



**FILTER
WATCH**

TARAAZ
TECHNOLOGY & HUMAN RIGHTS



A
REPORT
BY
FILTER
WATCH
AND
TARAAZ

DIGITAL RIGHTS & TECHNOLOGY SECTOR ACCOUNTABILITY IN IRAN:

THE CASE OF MESSAGING APPS

Acknowledgments

This report has come about as the result of a great deal of hard work and a series of expansive conversations on the part of the researchers at **Taraaz** and **Filterwatch**. The research itself was developed and undertaken by Roya Pakzad, in coordination with Melody Kazemi.

The authors of this report would also like to thank Kaveh Azarhoosh and James Marchant for their contributions throughout the drafting of this research, and extend their gratitude to Simin Kargar, Amir Rashidi and Farzaneh Badiei for kindly sharing their time and providing feedback on earlier versions of this publication. Special thanks also to Small Media's information designer Surasti Puri, for her wonderful work to bring this report to life.

Finally, the authors are also grateful to the team at **Ranking Digital Rights** (RDR) for their support and engagement throughout the process of designing and assembling this research. This report couldn't have come to fruition without invaluable feedback from RDR's Research Director, Amy Brouillette; RDR's Senior Policy Analyst, Nathalie Maréchal; and RDR's Company Engagement Lead and Research Analyst, Jan Rydzak. Last, but indeed not least, we are grateful for the support of RDR's Director, Jessica Dheere, and Founding Director, Rebecca MacKinnon.

It is our hope that our adapted version of the Ranking Digital Rights Corporate Accountability Index methodology might be of use to other researchers and advocates working to ensure that technology companies properly uphold their users' fundamental rights online.

Report produced in partnership between:



RANKING DIGITAL RIGHTS
METHODOLOGY ADAPTATION



Contents

4 Executive Summary

9 An Overview of Digital Rights in Iran

13 Technology Companies and Human Rights

15 Technology Companies and Human Rights in Iran

17 Transparency and Accountability in Technology Companies

17 The UN Guiding Principles on Business and Human Rights (UNGPR)

19 Evaluating the Human Rights Commitments of Technology Companies

19 Ranking Digital Rights: Accountability and Transparency in Iranian
Technology Companies

21 Who is this report for?

22 Data Collection and Analysis

25 Summary of Findings

34 Company Score-Cards

35 Soroush/Soroush Plus

36 Gap Messenger

37 Bale

38 BisPhone

40 WhatsApp

41 Telegram

42 General Recommendations

42 Recommendations for companies

45 Recommendations for the Iranian government

46 A few words for civil society groups and technology researchers

47 Methodology Appendix

48 Challenges and Lessons Learned

50 Indicators

59 Disclosure vs. Practice

60 Digital Rights Workbook: Start the Conversation in Your Company

64 Acronyms and Glossary of Terms

*The Iran Tech
Accountability
Report 2020*

*2019 Ranking
Digital
Rights (DD)
Corporate
Accountabil-
ity Index*

EXECUTIVE SUMMARY

DIGITAL RIGHTS & TECHNOLOGY SECTOR ACCOUNTABILITY IN IRAN

THIS report, **'Digital Rights & Technology Sector Accountability in Iran'**, examines the role of a frequently overlooked, but vitally important group of actors in the digital ecosystem of Iran: Iranian private-sector technology companies. From January to September 2020, we examined the digital rights commitments of a number of technology companies in Iran. This report highlights how technology companies' activities impact the digital rights of Iranians and summarizes companies' responsibilities in upholding those rights.

The report's methodology is based on an adapted version of **the 2019 Ranking Digital Rights (RDR) Corporate Accountability Index**. Since 2015, the RDR Corporate Accountability Index has evaluated "the world's most powerful internet, mobile, and telecommunications companies' disclosed policies and practices affecting users' freedom of expression and privacy." Digital rights researchers around the world, including in Russia, Kenya, Senegal, countries from the Arab region, India, and Pakistan, have adapted the methodology to assess companies in their own countries and to guide them towards greater transparency.¹ Now for the first time, the RDR

methodology is being applied to assess the policies of private technology companies in Iran.

In order to show their commitment to users' fundamental rights, the first step for companies is to disclose their policies and practices affecting those rights. Transparency enables the demand for accountability; once policies and practices are available publicly, journalists can use them in their investigative reporting; technology auditors can test products to ensure what is said matches actual practice; and civil society groups and legal scholars can evaluate the pitfalls and strengths of corporate policies. By publishing this report, we hope to bring attention to the importance of transparency and human rights — as laid out in the UN Guiding Principles on Business and Human Rights — in relation to Iranian technology companies.²

In this iteration, we assessed the publicly disclosed policies and practices of the messaging services used on a daily basis by Iranian internet users. This includes four domestic Iranian messaging services (Soroush, Gap, Bale, and BisPhone) in addition to two of their foreign counterparts: WhatsApp and Telegram. Although we decided to rank messaging apps, readers should know that

¹RDR Adaptations, Ranking Digital Rights, <https://bit.ly/2H40QcT>

²The UN Guiding Principles on Business and Human Rights, HR/PUB/11/04, United Nations, 2011, <https://bit.ly/2Iyy0Z7>

almost all indicators used to assess messaging apps apply to other mobile services and internet companies as well.

