Telecoms Corporate Accountability Practices in terms of Digital Freedoms in Georgia

Tbilisi, Georgia

2022

Contents

The study was prepared by the Institute for the Development of Freedom of Information (IDFI). IDFI is responsible for the content of this material.

Introduction

As of July 2022, there are more than 1 million (1,011,791) internet subscribers in Georgia. According to the national Telecommunication Authority (Communication Commission), 80% of these subscribers are split between the two main telecommunications companies: Magticom and Silknet.[1]

Considering the large segment of the population these two Internet Service Providers (ISPs) cover, it is important to closely examine their terms of use, privacy policies, and other disclosures about commitments to respect users' rights, in order to understand/identify any gaps and challenges. Methods used for collecting and storing personal information have gone through significant transformations and are different even for individual companies and organizations that accumulate and manage data from millions of users. Despite this, many users give their consent for the storage, processing, and use of their personal data without carefully reviewing the associated terms and policies.

The Georgian legislation provides some degree of guidance and protection for citizens in this regard. First and foremost the Law of Georgia on Personal Data Protection[2] lays out basic grounds for the principles of data processing, rights and obligations of data controllers and data processors, data security, rights of data subject, and most importantly, establishes the Personal Data Protection Service which is the main regulatory authority in this field. Another major piece of legislation in this respect is the Law of Georgia On Electronic Communications[3], which lays down the legal and economic framework for activities carried out through electronic communication networks and associated facilities, the principles for creating and regulating a competitive environment in this field, determines the functions of the national regulatory authority (the Georgian National Communications Commission), and the rights and obligations of natural and legal persons in the process of possessing or using electronic communication networks and facilities, or when providing services via such networks and facilities. Lastly, (the Georgian National Communications Commission has issued two more decrees that are relevant in this regard, "the regulation on dissemination of content harmful for minors on the Internet"[4], which mandates the implementation of a parental control mechanism by ISPs and other media providers to block off inappropriate content at the request of the user, and "the regulation on the provision of services and the rights of consumers in the field of electronic communications"[5], which establishes the basic standards of terms of use, the minimum timeframes for user notification, minimum standards of service provision, and the minimum standard of responding to user demands/complaints.

1 Website of the Communications Commission: Internet - Subscribers by technologies. Available at: https://bit.ly/3D4Ohd6
2 Law of Georgia on Personal Data Protection
3 Law of Georgia on Electronic Communications
4 The regulation on dissemination of content harmful for minors on the Internet
5 The regulation on the provision of services and the rights of consumers in the field of electronic communications

This study will aim to outline the key challenges related to the availability of policies regarding the protection of personal data, terms of use, and other corporate practices of the major telecom operators in Georgia. To this end, the project team partnered with Ranking Digital Rights (RDR)[6] to adapt their research methodology to the local context in Georgia. RDR provided technical assistance and guidance for the adaptation process, including the necessary materials to conduct the data collection and analysis. The researchers selected a subset of the indicators from the 2020 RDR Corporate Accountability Index methodology[7], that are best suited to **study the two largest private companies in the sphere of telecommunications in Georgia: Magticom and Silknet.** This report shows the results from the evaluation and analysis of the policies and human rights commitments of these ISPs, based on the publicly available data on the companies' official web portals.

Key Findings

- As a result of the evaluation, Magticom scored 39.45/100 points while Silknet fared slightly better with 44.98/100 points. However, both companies still fall short, with vast room for improvement.

- Neither company discloses the processes for responding to demands (from private entities, government agencies, or court demands) to restrict content or accounts, nor publishes the associated data (for example, as part of transparency reports).

- Neither company discloses information about their network management practices, specifically, whether or not they engage in network prioritization, blocking, or delaying traffic for any reason.

- Both companies have a log of their ToS versions. Magticom's archive of changes to the terms of service is one click away from the front page and contains information about all prior changes, meanwhile, Silknet's archive only dates back to 2021.

- Neither company clearly discloses information about the processes it uses to identify content or accounts that violate the established rules of the ToS.

