**Security**

Vodafone only discloses that it takes 'reasonable steps' to secure user information. Vodafone does not disclose that it employs encryption over its network, or if it allows users to encrypt communications over their network. Vodafone also does not disclose that it provides any guidance to users on securing their communications over their network.

4. **Reliance Communications Limited**

***www.rcom.co.in***

**Industry**: Telecommunications

**Services evaluated**: Broadband and Narrowband mobile internet services

**Market Capitalization**: INR 118.35 Billion

Reliance Communications Limited ("**RCL**") is an Indian telecommunication services provider, and a part of the Reliance Anil Dhirubai Ambani group of companies. RCL is the fourth largest telecommunications provider in India, with a market share of

[61] Vodafone Law Enforcement Disclosure Report, *available at* https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html.

11.20% of Indian internet subscribers.[62] Reliance also owns one of ten submarine cable landing stations in India, responsible for India's connectivity to the global internet.

### A. Commitment

RCL does not disclose any policy commitment towards the protection of online freedoms. Although RCL has filed business responsibility reports which include a report on the company's commitment towards human rights, the same do not make a reference to privacy or freedom of expression of its users either.[63] RCL does not disclose that it undertakes any impact assessment of how its services may impact online freedoms.

While RCL does maintain a whistle-blower policy for reporting any unethical conduct within the company, the policy too does not expressly mention that it covers any conduct in violation of user privacy or freedom of expression. RCL is a member of at least three industry bodies which work towards stakeholder engagement on the issues of privacy and consumer protection and welfare, namely, the Data Security Council of India, the Internet Service Providers Association of India and the Association of Unified Telecom Service Providers of India (although none of these bodies expressly mention that they advocate for freedom of expression).

RCL maintains a comprehensive manual of practice for the redressing consumer complaints.[64] The manual of practice specifies the procedure for grievance redressal as well the timelines within which grievances should be resolved and the appellate authorities which can be approached, however, it does not specify whether complaints regarding privacy or freedom of expression are covered under this policy.

---

[62] *Performance Indicator Report*, TELECOM REGULATORY AUTHORITY OF INDIA, (August, 2016) *available at* (http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator_Report_05_August_2016.pdf.

[63] Business Responsibility Reports, RELIANCE COMMUNICATIONS LTD., *available at* http://www.rcom.co.in/Rcom/aboutus/ir/pdf/Business-Responsibility-Report-2015-16.pdf.

[64] Manual of Practice, RELIANCE COMMUNICATIONS LTD., *available at* http://www.rcom.co.in/Rcom/personal/customercare/pdf/Manual_of_Practice.pdf.

## B. Freedom of Expression

**General**

RCL's terms of use for its internet services are part of its Telecom Consumer's Charter,[65] its Acceptable Use Policy ("AUP")[66] and its Consumer Application Form,[67] which are not easily accessible through the RCL website. The charter contains the terms for its post-paid and pre-paid services as well the terms for broadband internet access. RCL discloses that it may change the terms of use of its services without any prior notification to its users.

**Content Restriction and Termination of Services**

RCL's AUP lists certain categories of content which is not permitted, which includes vague categories such as 'offensive', 'abusive' or 'indecent', which are not clearly defined. In the event that a user fails to comply with its terms of use, RCL discloses that their services may be terminated or suspended. Further, as per the CAF, RCL reserves the right to terminate, suspend or vary its services at its sole discretion and without notice to users. The terms of use also require the subscriber/user to indemnify RCL in case of any costs or damages arising out of breach of the terms by any person with or without the consent of the subscriber.

RCL discloses that upon receiving any complaints or upon any intimation of violation of its terms of use, RCL shall investigate the same, which may also entail suspension of the services of the user. RCL does not disclose that it provides users any notice of such investigation or reasons for suspension or termination of the services. RCL does not disclose specific or aggregate data regarding restriction of content upon requests by private parties or governmental authorities.

RCL does not disclose its network practices relating to throttling or prioritization of any content or services on its network. However, RCL has published an opinion to the Telecom Regulatory Authority of India, wherein it supported regulation prohibiting

---

65 *See* http://www.rcom.co.in/Rcom/personal/home/pdf/1716-Telecom-Consumer-Charter_TRAI-180412.pdf.

66 *See* http://www.rcom.co.in/Rcom/personal/pdf/AUP.pdf.