Key Findings and Observations

- ✦ Almost all the assessed companies disclosed pieces of information about their privacy policy and terms of services (ToS). In several cases, among both domestic and foreign apps, such information was integrated in Frequently Asked Questions (FAQ) pages and other publicly available documents on companies' websites as opposed to a specific page for privacy policies or ToS. It is important that this information be easily findable by users before signing up to use a service.
- ✦ Companies received the lowest scores in disclosure about handling governments and third-parties' requests for access to users' information, censoring content, and restricting accounts. None of the Iranian companies disclosed the degrees to which, or how they enforce their terms of services and privacy policies. In addition, neither did they disclose information about their employees' training programs on digital rights, conducting human rights impact assessments, and engaging with civil society groups and other stakeholders.
- ✦ Foreign messaging services also received far from perfect scores. Given these companies' significant number of Iranian and Persian-speaking users, the lack of Persian-translated versions of privacy policies, terms of services, educational materials about safety and security, and appeals processes, in addition to lack of transparency around country and language-specific procedures for enforcing terms of services may have discriminatory impacts on Iranian users, especially for people with lower levels of (digital) literacy. In addition, the levels of access available to companies' APIs, especially in the case of Telegram, have unlocked new forms of potential misuses. This shows the importance of companies' role in preventing such misuses by conducting human rights impact assessments, and by applying and disclosing more rights-respecting developers policies and terms of use.
- ✦ In the case of one Iranian messaging company, we noticed discrepancies between disclosures in the English version of the company's website as compared to the Persian and Arabic versions. The company also advertised the same product via another brand name for international users. In this case, the justification was to evade technological sanctions against Iranian companies and be able to enter the international market. However, these practices create ambiguities about companies' accountability mechanisms toward different legal jurisdictions and data protection regulations. We also noticed that despite some Iranian companies' claims for applying best privacy practices such as end-to-end encryption, there is no public document about technical details.
- ✦ Unchecked and state-controlled internet localization plans — often accompanied by Iranian government's partnerships and

investment in the growth of the domestic technology sector — have created ambiguities around accountability and companies' governance practices. The addition of e-government services into messaging apps has raised new concerns about data collection and data sharing between private companies and government agencies such as the Central Bank of Iran, the Ministry of Education, and the Islamic Republic of Iran Broadcasting (IRIB). These are examples of how infringements of the right to privacy and the right to freedom of expression may negatively impact other socio-economic, cultural, civil, and political rights as well. In the coming years we anticipate more of these partnerships and ambiguous governance practices, not only in Iran, but also in countries that have been expanding their own state-driven digital localization plans.

Overall, our assessment shows that while companies have made minor attempts to disclose their policies and practices, those disclosures are not sufficient to earn Iranian Internet users' trust in their services. It is our hope that companies will use this report as a guide for addressing the shortcomings we have identified, and to protect their users from actual and potential human rights harms.

Recommendations to technology companies

- ✦ Companies should be transparent about their processes for responding to governments' requests to access users' information, censor content, and restrict accounts. In addition, they should disclose information about how they enforce their terms of services, and handle data breaches and security loopholes. They should publish this information in comprehensive and structured forms and update them regularly.
- ✦ Given the growing partnerships between Iranian government agencies and domestic messaging services, companies should clearly disclose whether they provide Iranian government agencies with special direct or indirect access to users' information. In addition they should be transparent about their ownership and governance structures. This can be done by creating detailed and functional "about us," "contact us," and social media pages in addition to taking more formal steps such as releasing information about the extent of their partnerships with other public and private agencies, their financial reports, information about the board of directors, and reports of annual corporate meetings.
- ✦ Companies should apply industry best practices such as privacy by design principles in the design and development of their services. They should also release information about their internal security audits, release documents about their services' technical details and source

codes, and provide bounty programs in order to allow cybersecurity researchers to examine their services against any privacy and security vulnerabilities.

- ✦ Companies should follow the UN Guiding Principles on Business and Human Rights. They should create and publish a human rights policy and conduct regular human rights impact assessments to prevent risks, especially to vulnerable groups such as children, religious minorities, gender and sexual minorities, ethnic minorities, and refugees. They should limit their employees' access to users' data, educate their employees about digital rights, and engage in multi-stakeholder initiatives especially with civil society organizations.

vulnerable groups and Iranians of lower socio-economic status. Adding e-government features into private messaging services, providing short-sighted economic incentives for using local internet services vs international ones, or providing free state-backed services for technology start-ups such as data centers should not be simply publicized as the government's well-meaning plans for "supporting" domestic start-ups. In the absence of public and transparent oversight mechanisms, these ambiguous partnerships jeopardize users' trust in those companies, result in the over-regulation of those companies, create a culture of favoritism and unfair competition among private technology companies in Iran, and alienate them from the international market.

Recommendations to the Iranian government

- ✦ The Iranian government should stop its unchecked and mandatory digital localization plans that massively compromise net neutrality principles. These plans, which are mainly carried out by blocking access to international services, either through filtering or preferential tariffs for domestic services, have been undermining users' freedom of choice and freedom of access to information, with a disproportionate negative impact on

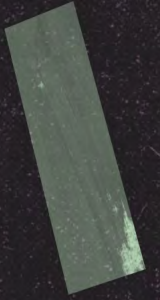
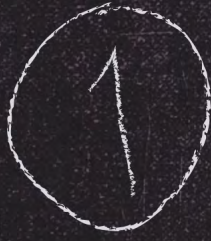
- ✦ The Iranian government should implement a robust and comprehensive data protection legal framework in line with internationally recognised human rights standards. They should set requirements for companies regarding their privacy and security practices. Until Iran possesses a comprehensive rights-respecting legal framework for data protection, they should halt the progress of the "Managing Social Messaging Apps" bill which restricts Iranians' online freedoms and gives the Armed Forces control over internet gateways.