- Silknet formally states that they limit the collection of user information to what is directly relevant and necessary to accomplish the purpose of their service, however, there is no evidence that Magticom has made such an official commitment.

6 https://rankingdigitalrights.org
7 https://rankingdigitalrights.org/2020-indicators/

Methodology of the study

RDR's Index methodology includes 58 indicators across three categories: governance, freedom of expression, and privacy, totalling more than 300 specific questions that are used to evaluate the company's disclosures and human rights commitments to respecting users' rights. For this study, the researchers selected 20 indicators that are especially relevant for the context in Georgia.

The indicators selected for this study cover the following topics:

- Data about content and account restrictions to enforce terms of service
- Process for responding to private requests and government demands to restrict content or accounts
- Data about private requests and government demands to restrict for content and accounts
- User notification about content and account restriction
- Network management and network shutdowns
- Addressing security vulnerabilities

Each indicator has a list of elements (the full list of questions evaluated can be found in the appendix), and companies receive credit (full, partial, or no credit) for each element they fulfill. The evaluation includes an assessment of disclosure for every element of each indicator, based on one of the following possible answers:

- *"Yes"/ full disclosure*: Company disclosure meets the element requirement.
- *"Partial"*: Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of the element.
- *"No disclosure found"*: Researchers were unable to find information provided by the company on its website that answers the element question.
- *"No"*: Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of "no disclosure found," although both result in no credit.
- *"N/A"*: Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company's score

Once the evaluation of the elements is complete, then final scores are calculated based on the following points:

- Yes/full disclosure = 100
- Partial = 50
- No = 0
- No disclosure found = 0
- N/A = excluded from score and averages

As a result of the evaluation, Magticom scored 39.45 points, while Silknet fared slightly better with 44.98 points. In both cases, there were numerous unscored indicators due to the absence of relevant data or policies. Specifically, data about content and account restrictions is not disclosed by either company. No disclosures were found for processes for responding to demands (private, government, or court demands) to restrict content or accounts, nor the associated data. However, this data can be requested from Georgia's Communications Commission, which is the main government agency that can make demands to block or restrict websites based on content. In the period from 2017 to September 26, 2022, the commission sent 65 demands to block a total of 480 websites by providers. The majority of blocked websites are due to copyright violations (77%), production violating Georgian legislation (16.5%), and pornography (6.5%)[8]. Neither ISP publicly discloses how they handle demands from foreign government entities (although when inquired Magticom stated that any demand made from a foreign jurisdiction would have to be officially recognised by the Georgian court before being considered by the ISP). No information could be found about the network management practices of the ISPs, specifically, whether or not they engage in network prioritization, blocking, or delaying traffic for any reason. Lastly, neither company has published information about the process/procedures for addressing security vulnerabilities discovered by external security researchers.

Results of the study

Freedom of Expression and Information

Both companies have easily accessible terms of service (ToS), which are available within one click from their respective homepage. The ToS are available in the national language (Magticom also provides theirs in English and Russian), and are presented clearly, in a readable font, spacing, and understandable language, with some charts to ease perceptibility.

As for the changes to the terms of service, both companies' service agreement states that the ISP will directly inform users about changes to the terms of service 30 days prior if the changes lead to a fee increase or if the ISP is otherwise legally obligated. However, the two companies differ in their practices of publishing archives. While Magticom's archive is one click away from the front page and contains information about all prior changes to the terms of service as well as minor changes to available products, Silknet's archive only goes back to 2021.

Silknet's subscription agreement lists the types of activities not permitted by the company, which may lead to the restriction of a user's account. Magticom has a separate fair use policy for the same purpose. Both companies disclose their process for enforcing rules once violations are detected. However, neither

8 Blocked Websites in Georgia: Legal and Practical Analysis

company clearly discloses information about the processes it uses to identify content or accounts that violate the established rules.