67 *See* http://myservices.relianceada.com/ImplNewServiceAction.do#.

throttling or prioritization of traffic. However, RCL was the network partner for Facebook's Free Basics platform which was supposed to provide certain services free of cost through the RCL network. The Free Basics initiative was abandoned after the TRAI prescribed regulations prohibiting price discrimination by ISPs.[68]

### C. Privacy

RCL scores the lowest on this indicator of the companies surveyed. RCL does not disclose that it has a privacy policy which governs the use of its internet services. RCL's AUP only discloses that it may access and use personal information which is collected through its services in connection with any investigation of violation of its AUP, and may share such information with third parties for this purpose, as it deems fit. Further, RCL's terms of use further disclose that it may provide user information to third parties including security agencies, subject to statutory or regulatory factors, without any intimation to the user.

**Security**

RCL does not disclose any information on the security mechanisms in place in its network, including whether communications over the network are encrypted or whether end-to-end encrypted communications are allowed.

### 5. Shaadi.Com

www.shaadi.com

Industry: Internet Marriage Arrangement

Services evaluated: Online Wedding Service

---

[68] *Prohibition Of Discriminatory Tariffs For Data Services Regulations,* TELECOM REGULATORY AUTHORITY OF INDIA, February 8, 2016), available at *http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf.*

Shaadi.com, a subsidiary of the People group, is an online marriage arrangement service launched in 1996.[69] While India is its primary market, the service also operates in the USA, UK, Canada, Singapore, Australia and the UAE. As of 2017, it was reported to have a user base of 35 million.

### A. Governance

Shaadi.com makes no explicit commitment to freedom of expression and privacy, and does not disclose whether it has any oversight mechanisms in place. The company also does not disclose whether it has any internal mechanisms such as employee training on freedom of expression and privacy issues, or a whistleblower policy. Further, there are no disclosures as to any process of impact assessment for privacy and freedom of expression related concerns. The company does not disclose if it is part of any multi-stakeholder initiatives, or other organizations that engage with freedom of expression and privacy issues, or groups that are impacted by the company's business.

While details of a Grievance Officer are provided in the company's Privacy Policy, it is not clearly disclosed if the mechanism may be used for freedom of expression or privacy related complaints. The company makes no public report of the complaints that it receives, and provides no clear evidence that it responds to them.

### B. Freedom Of Expression

**General**

The Terms of Service are easily locatable on the website, and are available in English. The Terms are presented in an understandable manner, with section headers, but provide no additional guidance such as summaries, tips or graphics to explain the terms.

Shaadi.com makes no disclosure about whether it notifies users to changes in the Terms, and how it may do so. Shaadi.com also does not maintain any public archives or change log.

---

[69] Shaadi.com Terms of Use/Service Agreement, *available at* http://www.shaadi.com/shaadi-info/index/terms (Last visited on November 10, 2016).

**Content Restriction and Termination of Services**

Shaadi.com discloses an indicative list of prohibited activities and content, but states that it may terminate services for any reason. Shaadi.com makes no disclosures about the process it uses to identify violations and enforce rules, or whether any government or private entity receives priority consideration in flagging content.

Shaadi.com does not disclose data about the volume and nature of content and accounts it restricts.

Shaadi.com makes no disclosures about its process for responding to requests from any third parties to restrict any content or users. The Terms do not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Shaadi.com makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities. Shaadi.com discloses that it notifies users via email when restricting their accounts.

Shaadi.com also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the the number of accounts or URLs affected, the types of subject matter associated with the requests, etc.

Registration for the service requires a Mobile Number, which may be tied to offline identity.

### A. Privacy[70]

**General**

The Privacy Policy is easily locatable on the website, and is available in English. The Policy is presented in an understandable manner, with section headers, but provides no additional guidance such as summaries, tips or graphics to explain the terms.

---

[70] Shaadi.com Privacy Policy, available at http://www.shaadi.com/shaadi-info/index/privacy (Last visited on November 10, 2016).

Shaadi.com discloses that material changes to the Privacy Policy will be notified by posting a prominent link on the Homepage. Further, if personally identified information is used in a materially different manner from that stated at the time of collection, Shaadi.com commits to notify users by email. However, Shaadi.com does not disclose a time frame within which it notifies users prior to the changes coming into effect. Shaadi.com also does not maintain any public archives or change log.