AN OVERVIEW OF DIGITAL RIGHTS IN IRAN

NATIONAL
INFORMATION
NETWORK

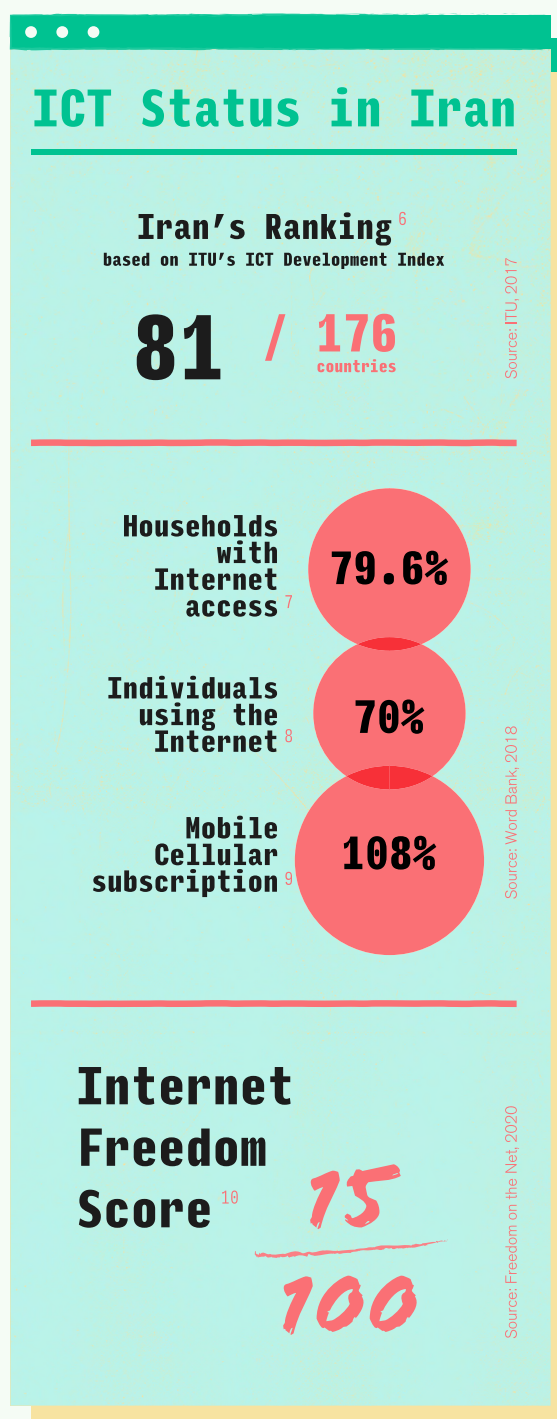
*Iran's
Information and
Communications
Technologies
have undergone
significant
growth.*



IN 2016, the United Nations (UN) Human Rights Council released a resolution stating that “the same rights people have offline must also be protected online.”³ Access to the internet plays a pivotal role in the enjoyment of our human rights in the digital age, and as the line between the online and offline worlds continues to blur, human rights violations have become a fact of Internet life. Having ratified both the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), Iran has a duty to respect, protect, and fulfill its citizens’ rights as enshrined in these UN conventions.⁴ To understand Iran’s track record in upholding its human rights commitments in the digital age, let’s take a step back and look at the country’s digital technologies from both technical and policy standpoints.

During the past decade, Iran’s Information and Communications Technologies (ICTs) have undergone significant growth. Starting in 2006, the Iranian government introduced its plan to develop what it calls the ‘National Information Network’ (NIN). One goal of the NIN has been to develop an infrastructure to enhance the speed and accessibility of the Internet. Other major goals include: fostering resilience

[Fig 1]



³ “The promotion, protection and enjoyment of human rights on the Internet,” A/HRC/32/L.20, UN Human Rights Council, June 27, 2016, <https://bit.ly/3oKIDUH>

⁴ Both UN conventions were ratified by Iran in 1976. You can find the information on Status of Ratification: Interactive Dashboard, <https://indicators.ohchr.org/>

with respect to potential technological and monetary sanctions; establishing security measures against cyberattacks; subsidizing and encouraging domestic startups, e-business, and entrepreneurial initiatives.⁵

However, another clear intent of the Iranian government has been to make the NIN into a tool for the state to maintain its internet control and apply its damaging digital localization policies. Such un-checked localization strategies have undermined the principles of net neutrality and pressured Internet Service Providers to block access to content online.¹¹ Rather than allowing the Iranian internet to be simply one sector of a larger global internet, Iran's leaders have increasingly sought to make internet users in Iran dependent on domestic digital technologies that are often under direct or indirect state control. Many human rights organisations have warned that the process is likely to lead to the further isolation of Iranian internet users in the future.¹²

In connection, it is also important to note that the U.S. efforts to isolate and sanction Iran have, in fact, helped the Iranian government to advance its unchecked digital localization plans.¹³ The issue is not always the U.S. sanctions themselves, but the ambiguities around them. In 2014 the U.S. government issued General License D-1 to authorize American technology companies to provide certain "personal communications" technologies for Iranians with a goal of fostering Internet freedom in Iran. As of today, the General License D-1 has stayed intact.¹⁴ However, to avoid any potential legal, reputational, and financial harms, it seems that many American technology companies simply hope to avoid the complications of doing any business with Iran, even when this business is legal.¹⁵ The result of this has been widespread frustration among Iranian internet users and technology entrepreneurs in Iran, which plays into the Iranian government's narrative of digital localization and their message to the domestic technology sector of "do it our way or no way."

⁵ Supreme Council for Cyberspace Resolution, "Explanatory Document on the Requirements of the National Information Network," Islamic Parliament Research Center of The Islamic Republic of Iran, September 18, 2017, <https://bit.ly/3jExXD8>

⁶ "Measuring the Information Society Report 2017", International Telecommunication Union, <https://bit.ly/3khhMDW>

⁷ "UPR Session 34, Iran Freedom of Expression and Internet Freedom", UPROAR, <https://bit.ly/2HfId76>

⁸ "Individuals Using the Internet", World Bank, 2018, <https://bit.ly/3464BZY>

⁹ "Mobile Cellular Subscriptions (per 100 people) - Islamic Republic of Iran", World Bank, 2018 <https://bit.ly/3j4MqIf>

¹⁰ "Freedom on the Net Report 2020 - Iran", Freedom House, 2020, <https://bit.ly/2TztVKn>

¹¹ "Tightening the Net: Internet Security and Censorship in Iran - Part 1: The National Internet Project", Article 19, 2016, <https://bit.ly/3k4gKnL>

¹² "Joint submission to the Universal Periodic Review of the Islamic Republic of Iran by Article 19 and Access Now", Access Now, April 4 2019, <https://bit.ly/3m5CKzh> Fa version: <https://bit.ly/2H88DIv>

¹³ Azin Mohajerin, "To Help the Iranian People, Reverse Tech Sanctions Asap", Atlantic Council, January 17, 2020, <https://bit.ly/3o09lIf>

¹⁴ Mahsa Alimardani and Roya Pakzad, "Silicon Valley preaches diversity and inclusion while excluding Iranians", Atlantic Council, April 8, 2019, <https://bit.ly/3dug3BC>

¹⁵ Examples include Google's decision to block the App Engine and the Google Cloud Platform, Amazon's decision to block AWS for Iranians inside the country, and more. Check out this link to see the services that are not available inside Iran: <https://bit.ly/31eB0eL>