There is also a major gap in the way the companies chose to notify users about content and account restrictions. Neither company makes any official mention in their policies available online of notifying users about content restrictions, although there have been sporadic instances of informative messages being displayed on blocked websites. The latest example was the restriction of popular Georgian multi-media portals, that were hosting pirated movies and TV-shows[9]. After getting blocked the websites display a message saying "The page is undergoing reconstruction". As for account restrictions, Silknet's publicly available subscription agreement states that users will be directly notified in case of their accounts being suspended or restricted. However, Magticom's publicly available service agreement template is quite ambiguous in this regard, stating that the ISP will take appropriate measures to inform the user in case of their account being restricted or temporarily suspended (due to missed payment or maintenance), however, no specific measures are mentioned and other cases of restriction are not discussed.

Lastly, some similarities are found between the companies in the way they handle information about network shutdowns. Silknet's subscription agreement mentions the case for single users and accounts, but there is no mention of restricting service to a group or area. Furthermore, the publicly available agreement template is vague, not listing specific reasons that may lead to a shutdown. The same is outlined in Magticom's standard conditions of service provision, with an approximately similar level of specificity, with the addition of clearly disclosing why it may restrict access to specific applications or protocols (at least VoIP services). Magticom's Internet service provision contract template states that the ISP directly notifies users in case of a service interruption due to maintenance, for all other cases of shutdowns, the article is vague and states that the users will be notified in accordance with the ISP's discretion. In contrast, Silknet's subscription agreement states that users will be directly notified when the company shuts down a network or restricts access to a service. Neither companies disclose its process for responding to government demands to shut down a network or restrict access to a service, nor any statistics depicting the number of network shutdown demands received from the specific legal authorities that make the demands or the number of government demands with which it complied. Furthermore, neither company mentions its commitment to push back on government demands to shut down networks or restrict access to services. Although it has to be noted, that there has been no precedent of such shutdowns in Georgia over the past years.

Privacy

Both surveyed companies have made their privacy policies accessible one click away from their homepage, available in Georgian and English, as well as Russian in Magticom's case. Both policies are formatted clearly and written in simple language, with section headers and readable

[9] https://formulanews.ge/News/60896

font size. Although both companies commit to disclosing any changes made to the privacy policy by publishing a notice on their website, neither of them provides a timeframe within which the notice will be posted prior to the changes coming into effect, and neither of them maintains a public archive or a change log.

Both Magticom and Silknet clearly disclose the types of user information they collect and how they collect each type of user information, however only Silknet formally states that they limit the collection of user information to what is directly relevant and necessary to accomplish the purpose of their service. Similarly, both companies list the types of user information they infer and describe the methods of inference such as data analysis of users' activities, preferences, or attributes, as well as data collected by combining datasets and utilizing data-mining techniques.

Magticom clearly discloses for what purpose collected information may be shared and what types of third parties it may be shared with, however, Silknet does not list the types of information. Both companies clearly state that they may share user information with Law enforcement agencies, regulatory bodies, courts, or other public authorities if mandated or authorized by law. The companies provide broad categories of third parties with whom user information may be shared but do not disclose the types of information that are shared with specific third parties.

Both companies list the purposes for the collection of each type of user data and broadly state the purpose for inference. Both companies disclose information regarding combining data from various services and list reasons such as selecting custom offers and promotions based on user activities, offering other products and services based on users' interests, and contacting users with notifications about changes to the service or product.

In terms of retention of user information, Silknet has a significantly more transparent practice, clearly disclosing how long it retains each type of user information. The company states that it retains aggregate data and data stored in anonymized/de-identified form, which does not constitute personal data, as it cannot be linked to an identified or identifiable natural person. The ISP also lists the purposes for retaining such data including analyzing and further developing the services, products, managerial, internal corporate, and third-party reports. However, it does not clearly disclose the types of such data, nor the process of de-identification. Additionally, Silknet clearly declares a specific timeframe (4 years) for deleting user information upon the termination of the account. Meanwhile, Magticom's disclosed practices are more vague, stating that they store information for as long as it is allowed by law. If there's no legal specification, it is only stored for as long as needed. Moreover, they retain some personal information for a "reasonable" period of time after the termination of a contract, specific timeframes are provided, nor are the specific types of information it refers to.