**Collection, Use and Sharing of Personal Information**

Shaadi.com clearly discloses the types of personal and non personal information it may collect, but does not explicitly disclose how it collects the information. There is no commitment to limit collection only to information that is relevant and necessary to accomplish the purpose of the service.

While the Privacy Policy states the terms of sharing information, it makes no type-specific discloses about how different types of user information may be shared or the purpose for which it may be shared. Shaadi.com also does not disclose the types of third parties with which information may be shared. Shaadi.com clearly discloses that it may share user information with government or legal authorities.

The Privacy Policy discloses the purposes for which the information is collected, but does not disclose if user information is combined from different services. Shaadi.com makes no commitment to limit the use of information to the purpose for which it was collected. Shaadi.com makes no disclosures about how long it retains user information. It does not disclose whether it retains de-identified information, or its process for de-identification.

Shaadi.com does not disclose whether it collects information from third parties through technical means, how it does so, or its policies about use, sharing, retention etc. Shaadi.com does not make any disclosures about its processes for responding to third party requests for user information. The Privacy Policy does not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Shaadi.com makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities.

Shaadi.com also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the number of accounts affected, the type of authority or legal process through which the request was made, etc.

**User Control over Information**

Shaadi.com does not disclose the time frame within which it may delete user information, if at all, after users terminate their account. Shaadi.com does not disclose whether users can control the collection of information by Shaadi.com. The Policy states that users are allowed to remove both public or private information from the database. However, certain (unspecified) financial information and account related information submitted at the time of registration may not be removed or changed.
Shaadi.com does not disclose if users are provided options to control how their information is used for targeted advertising, or if targeted advertising is off by default.
Shaadi.com does not disclose whether users may access a copy of their information, or what information may be available.

Shaadi.com does not disclose whether it notifies users when their information is sought by government entities or private parties.

**Security**

Shaadi.com discloses that it follows generally accepted industry standards to protect personal information. Employees are granted access on a need to know basis. Shaadi.com does not disclose whether it has a security team that audits the service for security risk, or whether it commissions third party audits.

Shaadi.com does not disclose whether it has any process, policy or mechanism in place for researchers to submit security vulnerabilities, and how it would respond to them. Shaadi.com does not explicitly commit to notify the relevant authorities without undue delay in case of a data breach. Shaadi.com does not disclose whether it notifies affected users about breaches, and any steps it may take to minimize impact.

Shaadi.com discloses that sensitive information, such as card numbers, are transmitted using the Secure Socket Layer protocol, but not whether all user communications are encrypted by default. Shaadi.com does not disclose whether it uses advanced authentication methods to prevent unlawful access. Shaadi.com does not disclose whether users can view their recent account activity, or if notifies users about unusual activity and possibly unauthorized access.

Shaadi.com publishes privacy and security tips on its website which provide guidance about risks associated with the service, and how they may be avoided.[71]

### 6. Hike Messenger

**www.get.hike.in**

**Industry**: Internet Instant Messaging

**Services evaluated**: Instant Messaging and VoIP application

Hike messenger is an Indian cross platform messaging application for smartphones. Users can exchange text messages, communicate over voice and video calls, and exchange pictures, audio, video and other files. Hike launched in November 2012 and, as of January 2016 Hike became the first Indian internet company to have crossed 100 million users in India. It logs a monthly messaging volume of 40 billion messages.[72] Hike's parent Bharti SoftBank is a joint venture between Bharti Enterprises and SoftBank, a Japanese telecom firm.[73] As of August 2016, hike was valued at $1.4 billion.[74]

#### A. Governance

---

[71] Shaadi.com Privacy Tips, available at http://www.shaadi.com/customer-relations/faq/privacy-tips (Last visited on November 10, 2016).

[72] https://blog.hike.in/hike-unveils-its-incredible-new-workplace-3068f070af08#.zagtgq5lk

[73] http://economictimes.indiatimes.com/small-biz/money/hike-messaging-app-raises-175-million-from-tencent-foxconn-and-others-joins-unicorn-club/articleshow/53730336.cms

[74] https://medium.com/@kavinbm/175-million-tencent-foxconn-d9cc8686821f#.7w6yljaii

Hike makes no explicit commitment to freedom of expression and privacy, and does not disclose whether it has any oversight mechanisms in place. Hike also does not disclose whether it has any internal mechanisms such as employee training on freedom of expression and privacy issues, or a whistleblower policy. Further, there are no disclosures as to any process of impact assessment for privacy and freedom of expression related concerns. Hike does not disclose if it is part of any multi stakeholder initiatives, or other organizations that engage with freedom of expression and privacy issues, or groups that are impacted by Hike's business.