However, the purpose of this report is neither to fully analyze the role that the Iranian authorities play in limiting the digital rights of people in Iran, nor to look at other foreign countries or companies' roles in affecting digital rights of Iranians. **The goal of this research is to highlight how Iranian technology companies' activities might impact the digital rights of Iranians and to summarize the responsibilities of those companies' for upholding these rights.**



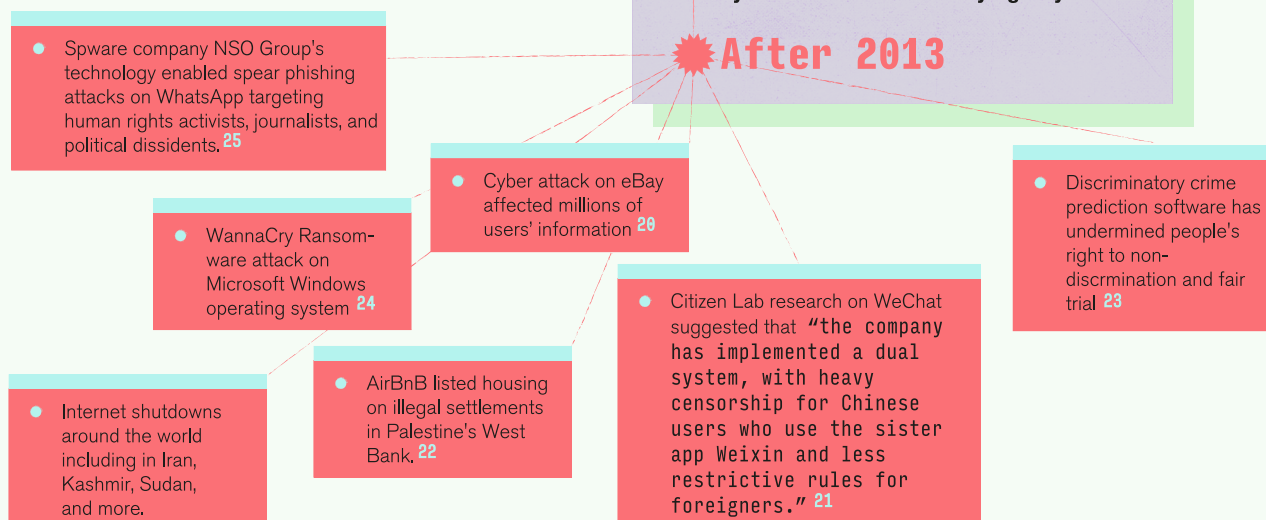
TECHNOLOGY COMPANIES AND HUMAN RIGHTS



THE IRAN TECH
ACCOUNTABILITY
REPORT 2020

In recent years, not a day has passed which didn't bring another story about the tangled relationships between human rights and technology. In the timeline, we highlight a few of the major global events involving technology companies and human rights over the past fifteen years.

[Fig 2]



¹⁶ Rebecca MacKinnon, “Consent of the Networked: The Worldwide Struggle For Internet Freedom,” (Basic Books, 2013), 133

¹⁷ The Global Network Initiative, 2008, <https://bit.ly/37ck4JD>

¹⁸ Google Transparency Report, <https://bit.ly/37eFvKm>

¹⁹ Glenn Greenwald, “NSA Prism Program Taps into User Data of Apple, Google and Others”, Guardian, June 7, 2013, <https://bit.ly/3khdd10>

²⁰ Samuel Gibbs, “Ebay Urges Users to Reset Passwords After Cyberattack”, Guardian, May 21, 2014, <https://bit.ly/342gShJ>

²¹ Lotus Ruan, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata, “One App, Two Systems How WeChat uses one censorship policy in China and another internationally,” November 2016, <https://bit.ly/2SXyZPN>

²² Hillary Leung, “Airbnb Faces Renewed Criticism Over Listing Occupied West Bank”, Time, May 15, 2019, <https://bit.ly/2T6FkrX>

²³ Angwin et al., “Machine Bias”, ProPublica, May 23, 2016, <https://bit.ly/2T1QsGA>

²⁴ Microsoft Security Response Center, “Customer Guidance for WannaCrypt Attacks” Microsoft, May 12, 2017, <https://bit.ly/31bHFX8>

²⁵ “NSO Group/ Q Cyber Technologies: Over One Hundred New Abuse Cases”, CitizenLab, October 29, 2019, <https://bit.ly/3j5YU2m>

Technology Companies and Human Rights in Iran

Iranian technology companies also demonstrate the ambivalent relationship between tech companies and human rights. Here we list a few incidents that happened in Iran to elaborate on emerging concerns about technology companies and human rights, and particularly on the issues around data protection, content takedowns, government requests, ambiguities around enforcing online community guidelines, transparency, and more.

Example 1 Knockoff Telegrams and Users Data Leak

In March 2020, news broke that 42 million records of users' information from HotGram and Talagram – two forked versions of Telegram – were leaked and exposed on a website. The records included users' account ID, username, phone number, and last login status.²⁶ After a few days, the website removed access to the data. However, it is clear that the damage to users' right to privacy has already been done. This is not the first time that digital rights advocates have raised concerns about such forked versions of Telegram. During the 2020 parliamentary elections, many users were added to these forked versions of Telegram groups involuntarily.²⁷ It is believed that by promising a

significant amount of money, those Telegram groups had been asking users to add as many other users as they could. The more users being forcefully added to the group, the more money the person who added them would receive!

The above examples show how fragile our privacy is when it comes to using digital services that don't have sufficient safeguards to protect users' information during data collection and storage. Given the lack of transparency around how users' data is collected, how it is stored and who has access to it, it's almost impossible to hold anyone to account when damage has been done. The example in the paragraph above shows how important it is for any messaging services to apply "privacy by design" principles and give power to users to control their privacy settings to prevent such privacy-invasive actions.²⁸

Another issue here is that HotGram and Talagram are both forked versions of Telegram. In this case, we must not only consider the responsibilities of app marketplaces (e.g. Cafe Bazaar, Myket, Sibapp) for conducting due diligence before hosting those apps on their platforms, but also question Telegram's Application Programming Interface or APIs' terms of service. To what extent should Telegram have safeguards and oversight over the ways that developers use Telegram's APIs to develop bots and knock-off Telegram apps?