Conclusions and recommendations

The results of the first study of Georgian telecoms' disclosure of their privacy, data protection, and freedom of expression policies demonstrate that there is a need for significant improvement to ensure that their corporate responsibility and transparency are in line with international best practices and human rights standards, considering they both received consolidated results below 50% of the maximum possible score. In particular, information about their services and policies across a number of areas, including transparency reporting, content restrictions, account restrictions, network shutdowns, and handling and securing user information, are not proactively published on their websites.

Under the conditions of rapid development of the digital space, telecommunications operators as large as Magticom and Silknet have a growing responsibility as well as a need to provide their users with information about the terms and conditions of their services as clearly as possible, and proactively inform them about their commitments and procedures for protecting their data. The results of this survey provide an efficient roadmap that should be considered by the target companies to advance their corporate accountability as well as corporate policies on confidentiality and protection of personal data in accordance with international standards.

General Recommendations

- Both companies need to implement specific processes for responding to private, government, and court demands to restrict content or accounts, as well as government demands from foreign jurisdictions. If such processes already exist, they need to be disclosed and made available publicly.

- Both companies should disclose on their homepage the number of government demands received by country, the number of accounts affected, the number of pieces of content or URLs affected, the number of government demands by different legal authorities, and the number of government demands which were complied with. This data should preferably be updated at least once a year, and be made available as structured data files.

- Information should be available about the network management practices of the ISPs. Specifically, whether or not they engage in network prioritization, blocking, or delaying traffic for any reason. The companies should clearly disclose that they do not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring the quality of service and reliability of the network.

- Processes should be developed and implemented for addressing security vulnerabilities discovered by external security researchers. This includes a submission mechanism, disclosure of a timeframe for responding to submissions, and commitment not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting processes.

- A public archive or change log of all amendments to the terms of service should be easily accessible through the homepage and should contain all historical, as well as recent changes.

- The company's policies should include a process for notifying users about account restrictions, the policy should be as clear and unambiguous as possible and ensure the notification of users in all cases.

- The ISPs need to explicitly disclose their process for restricting service to a group or area of users with a comprehensive list of possible reasons, along with the reasoning behind why it may restrict access to specific applications or protocols (VoIP, messaging, or other services). Furthermore, the process for responding to government demands to shut down a network should be further emphasized, and the number of network shutdown demands received by specific public authorities should be publicly available. A publicly available commitment from ISPs to push back on government demands to shut down networks or restrict access to services is an important step towards safeguarding digital freedoms.