Hike's Terms of Use provide contact details for submitting queries and complaints about the usage of the application. It notes that the complaints will be addressed in the manner prescribed by the Information Technology Act, 2000 and rules framed thereunder. The Terms do not disclose if the mechanism may be used for freedom of expression or privacy related issues. Hike makes no public report of the complaints that it receives, and provides no clear evidence that it responds to them.

### B. Freedom Of Expression[75]

**General**

The Terms of Service are easily locatable on the website, and are available in English. The terms are presented in an understandable manner, with section headers, and often provide examples to explain the terms.

Hike may make changes to the Terms at its discretion without any prior notice to the users. Hike does not disclose whether users are notified after changes have been made, or whether it maintains a public archive or change log.

Though the Terms disclose a range of content and activities prohibited by the service, Hike may delete content, for any reason at its sole discretion. Further, Hike may terminate or suspend the use of the Application at anytime without notice to the user.

---

75 Hike Terms of Use, available at http://get.hike.in/terms.html (Last visited on November 10, 2016).

**Content Restriction and Termination of Services**

Hike makes no disclosures about the process it uses to identify violations and enforce its rules, or whether any government or private entity receives priority consideration in flagging content. Hike does not disclose data about the volume and nature of content and accounts it restricts.

Hike makes no disclosures about its process for responding to requests from any third parties to restrict any content or users. The Terms do not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Hike makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities.

Hike also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the the number of accounts, etc.

Identity Policy

Mobile Numbers would be required to sign up for the service, which could potentially be connected to offline identity.

### C. Privacy[76]

**General**

The Privacy Policy is easily locatable on the website, and are available in English. The terms are presented in an understandable manner, with section headers, and often provide examples to explain the terms.

Hike discloses that changes to the Privacy Policy will be posted on Hike website, and does not commit to directly notifying users of changes. Users are advised to review the website from time to time to remain aware of the terms. Hike does not disclose a time

[76] Hike Privacy Policy, available at http://get.hike.in/terms.html (Last visited on November 10, 2016).

frame within which it may notify changes prior to them coming into effect. Hike also does not disclose whether it maintains a public archive or change log.

**Collection, Use and Sharing of Information**

Hike clearly discloses the types of user information it collects. However, Hike makes no explicit commitment to limit collection only to information that is relevant and necessary to accomplish the purpose of the service.

Hike discloses that user information may be shared for a variety of purposes, but does not disclose the type, or names of third parties that may be given access to the information. Hike discloses that it may share user information with government entities and legal authorities.

The Privacy Policy states the purposes for which user information is collected and shared, but makes no commitment to limit the use of information to the purpose for which it was collected.

Hike discloses that undelivered messages are stored with Hike's servers till they are delivered, or for 30 days, whichever is earlier. Messages or files sent through the service also reside on Hike's servers for a short (unspecified) period of time till the delivery of the messages or files is complete. Hike does not disclose the duration for which it retains information such as profile pictures and status updates. Hike does not disclose whether it retains de-identified information, or its process for de-identification. Hike discloses that, subject to any applicable data retention laws, it does not retain user information beyond 30 days from deletion of the account.

Hike does not disclose whether it collects information from third parties through technical means, and how it does so, or its policies about use, sharing, retention etc.

Hike does not make any disclosures about its processes for responding to third party requests for user information. The Privacy Policy does not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Hike makes no commitment

to pushback on inappropriate or overbroad requests from the government, or private entities.

Hike also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the number of accounts affected, the type of authority or legal process through which the request was made, etc.

Hike does not disclose whether it notifies users when their information is sought by government entities or private parties.

**User Control over Information**

Hike discloses that the user may chose to not submit certain user information, but also notes that this may hinder use of the application. Hike makes no disclosure about whether users may request deletion of their user information.

Hike discloses that users may opt out or opt in for specific services or products which may allow user information to be used for marketing or advertising purposes. Hike does not disclose if targeted advertising is on by default.

Hike does not disclose whether users may obtain a copy of their user information.