²⁶ Melody Kazemi, "Data Insecurity On Iran's Localised Internet," Filterwatch, Jun 19, 2020, <https://bit.ly/2H80a7J>

²⁷ "Add Your Friends, Make Money!," ISNA, February 15, 2020, <https://bit.ly/31cSxEk>

²⁸ "A Guide to Privacy by Design," October 2019, <https://bit.ly/3nV1kXJ>

Example 2 Maxim Taxi and Tehran Municipality Request

In April 2019, the Tehran Municipality requested access to users' data from a ride-sharing app, Maxim. In response, Hamid Bazrgar, the CEO of the company, refused to fulfill the request. He noted that their users' information is the company's "red line" that they are not willing to cross; Bazrgar added that he didn't want to jeopardize the trust his company had built with its users by complying with the municipality's request. He further stated that users' information should not be given out unless under special circumstances when there is a valid court order issued by an official judicial body.²⁹

This example shows that in the absence of a clear legal process, it could be easy for a non-judicial body to request access to private data. It also highlights the responsibility of companies in pushing back against requests that have not gone through official judicial processes.

Example 3 DigiKala and Identity Verification

An Iranian user raised a concern on Twitter about the way DigiKala, an e-commerce start-up in Iran, requested access to scanned copies of his national identity and debit cards. According to this user's Twitter thread, DigiKala

asked for copies of his cards to verify his identity and process a payment for a returned item.³⁰ However, requesting access to users' sensitive information via email is privacy-invasive and demonstrates neglect for proper cybersecurity practices. It is also not clear who and how many employees at DigiKala can see the user's copies of national identity cards and for how long DigiKala keeps this information. The example raises concern about how many other companies also request unjustified access to users' personally identifiable information without being challenged? And how many companies apologize for their actions and provide adequate remedies for users?

Example 4 Blogging Platforms and Content Takedowns

In 2010, site managers of three Iranian blogging platforms including Blogfa, Mihan Blog, and Blog Sky published an open letter to share their frustrations about heavy-handed government content filtering requests on their websites.³¹ In their letter, they mentioned that sometimes the Committee for Determining Instances of Criminal Content (CDICC), which is responsible for blocking "immoral" content, asked them to block an entire blog page solely on the basis of a single post that was written many years ago. To give another example, the site managers mentioned that to appeal the blocking decision, bloggers have to show up physically at the CDICC office and get

²⁹ Arash Karimbeigi, "Maxim Taxi: The Municipality wants our Customer Data," ICTAna, April 14, 2019, <https://bit.ly/2HbyPkW>

³⁰ Twitter thread from an Iranian user, Twitter, April 18, 2020, <https://bit.ly/3j1dmbL>

³¹ "Performance of the Filtering Organisation and the Weakening Position of Farsi Weblog Services," BlogFa, December 4, 2010, <https://bit.ly/3443sBT>

permission to unblock their blog pages. Not only do these practices have a chilling effect on users' freedom of expression online, but from the point of view of the letter's authors, it has a counterproductive effect and encourages users to choose non-Iranian blogging platforms over domestic ones. The authors of the letter asked the CDICC to allow them to at least first send a warning to bloggers, instead of taking down the entire blog page without any prior notice.

Transparency and Accountability in Technology Companies

THE above section has shed light on how technology companies' practices may lead to violations of digital rights; we have also seen examples of the ways in which companies themselves may play a positive role to protect Iranian citizens from governmental illegitimate requests which undermine users' rights.

Despite the fact that technology companies' practices in each country depend on the country's political system, economic structure, and legal frameworks, there are still broad similarities between companies' practices with respect to digital rights concerns. Below, we explore some resources that are built on

internationally accepted principles. These resources help human rights advocates to assess technology companies' disclosed policies and to guide them toward applying rights-respecting practices.

The UN Guiding Principles on Business and Human Rights (UNGPR)

One of the internationally accepted frameworks used to explain the human rights duties of companies is the UN Guiding Principles on Business and Human Rights (UNGPR).³² In 2011, the UN Human Rights Council unanimously endorsed the UNGPR as an official business and human rights framework, applicable to every state and company around the world. UNGPR comprises 31 principles which are divided into three foundational pillars: the state's duty to protect human rights, the corporation's duty to respect human rights, and the duty of both corporations and states to provide access to remedy.

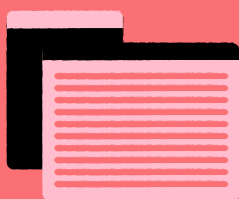
It is also important to note that by respecting human rights and following international guidelines, companies can guarantee that it would be less likely for them to face financial, reputational, and legal risks. This is achieved by gaining users' trust, avoiding boycotts, winning over their competitors, keeping away from sanctions, and attracting more international partnerships and transnational investment. This

³² The UN guiding Principles on Business and Human Rights, HR/PUB/11/04, United Nations, 2011, <https://bit.ly/2Iyy0Z7>



Pillar 1 States' duty to protect human rights

Governments should protect human rights by developing laws, regulations, and policies to ensure business practices don't infringe human rights.



Pillar 2 Corporates' duty to respect human rights

Businesses, regardless of their size, sector, or ownership model, should respect human rights in all their activities.

In order to adhere to their duties, they should carry out human rights due diligence. Human rights due diligence includes the following steps:

- ▶ Having a publicly available human rights policy;
- ▶ Conducting human rights impact assessments to understand how their services, activities, and business relationships might cause, contribute, or directly link to actual and potential adverse human rights impacts;
- ▶ integrate those findings in their policies and practices;
- ▶ track the responses; and communicate how they take measures to address the identified negative human rights impacts.



Pillar 3 States and corporates duty to provide access to remedy

When human rights are violated because of business's activities or services, both states and businesses have responsibility to ensure that victims have access to effective remedy.