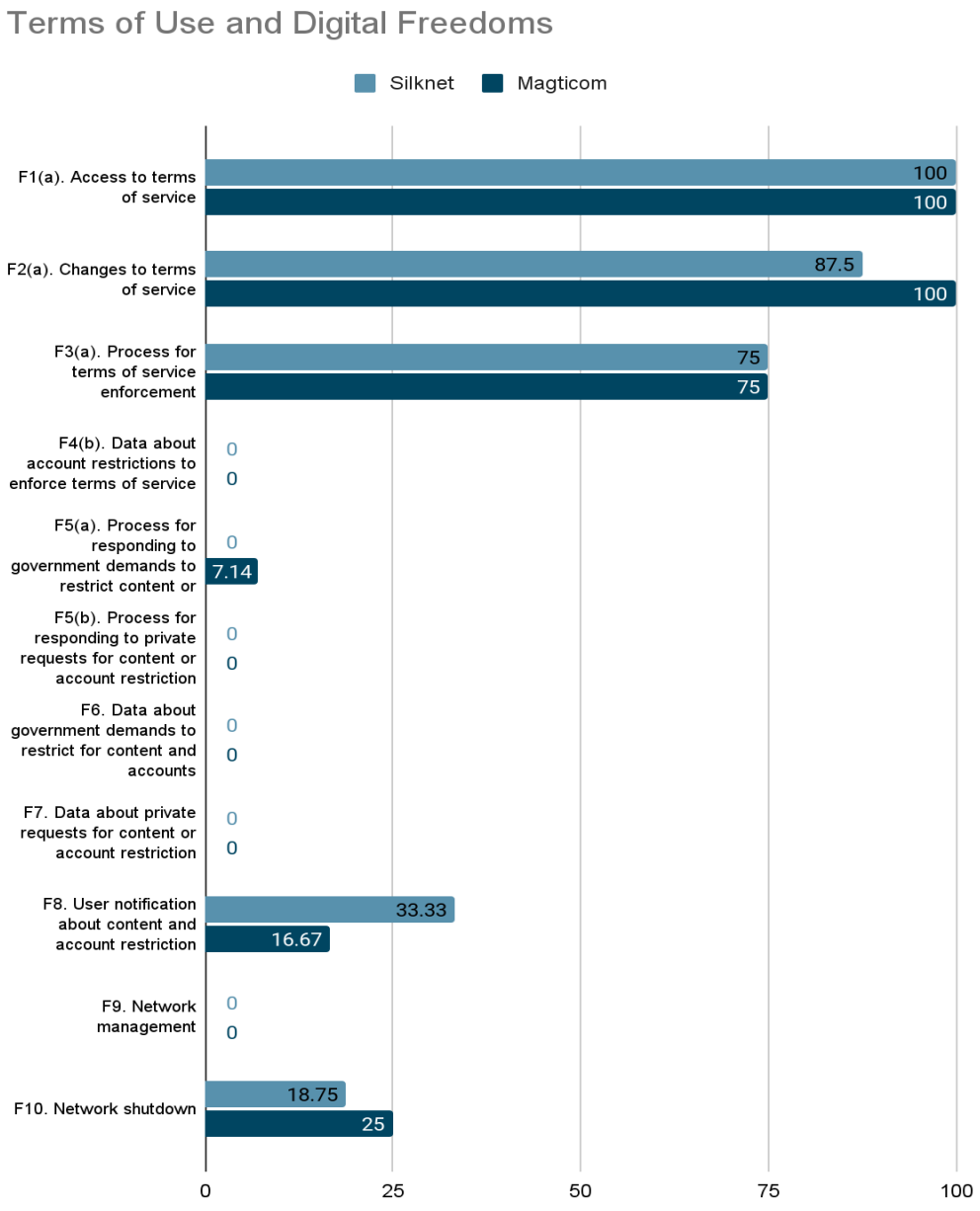
- For increased transparency, all changes made to the privacy policy should be archived, logged, and made available to the general public.