**Security**

Hike discloses that it has security practices and procedures to limit employee access to user information on a need to know basis only. Hike does not disclose whether it has a security team that audits the service for security risk, or whether it commissions third party audits. Hike does not disclose whether it has any process, policy or mechanism in place for researchers to submit security vulnerabilities, and how it would respond to them.

Hike does not explicitly commit to notify the relevant authorities without undue delay in case of a data breach, but discloses that it may attempt to notify the user

electronically. However, company does not the types of steps it would take to minimize impact of a data breach.

Hike does not disclose if transmission of user information is encrypted by default, or whether it uses advanced authentication methods to prevent unlawful access. Hike does not disclose whether users can view their recent account activity, or if notifies users about unusual activity and possibly unauthorized access.

Hike does not publish and materials that educate users about cyber risks relevant to their service.

### 7. Aircel

**www.aircel.com**

**Industry**: Telecommunications

**Services evaluated**: Broadband and Narrowband Mobile Internet Services

The Aircel group is a joint venture between Maxis Communications Berhad of Malaysia and Sindya Securities & Investments Private Limited. It is a GSM mobile service provider with a subscriber base of 65.1 million users. The company commenced operations in 1999 and has since become a pan India operator providing a host of mobile voice and data telecommunications services.

#### A. Governance

Aircel's Terms and Conditions state that it is a duty of all service providers to assure that the privacy of their subscribers (not affecting national security) shall be scrupulously guarded. However, the company makes no similar commitment to freedom of expression.

Aircel also does not disclose whether it has any oversight mechanisms in place. However, Aircel does disclose that it has established a Whistleblower Policy and an Ethics Hotline. Further, the Privacy Policy states that employees are expected to follow a Code of Conduct and Confidentiality Policies in their handling of user

information. There are no disclosures as to any process of impact assessment for privacy and freedom of expression related concerns. Aircel does not disclose if it is part of any multi stakeholder initiatives, or any other organizations that engage with freedom of expression and privacy issues, or groups that are impacted by Aircel's business.[77]

Aircel has a process for receiving complaints on its website under the section of Customer Grievance. However, it is not clearly disclosed whether this process may be applicable for freedom of expression and privacy related issues. Though Aircel does disclose information such as the number of complaints received and redressed, the number of appeals filed, it makes no disclosure if any complaints were specifically related to freedom of expression and privacy.[78]

### A. Freedom Of Expression

**General**

The Terms and Conditions are not easily locatable, and are found as part of a larger document titled Telecom Consumers Charter, which is itself posted as an inconspicuous link on the Customer Grievance page. The Terms are provided only in English, but it is likely that Aircel has a large Hindi speaking user base. The Terms are presented in an understandable manner, with section headers, but provide no additional guidance such as summaries, tips or graphics to explain the terms.[79]

Aircel discloses that it may make changes to the Terms without notice to users, or with written notice addressed to the last provided address, at its sole discretion. Aircel does not disclose if it maintains a public archive or change log.

---

[77] Aircel Whistle Blower Policy, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P3540044205 1324996434644 (Last visited on November 10, 2016).

[78] Aircel Whistle Blower Policy, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P3540044205 1324996434644 (Last visited on November 10, 2016).

[79] Aircel Whistle Blower Policy, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P3540044205 1324996434644 (Last visited on November 10, 2016).

**Content Restriction and Termination of Services**

The Terms prohibit certain activities, but Aircel discloses that it may terminate services for a user at its sole discretion for any reason, including a violation of its Terms.

Aircel makes no disclosures about its process it uses to identify violations and enforce its rules, or whether any government or private entity receives priority consideration in flagging content. Aircel does not disclose data about the volume and nature of content and accounts it restricts.

Aircel makes no disclosures about its process for responding to requests from third parties to restrict content or users. The Terms do not disclose the basis under which Aircel may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Aircel makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities. Aircel does not disclose if it notifies users when they try to access content that has been restricted, and the terms expressly waive users' right to notice if their services are suspended/terminated.

Aircel does not disclose its policy on network management, or whether it prioritizes, blocks, or delays certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability. Notably, in its comments to the Telecom Regulatory Authority of India on the issue of regulation of Over-The-Top Services, it argued for the right of Telecom Service Providers to negotiate commercial agreements with OTT providers, as well as the right to employ non price differentiation and network management practices.[80]

Aircel discloses that it may terminate its services in wholly or in part, at its sole discretion, and for any reasons, including directions from the government. Aircel does not disclose its process for responding to requests for network shutdowns, or the legal authority that makes the requests, nor does it commit to push back on such requests.