[Fig 3]

is especially important for those start-ups who want to expand their market beyond Iran's borders. According to Sazman Nezam Senfi Rayanei Keshvar (or NASR)'s survey of 347 Iranian start-ups, 11.8% responded that they

are active in international markets and are hoping to increase their international presence in the near future.³³ **They should know that in order to play internationally, they have to adhere to international standards too!**

³³ "An Analysis of of the Startup Space in Iran", Computer Guild Organisation of Iran, November/December 2019, <https://bit.ly/3j0MkS1>

Evaluating the Human Rights Commitments of Technology Companies

UNGPs apply to all companies in every industry, including the ICT sector. To make UNGPs more practical for ICT companies, technology and human rights researchers have developed resources to assess and guide companies towards greater transparency and rights-respecting practices. Among these resources are the Ranking Digital Rights Corporate Accountability Index, a ranking method to “evaluate [the] most powerful internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy of internet users across the world.”³⁴

Ranking Digital Rights: Accountability and Transparency in Iranian Technology Companies

For this project, we opted to use the 2019 Ranking Digital Rights Corporate Accountability Index methodology to assess the digital rights commitments of technology companies in Iran. We decided to use the RDR Index methodology for several reasons:

1. The methodology is not for a specific region or country; it is global. The RDR Index

methodology is based on internationally accepted human rights frameworks and is in line with the UN Guiding Principles on Business and Human Rights. The open source nature of the RDR Index methodology means that it can be readily adapted by others seeking to apply the methodology to companies locally or regionally.

2. By providing detailed privacy, freedom of expression and governance indicators — and several elements for each indicator — the RDR Index is a practical tool not only to assess and rank companies but to identify major weaknesses and strengths. This helps researchers to provide tailored recommendations based on a company’s assessment against each indicator. Companies themselves can also use the methodology to identify and address their shortcomings.
3. Digital rights researchers from different economies and political systems (including in Russia, Kenya, Senegal, countries from the Arab region, India, Pakistan) have also adapted the methodology to rank companies in their country and to guide them towards better digital rights practices.³⁵ By adding Iranian technology companies to the growing list of RDR adaptation projects, we hope to contribute to the global debate around digital rights and business responsibilities, especially in the context of closed and semi-closed political systems.

³⁴ “2019 Ranking Digital Rights Corporate Accountability Index”, Ranking Digital Rights, <https://bit.ly/2SZb421>

³⁵ “RDR Adaptations”, Ranking Digital Rights, <https://bit.ly/2H40QcT>

While the RDR Index methodology focuses on the right to privacy and the right to freedom of expression, readers should acknowledge that human rights are all “interrelated, interdependent and indivisible.”³⁶ Infringement on one may violate another and protection of one right may fulfill others. Especially in the context of vulnerable groups, the implications of infringing on online privacy and freedom of expression go beyond these two rights and negatively impacts other civil, political, socio-cultural, and economic rights. Here is an example: It is a fact that the Iranian government restricts the right of the Baha’i religious minority community to higher education by not accepting them to Iranian universities. As a result, this religious minority group relies heavily on e-learning platforms.³⁷ Imagine a data breach happens as a result of a company’s lack of security measures, or its compliance with authorities’ requests to access users’ information. In this case, it is not only users’ right to privacy that has been violated; as a result of the company’s action — or alternatively, lack of action — users’ rights to education, freedom of thought, conscience and religion, and even their right to life, liberty and security are potentially infringed.

For this iteration of the report, we chose to apply the 2019 RDR Index methodology to messaging app companies. Although we decided to rank messaging apps, readers should know that almost all of the indicators used to rate messaging apps apply to other mobile services and internet companies as well. Here are our reasons for choosing messaging apps:

1. Globally, messaging services are becoming more and more popular and instrumental in people’s lives. In March of 2019, Facebook CEO Mark Zuckerberg shared his view that “privacy-focused communications platforms will become even more important than today’s open platforms” and that “the future of communication will increasingly shift to private, encrypted services.”³⁸ In addition, according to We Are Social rating, after Facebook and YouTube, messaging services number among the most-used online services in the world.³⁹ Iran is not an exception from the global trend toward increasing use of closed-communication messaging services. Given the state’s media monopoly and lack of press freedom, messaging services play an important role for Iranians to practice their right to access information and freedom of expression. Before it was blocked, Telegram had 40

³⁶ “What are Human Rights,” The Office of the High Commissioner for Human Rights (UN Human Rights), <https://bit.ly/2TWHFwG>

³⁷ Tara Sepehri Far, “Glimmer of Hope in Iran for Long-Persecuted Baha’is?,” Human Rights Watch, January. 29, 2019, <https://bit.ly/34DaCNI> and “Iran: Allow Baha’i Students Access to Higher Education,” Human Rights Watch, Sep. 19, 2007, <https://bit.ly/3kGDt9t>

³⁸ Mark Zuckerberg, “A Privacy-Focused Vision for Social Networking,” Facebook, March 6, 2019, <https://bit.ly/3k82UA0>

³⁹ Claire Wardle, “Monitoring and Reporting Inside Closed Groups and Messaging Apps,” Verification Handbook 3, <https://bit.ly/3lSG05M>

million users in Iran;⁴⁰ WhatsApp Messenger was downloaded 33 million times on Cafe Bazaar.⁴¹ Even domestic messaging services are among the top downloaded services on Cafe Bazaar.

2. Legislative and financial support from the government places messaging apps at the center of Iran's digital localisation planning. On many occasions, the current ICT Minister Mohammad-Javad Azari Jahromi, has expressed his support of domestic messaging apps.⁴² With the lack of strong data protection laws and safeguards in Iran, the current draft of the "Managing Social Messaging Apps" bill, if passed, would heavily regulate messaging apps and pave the way for authorities to control those services.⁴³ In addition, to implement the localization agenda, the government decided to apply lower data tariffs on domestic messaging apps.⁴⁴ To further incentivize the use of these services, several government agencies and Iran's state-owned Central Bank have partnered with the messaging app companies in order to add mandatory built-in e-government and e-banking features. For instance, in April of this year, in response to the COVID-19 pandemic and school closures, The Ministry of Education used a social messaging app's infrastructure in order to provide a service called 'Shad', as an official

mandatory e-learning application for students and teachers to use.⁴⁵

This shows the important role that messaging apps play in Iranians' personal and professional lives with implications for various civil, political, economic, social, and cultural rights. In short, **assessing messaging apps can be a good starting point and a test case for exploring the overall health and shortcomings of start-up tech companies in Iran.**

Who is this report for?

This report – and the attached workbook – is for:

- ✦ **Technology companies in Iran** who are committed to respect human rights and are willing to do so by protecting their users. The ranking component of the report helps companies to spot their weaknesses and strengths and gives them access to a practical tool to compare themselves with their competitors.