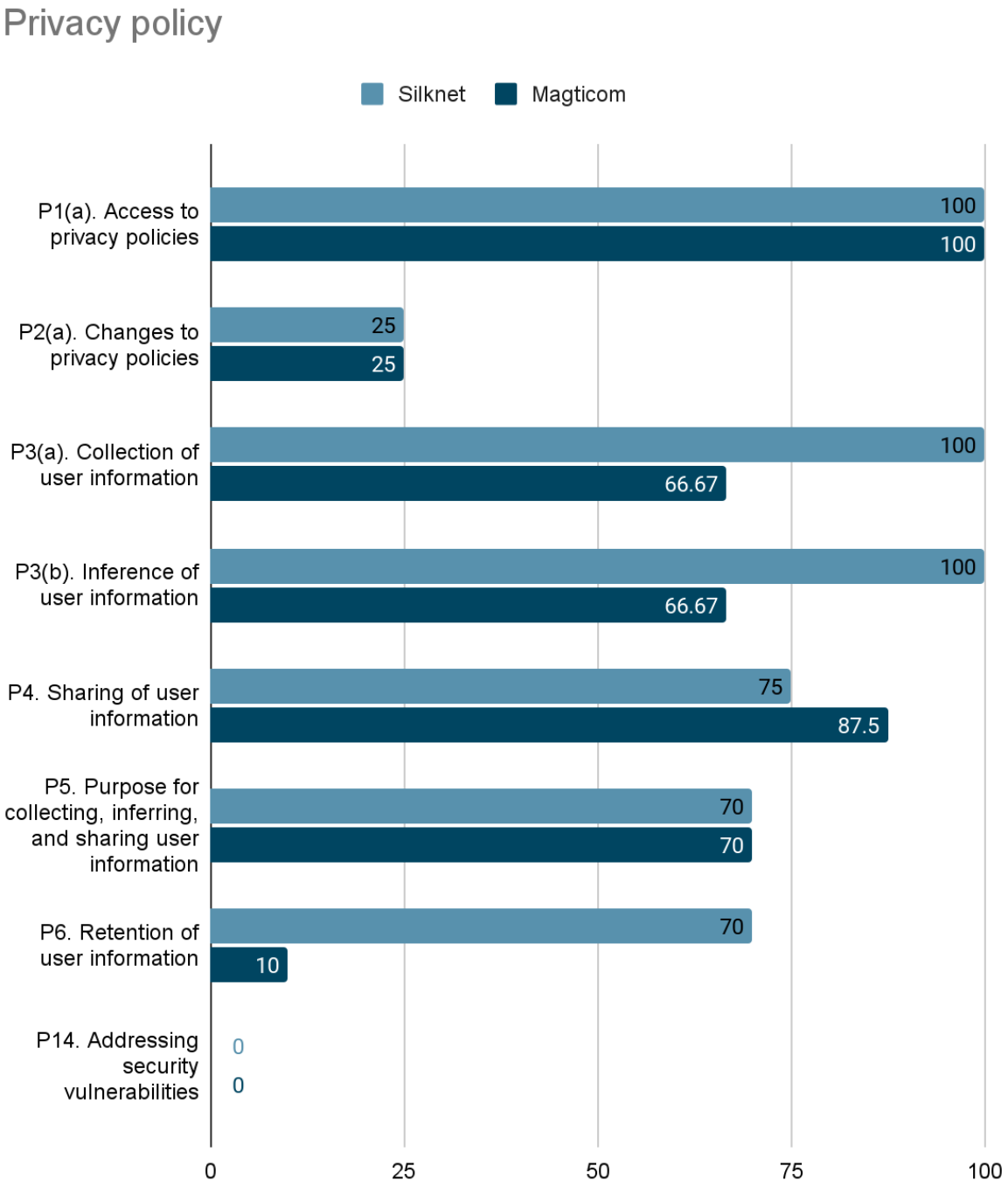
- ISPs should explicitly commit to limiting the collection of user information to what is directly relevant and necessary to accomplish the purpose of their service. Furthermore, ISPs should clearly disclose what types of collected information may be shared, what types of third parties it may be shared with, and for what specific purposes.

- ISPs should clearly disclose how long they retain each type of collected user information, as well as their methods for the de-identification of personal data.

Scorecard

	Silknet	Magticom
Total score	**44.98**	**39.45**




Privacy policy
Silknet
Magticom
P1(a). Access to privacy policies
100
100
P2(a). Changes to privacy policies
25
25
P3(a). Collection of user information
100
66.67
P3(b). Inference of user information
100
66.67
P4. Sharing of user information
75
87.5
P5. Purpose for collecting, inferring, and sharing user information
70
70
P6. Retention of user information
70
10
P14. Addressing security vulnerabilities
0
0
0
25
50
75
100

Appendix - Study Questions and Detailed Study Methodology

Ranking Digital Rights (RDR) is an independent research program at the policy think tank New America. RDR works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect user's rights. RDR evaluates the policies and practices of the world's most powerful tech and telecom companies and studies their effects on people's fundamental human rights. They are the only organization in the world that produces an open dataset on companies' commitments and policies affecting users' freedom of expression and privacy. Since 2015, the organization has published the RDR Corporate Accountability Index, which ranks the 26 most powerful companies worldwide, based on their own research methodology with standards grounded in international human rights standards. In 2021, the RDR Index was split[10] into the Big Tech Scorecard, with the first edition published in April[11], and the Telco Giants Scorecard, with the first edition coming up in December 2021, to ensure more detailed attention to the harms that these different services and industries are responsible for.