---

[80] Aircel Whistle Blower Policy, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P3540044205 1324996434644 (Last visited on November 10, 2016).

The terms waive the users' right to notice when services are suspended. Aircel also provides no data about the number of request received or complied with.

Aircel discloses that it requires government approved identification in order to perform verifications.

### B. Privacy[81]

**General**

The Privacy Policy is easily locatable on the website, and is available in English. It is likely that Aircel has a large Hindi and vernacular speaking user base. However, the website does not provide any other language versions of the Privacy Policy. The Policy is presented in an understandable manner, with section headers, but provides no additional guidance such as summaries, tips or graphics to explain the terms.

The Privacy Policy states that changes will be reflected on the website, and makes no disclosure about whether it will directly notify users. Aircel does not disclose a time frame within which it may notify users prior to the changes coming into effect. Aircel also does not maintain any public archives or change log.

**Collection, Use and Sharing of Information**

Though Aircel discloses the types of user information it may collect, it does not explicitly disclose how it collects the information. Aircel makes no commitment to limit collection only to information that is relevant and necessary to accomplish the purpose of the service.

While the Privacy Policy states the terms of sharing information, it makes no type-specific disclosures about how different types of user information may be shared. Further, while Aircel broadly discloses the type of third parties with which it may share information, it does not provide a specific list of names. Aircel clearly discloses that it may share user information with government or legal authorities.

---

[81] Aircel Whistle Blower Policy, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=P3540044205 1324996434644 (Last visited on November 10, 2016).

The Privacy Policy broadly states the purposes for which the information is collected, but does not disclose in more specific terms the purposes for which various types of user information may be collected. Aircel also does not disclose if user information is combined from different services. Aircel makes no commitment to limit the use of information to the purpose for which it was collected.

Aircel makes no disclosures about how long it retains user information, and the Privacy Policy states that it may retain information for as long as it requires. Aircel does not disclose whether it retains de-identified information, or its process for de-identification. Aircel does not disclose the time frame within which it may delete user information, if at all, after users terminate their account.

Aircel does not disclose whether it collects information from third parties through technical means, how it does so, or its policies about use, sharing, retention etc. Aircel does not make any disclosures about its processes for responding to third party requests for user information. The Privacy Policy does not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Aircel makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities.

Aircel also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the number of accounts affected, the type of authority or legal process through which the request was made, etc.

Aircel does not disclose whether it notifies users when their information is sought by government entities or private parties.

**User Control over Information**

Aircel does not disclose whether users can control the collection of information by Aircel. The Privacy Policy discloses that if information is not provided, or consent for usage is withdrawn, Aircel reserves the right to discontinue the service for which the

information is sought. Aircel does not disclose if users can request the deletion of information.

Aircel discloses that users can opt in or opt out of receiving telemarketing communications, and discloses that they must be specifically opted in for. However, Aircel does not disclose any options with respect to the usage of use information for such purposes. Users may only choose to opt in or opt out of receiving commercial communications, and have no control over whether user information is used in the first place.[82]

Aircel does not disclose whether users may access a copy of their information, or what information may be available.

**Security**

Aircel discloses that it has adopted measures to protect information from unauthorized access and to ensure that personal information is accessible to employees or partners employees strictly on a need to know basis. Aircel discloses that its employees are bound by a Code of Conduct and Confidentiality Policies. Aircel does not disclose whether it has a security team that audits the service for security risk, or whether it commissions third party audits.

Aircel does not disclose whether it has any process, policy or mechanism in place for researchers to submit security vulnerabilities, or how it would respond to them.

Aircel does not explicitly commit to notify the relevant authorities without undue delay in case of a data breach. Aircel does not disclose whether it notifies affected users about breaches, or any steps it may take to minimize impact.

Aircel discloses that highly confidential information such as passwords and credit card numbers are transmitted using the Secure Socket Layer protocol. However, Aircel does not disclose if all user communications are encrypted by default. Aircel also does

[82] Aircel National Customer Preference Registry, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=customercare_ndnc_page (Last visited on November 10, 2016).

not disclose whether it uses advanced authentication methods to prevent unlawful access. Aircel does not disclose whether users can view their recent account activity, or if it notifies users about unusual activity and possibly unauthorized access.