The purpose of the accompanying workbook is to help companies to start discussion around digital rights internally. The workbook assists companies in

⁴⁰ "How Many Iranian Telegram and Domestic Messaging App Users are There," IRNA , May 22, 2019, <https://bit.ly/2T2jRk9>

⁴¹ WhatsApp Download Page, Cafe Bazaar, <https://bit.ly/31cTUmm>

⁴² "Jahromi: We are Obligated to Support Domestic Messaging Apps", IRINN, May 23, 2018, <https://bit.ly/37fd6DY>

⁴³ Melody Kazemi, "Policy Monitor - July 2020," Filterwatch, Aug. 14, 2020, <https://bit.ly/3gxr2Kv>

⁴⁴ "Use Domestic Messaging Apps with 1/3 [Data] Traffic", Pars Online, <https://bit.ly/37aTnVI>

⁴⁵ "Student Social Network (SHAD) is Ready for Operation," Iran's Ministry of Education, April 9, 2020, <https://bit.ly/3k76KKh>

learning how to navigate digital rights issues from the perspectives of the company's top executives, board members, designers and technologists, and their human resource, legal and communications teams.

In addition, this report informs investors (Iranian and foreign groups) who want to make investment in companies that are respectful to international norms. They can use the indicators to evaluate companies' track records with respect to their transparency around digital rights, and make informed investment decisions.

✦ **Civil society groups and journalists** inside and outside Iran who evaluate companies and help users to make better decisions in choosing digital services. Although we only ranked a few messaging apps during this research, the report – and the accompanying workbook – will help digital rights advocates inside Iran to evaluate other categories of mobile and web-based apps and services and compare them with each other against digital rights indicators. This will help them to hold companies to account with respect to their disclosed policies, and to demand greater transparency and higher digital standards. It will also help them to scrutinize government policies with respect to digital rights and technology companies. We also invite cybersecurity researchers and privacy engineers to use this report to test companies' products in order to ensure that

companies' disclosure about technical details matches the actual practice.

✦ **Users** who want to know how companies handle their information and want to protect themselves from online harms. It will help them put transparency, privacy and respect for freedom of expression and access to information at the center of their decisions when they choose and use digital services.

✦ Last but not least, this report is for **digital rights researchers and business and human rights practitioners** who work on adapting the RDR Index methodology for assessing technology companies in politically closed and semi-closed countries. In particular, we believe this report will help broader international digital rights advocates to understand the nuances of digital localization strategies. Our work helps digital rights researchers who study the ways to achieve a balance between damaging localization of ICT infrastructure due to governments' aggressive policies, on the one hand, and exploitative practices of transnational companies toward communities and countries of the Global South (a process that is often perceived as “digital colonialism”) on the other.⁴⁶

Data Collection and Analysis

We carried out this research project from January to September 2020.

⁴⁶ Abeba Birhane, “The Algorithmic Colonization of Africa,” July 18, 2019, Real Life, <https://bit.ly/342wmSR>

Step 1

The first researcher looked into the privacy policies, terms of services, Frequently Asked Questions (FAQ) pages, blog posts or any other publicly available documents (or multi-media content) published officially by the company without being required to create an account and log in to that service or the company's website up through our data collection end date of May, 2020. Based on those materials, the company was assessed against every indicator — relevant to messaging apps — in the Privacy (P), Freedom of Expression (F) and Governance (G) categories of RDR index. It is important to note that RDR ranks companies based on their *public disclosure* of policies and practices that affect privacy and freedom of expression. It does not test companies' products nor evaluates the veracity of any of those companies' claims.⁴⁷

For every element of each indicator, there were three possible scores:

- ✦ For full disclosure: score = 100
- ✦ For partial disclosure: score = 50
- ✦ For “no disclosure” and “no”: score = 0

“Full disclosure” means the company's disclosure meets the requirements for that element in an indicator; “partial disclosure” means researchers have found information about the element's requirement but the disclosure was not enough to meet the element requirement; “no disclosure” means researchers could not find any publicly available document that meets the element's requirement. “No”

⁴⁷ This is important because sometimes, in practice, a company might meet certain privacy or freedom of expression requirements (e.g. has an internal policy in resisting government's data request, ask security researchers to audit its products, etc.) but it doesn't disclose it. The opposite is true as well: sometimes companies disclose a policy or practice but in practice they don't fully enforce that policy.

means the disclosure exists however what is disclosed does not meet the element's requirement. For further information about each element for a specific company check out the company's [at this link](#).

We calculate the final score of each indicator by adding up the score of each element divided by the total number of elements in that indicator.

Step 2

The second researcher verified the score given to each element by the first researcher.

Step 3

The first and second researchers compared the results to ensure the consistency in their assessments.

Step 4

The third researcher cross-checked each element to ensure that the evaluation is consistent for each company.

Step 5

The team calculated final scores and drafted the report.

Step 6

The report was reviewed by researchers at RDR, along with three other digital rights researchers (a legal scholar, a social media governance scholar, and an Internet security researcher) who are native speakers of the Persian language and knowledgeable about digital rights in Iran.

Step 7

The workbook was developed to further help companies to address their duty to respect human rights.

Total Scores for Privacy and Freedom of Expression Indicators

We assessed all companies' disclosures against privacy and freedom of expression indicators (you can find the full list of indicators and their elements in the Indicators section of the Appendix, on [page 50](#), and on the [Filterwatch website](#))

To summarize and visualize the result in a more understandable manner we divided and merged 'Privacy and Freedom of Expression' indicators into six main categories. The total scores, shown in [\[Fig. 5\]](#), are the average of the following six categories.