The standards developed by RDR to assess companies are built on more than a decade of work by the human rights, privacy, and security communities. These standards include the U.N. Guiding Principles on Business and Human Rights, which affirm that just as governments have a duty to protect human rights, companies also have a responsibility to respect human rights. The RDR Index methodology also builds on the Global Network Initiative principles and implementation guidelines, which address ICT companies' specific responsibilities towards freedom of expression and privacy in the face of government demands to restrict content or hand over user information. It further draws on a body of emerging global standards and norms around data protection, security, and access to information.

The full RDR Index methodology includes 58 indicators, across three categories (Governance, Freedom of Expression, and Privacy), to measure if and how companies disclose policies and practices that affect users' freedom of expression and privacy. Each indicator has its own list of elements, which are the specific questions used to assess the companies' disclosures.

For this study, Georgian companies were assessed based on the following 20 indicators selected for their relevance to the country's context.

Indicators and their elements

Freedom of Expression and Information

- F1(a). Access to terms of service
    1. Are the company's terms of service easy to find?
    2. Are the terms of service available in the primary language(s) spoken by users in the company's home jurisdiction?

[10] https://rankingdigitalrights.org/2022/02/23/new-corporate-accountability-index-big-tech-scorecard/
[11] https://rankingdigitalrights.org/index2022/

3. Are the terms of service presented in an understandable manner?

- F2(a). Changes to terms of service

1. Does the company clearly disclose that it directly notifies users about all changes to its terms of service?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
4. Does the company maintain a public archive or change logs?

- F3(a). Process for terms of service enforcement

1. Does the company clearly disclose what types of content or activities it does not permit?
2. Does the company clearly disclose why it may restrict a user's account?
3. Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?
4. Does the company clearly disclose how it uses algorithmic systems to flag content that might violate the company's rules?
5. Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?
6. Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?
7. Does the company clearly disclose its process for enforcing its rules once violations are detected?

- F4(a). Data about content restrictions to enforce terms of service

1. Does the company publish data about the total number of pieces of content restricted for violating the company's rules?
2. Does the company publish data on the number of pieces of content restricted based on which rule was violated?
3. Does the company publish data on the number of pieces of content it restricted based on the format of content? (e.g. text, image, video, live video)?
4. Does the company publish data on the number of pieces of content it restricted based on the method used to identify the violation?
5. Does the company publish this data at least four times a year?
6. Can the data be exported as a structured data file?

- F4(b). Data about account restrictions to enforce terms of service

1. Does the company publish data on the total number of accounts restricted for violating the company's own rules?
2. Does the company publish data on the number of accounts restricted based on which rule was violated?
3. Does the company publish data on the number of accounts restricted based on the method used to identify the violation?
4. Does the company publish this data at least four times a year?
5. Can the data be exported as a structured data file?

- F5(a). Process for responding to government demands to restrict content or accounts

1. Does the company clearly disclose its process for responding to non-judicial government demands?
2. Does the company clearly disclose its process for responding to court orders?
3. Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?
4. Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?
5. Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?
6. Does the company commit to push back on inappropriate or overbroad demands made by governments?
7. Does the company provide clear guidance or examples of implementation of its process of responding to government demands?

- F5(b). Process for responding to private requests for content or account restriction

1. Does the company clearly disclose its process for responding to requests to remove, filter, or restrict content or accounts made through private processes?
2. Do the company's explanations clearly disclose the basis under which it may comply with requests made through private processes?
3. Does the company clearly disclose that it carries out due diligence on requests made through private processes before deciding how to respond?
4. Does the company commit to push back on inappropriate or overbroad requests made through private processes?
5. Does the company provide clear guidance or examples of implementation of its process of responding to requests made through private processes?