Aircel publishes information about Security Awareness and Alerts that details various threats on the internet, and how they may be countered.[83]

## 8. Reliance Jio

**www.jio.com**

**Industry**: Telecommunications

**Services evaluated**: Broadband and Narrowband mobile internet services

Reliance Jio Infocomm Ltd. is a wholly owned subsidiary of Reliance Industries Ltd., and provides wireless 4G LTE service network across all 22 telecom circles in India. It does not offer 2G/3G based services, making it India's only 100% VoLTE network. Jio began a massive rollout of its service in September 2016, as was reported to have reached 5 million subscribers in its first week.[84] As of October 25, 2016, Jio is reported to have reached 24 million subscribers.[85]

### A. Governance

Jio does not score well in the Governance metrics. It makes no explicit commitment to freedom of expression and privacy, and does not disclose whether it has any oversight mechanisms in place. The company also does not disclose whether it has any internal

---

[83] Aircel National Customer Preference Registry, *available at* http://www.aircel.com/AircelWar/appmanager/aircel/karnataka?_nfpb=true&_pageLabel=customercare_ndnc_page (Last visited on November 10, 2016).

[84] http://www.counterpointresearch.com/reliancejio/

[85] http://economictimes.indiatimes.com/tech/internet/gujarat-andhra-top-circles-for-jio-subscribers-cross-24mn-mark/articleshow/55040351.cms

mechanisms in place such as employee training on freedom of expression and privacy issues, or a whistleblower policy. Further, there are no disclosures as to any process of impact assessment for privacy and freedom of expression related concerns. The company does not disclose if it is part of any multi-stakeholder initiatives, or other organizations that engage with freedom of expression and privacy issues, or groups that are impacted by the company's business.

Jio's website discloses a process for grievance redressal, along with the contact details of for their Grievance Officer. The Regulatory Policy also lays down a Web Based Complaint Monitoring System for customer care. However, neither mechanism clearly discloses that the process may be for freedom of expression and privacy issues. In fact, the Grievance Redressal process under the Terms and Conditions process seems primarily meant for copyright owners alleging infringement. Jio makes no public report of the complaints it receives, and provides no clear evidence that it responds to them.[86]

### A. Freedom Of Expression[87]

**General**

The Terms of Service are easily locatable on the website, and are available in English. It is likely that Jio has a large Hindi and vernacular speaking user base. However, the website does not have any other language versions of the Terms of Service.

The Terms are presented in an understandable manner, with section headers, but provide no additional guidance such as summaries, tips or graphics to explain the terms.

Jio discloses that changes to the Terms of Service may be communicated through a written notice to the last address given by the Customer, or through a public notice in print media. However, this may be at Jio's sole discretion. Further, Jio does not

---

[86] Jio Terms and Conditions, *available at* https://www.jio.com/en-in/terms-conditions (Last visited on November 10, 2016).

[87] Jio Terms and Conditions, *available at* https://www.jio.com/en-in/terms-conditions (Last visited on November 10, 2016).

disclose a time frame within which it notifies users prior to the changes coming into effect. Jio also does not maintain any public archives or change log.

The Terms of Service disclose a range of proscribed activities, and states that any violation of the Terms may be grounds to suspend or terminate services. However, Jio makes no disclosures about its process of identifying violations and enforcing rules, or whether any government or private entity receives priority consideration in flagging content. There are no clear examples provided to help users understand the provisions.

Jio does not disclose data about the volume and nature of content and accounts it restricts.

**Content Restriction and Termination of Services**

Jio makes no disclosures about its process for responding to requests from third parties to restrict content or users. The Terms do not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to requests. Jio makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities. Jio does not disclose if it notifies users when they try to access content that has been restricted, or if it notifies users when their account has been restricted.

Jio also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the the number of accounts or URLs affected, the types of subject matter associated with the requests, etc.

Jio does not disclose its policy on network management, or whether it prioritizes, blocks, or delays certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability.

Jio makes no disclosures about its policy on network shutdowns, or why it may shut down service to a particular area or group of users. Jio does not disclose its process for responding to such requests, or the legal authority that makes the requests, or whether

it notifies users directly when it restricts access to the service. It also provides no data about the number of request received or complied with.

Jio requires that users verify their identity with government issued identification such as Passport, Driver's License or Aadhaar.