- F6. Data about government demands to restrict for content and accounts

1. Does the company break out the number of demands it receives by country?
2. Does the company list the number of accounts affected?
3. Does the company list the number of pieces of content or URLs affected?
4. Does the company list the types of subject matter associated with the demands it receives?
5. Does the company list the number of demands that come from different legal authorities?
6. Does the company list the number of demands it knowingly receives from government officials to restrict content or accounts through unofficial processes?
7. Does the company list the number of demands with which it complied?
8. Does the company publish the original demands or disclose that it provides copies to a public third-party archive?
9. Does the company report this data at least once a year?
10. Can the data be exported as a structured data file?

- F7. Data about private requests for content or account restriction

1. Does the company break out the number of requests to restrict content or accounts that it receives through private processes?
2. Does the company list the number of accounts affected?
3. Does the company list the number of pieces of content or URLs affected?
4. Does the company list the reasons for removal associated with the requests it receives?

5. Does the company clearly disclose the private processes that made requests?
6. Does the company list the number of requests it complied with?
7. Does the company publish the original requests or disclose that it provides copies to a public third-party archive?
8. Does the company report this data at least once a year?
9. Can the data be exported as a structured data file?
10. Does the company clearly disclose that its reporting covers all types of requests that it receives through private processes?

- F8. User notification about content and account restriction

1. If the company hosts user-generated content, does the company clearly disclose that it notifies users who generated the content when it is restricted?
2. Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?
3. In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)?
4. Does the company clearly disclose that it notifies users when it restricts their account?

- F9. Network management (telecommunications companies)

1. Does the company clearly disclose a policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?
2. Does the company engage in practices, such as offering zero-rating programs, that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network?
3. If the company does engage in network prioritization practices for reasons beyond assuring quality of service and reliability of the network, does it clearly disclose its purpose for doing so?

- F10. Network shutdown (telecommunications companies)

1. Does the company clearly disclose the reason(s) why it may shut down service to a particular area or group of users?
2. Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?
3. Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?
4. Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?
5. Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?
6. Does the company clearly disclose the number of network shutdown demands it receives?
7. Does the company clearly disclose the specific legal authority that makes the demands?
8. Does the company clearly disclose the number of government demands with which it complied?

Privacy

- P1(a). Access to privacy policies

1. Are the company's privacy policies easy to find?
2. Are the privacy policies available in the primary language(s) spoken by users in the company's jurisdiction?
3. Are the policies presented in an understandable manner?

- P2(a). Changes to privacy policies

1. Does the company clearly disclose that it directly notifies users about all changes to its privacy policies?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
4. Does the company maintain a public archive or change logs?

- P3(a). Collection of user information

1. Does the company clearly disclose what types of user information it collects?
2. For each type of user information the company collects, does the company clearly disclose how it collects that user information?
3. Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?

- P3(b). Inference of user information

1. Does the company clearly disclose all the types of user information it infers on the basis of collected user information?
2. For each type of user information the company infers, does the company clearly disclose how it infers that user information?
3. Does the company clearly disclose that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?

- P4. Sharing of user information

1. For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
2. For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?
3. Does the company clearly disclose that it may share user information with government(s) or legal authorities?
4. For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information?

- P5. Purpose for collecting, inferring, and sharing user information

1. For each type of user information the company collects, does the company clearly disclose its purpose for collection?
2. For each type of user information the company infers, does the company clearly disclose its purpose for the inference?

3. Does the company clearly disclose whether it combines user information from various company services and if so, why?
4. For each type of user information the company shares, does the company clearly disclose its purpose for sharing?
5. Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred?

- P6. Retention of user information

1. For each type of user information the company collects, does the company clearly disclose how long it retains that user information?
2. Does the company clearly disclose what de-identified user information it retains?
3. Does the company clearly disclose the process for de-identifying user information?
4. Does the company clearly disclose that it deletes all user information after users terminate their account?
5. Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?

- P14. Addressing security vulnerabilities

1. Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?
2. Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities?
3. Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?