### B. Privacy[88]

**General**

The Privacy Policy is easily locatable on the website, and is available in English. It is likely that Jio has a large Hindi and vernacular speaking user base. However, the website does not have any other language versions of the Privacy Policy

The Policy is presented in an understandable manner, with section headers, but provides no additional guidance such as summaries, tips or graphics to explain the terms.

Jio commits to make all efforts to communicate significant changes to the policy, but does not disclose its process for doing so. The policy recommends that users periodically review the website for any changes. Jio does not disclose a time frame within which it notifies users prior to the changes coming into effect. Jio also does not maintain any public archives or change log.

**Collection, Use and Sharing of Information**

Jio clearly discloses the types of personal and non personal information it may collect, but does not explicitly disclose how it collects the information. There is no commitment to limit collection only to information that is relevant and necessary to accomplish the purpose of the service.

Jio commits to not sell or rent user information to third parties, but discloses that it may use and share non personal information at its discretion.

Jio discloses the broad circumstances in which it may share personal information with third parties and the types of entities it may disclose such information to. The policy

---

[88] Jio Terms and Conditions, *available at* https://www.jio.com/en-in/terms-conditions (Last visited on November 10, 2016).

states that such partners operate under contract and strict confidentiality and security restrictions. However, it does not specifically disclose the names of third parties it shares information with. Jio clearly discloses that it may share user information with government or legal authorities.

Jio discloses that it may share user information with third party websites or applications at the behest of the user (for instance, when logging into services with a Jio account). It discloses that Jio will provide notice to the user, and obtain consent regarding the details of the information that will be shared. In such a situation, the third party's privacy policy would be applicable to the information shared.

The Privacy Policy broadly states the purposes for which the information is collected, but does not disclose if user information is combined from different services. In detailing the types of third parties that Jio may share user information with, Jio also discloses the respective purposes for sharing. However, Jio makes no commitment to limit the use of information to the purpose for which it was collected.

Jio does not disclose whether it collects information from third parties through technical means, and how it does so, or its policies about use, sharing, retention etc.

Jio does not make any disclosures about its processes for responding to third party requests for user information. The Privacy Policy does not disclose the basis under which it may comply with government or private party requests, nor whether any due diligence is conducted before responding to the requests. Jio makes no commitment to pushback on inappropriate or overbroad requests from the government, or private entities.

Jio also does not publish any data about the requests it receives, and how it responds to them. This could include, for instance, the number of requests received, the number of requests complied with, the number of accounts affected, the type of authority or legal process through which the request was made, etc.

Jio does not disclose whether it notifies users when their information is sought by government entities or private parties.

**User Control over Information**

Jio makes no disclosures about how long it retains user information. It does not disclose whether it retains de-identified information, or its process for de-identification. Jio does not disclose the time frame within which it may delete user information, if at all, after users terminate their account.

Jio does not disclose whether users can control the collection of information by Jio. The Privacy Policy does allow requests for access, correction or deletion of user information, but also notes that deletion of certain (unspecified) information may lead to termination of the service. However, deletion of information would be subject to any applicable data retention laws, law enforcement requests, or judicial proceedings. Further, the request may be rejected if there is extreme technical difficulty in implementing it, or may risk the privacy of others.

Though the Privacy Policy allows for access requests, it does not disclose what user information may be obtained, or whether it may be made available in a structured data format. Jio does not disclose if targeted advertising is on by default, or whether users can control how their information is used for these purposes.

Jio discloses that it has adopted measures to protect information from unauthorized access and to ensure that personal information is accessible to employees or partners employees strictly on a need to know basis. Jio does not disclose whether it has a security team that audits the service for security risk, or whether it commissions third party audits.

Jio discloses that it has reasonable security practices and procedures in place in line with international standard IS/ISO/IEC 27001, to protect data and information. Jio does not disclose whether it has any process, policy or mechanism in place for researchers to submit security vulnerabilities, and how it would respond to them. Jio does not explicitly commit to notify the relevant authorities without undue delay in case of a data breach. Jio does not disclose whether it notifies affected users about breaches, and any steps it may take to minimize impact.

Jio does not disclose if transmission of user information is encrypted by default, or whether it uses advanced authentication methods to prevent unlawful access. Jio does not disclose whether users can view their recent account activity, or if notifies users about unusual activity and possibly unauthorized access.

Jio does not publish and materials that educate users about cyber risks relevant to their service.