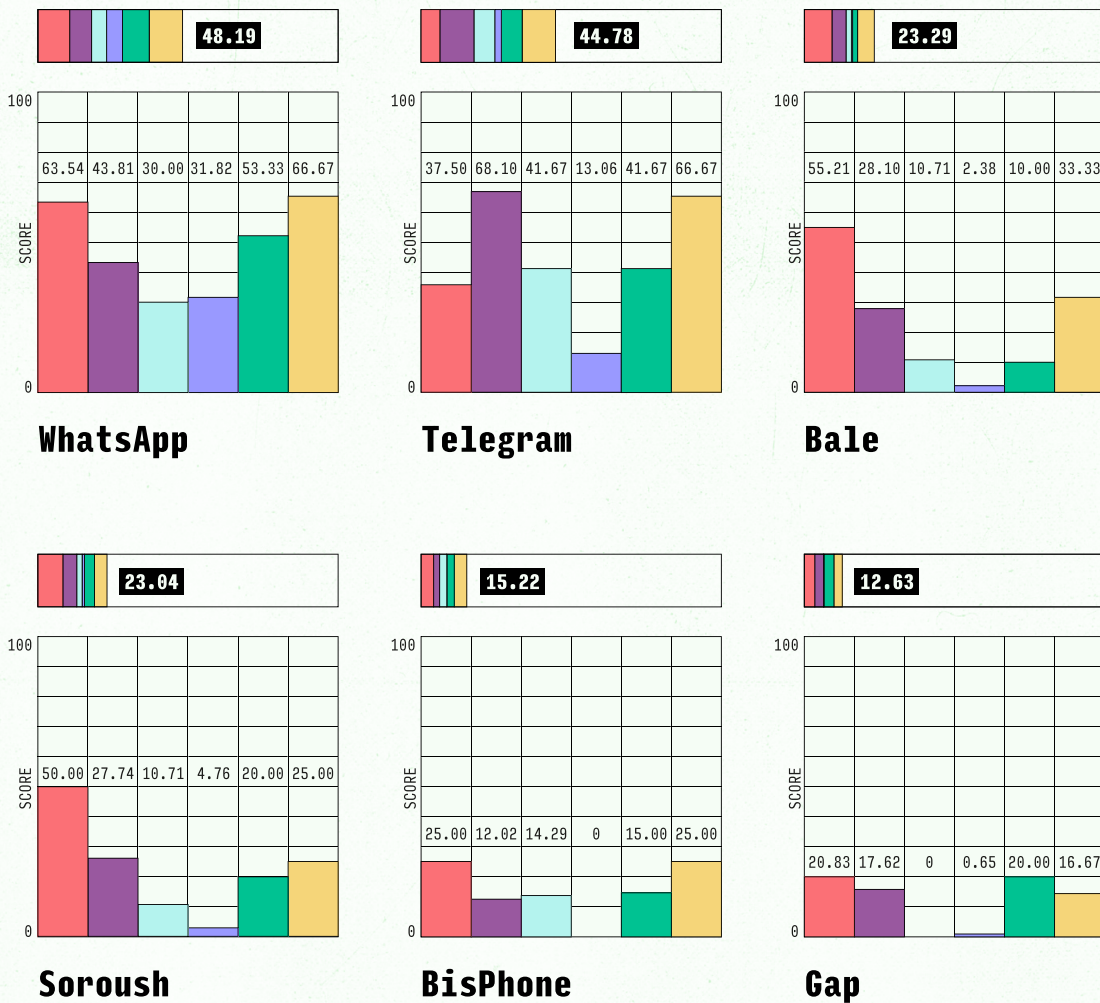
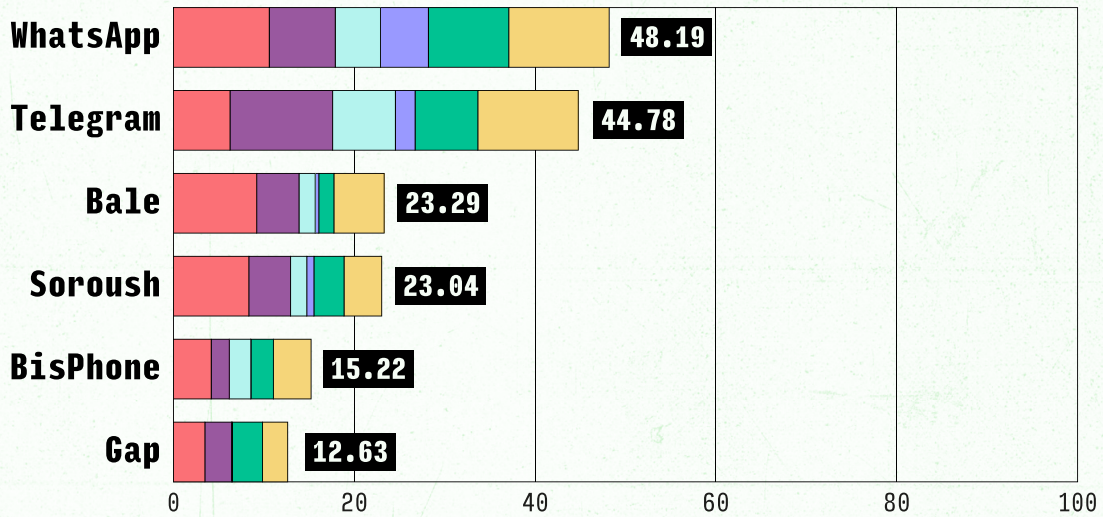
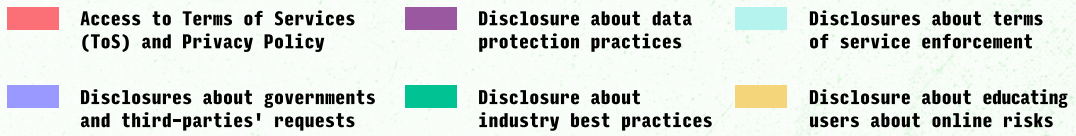
- ✦ All six companies are far from being perfect in their disclosure practices. WhatsApp with 48.19/100 earns first place, and Gap with 12.63/100 receives the lowest score.
- ✦ Among Iranian companies, Bale receives the highest scores in disclosing its policies and practices in relation to respecting users' privacy and freedom of expression. Soroush nearly ties with Bale, followed by BisPhone and Gap, respectively. However, the companies all rank behind the two most popular foreign messaging apps among Iranians, WhatsApp and Telegram, by more than 20 points.
- ✦ All of the assessed Iranian companies receive scores for publishing pieces of information about their privacy policy and terms of service. However, in several cases, among both Iranian and foreign apps, such information was integrated in Frequently

[Fig 4]

Access to Terms of Services (ToS) and Privacy Policy and information about their updates	F1, F2, P1, P2
Disclosures about data collection, data sharing, data retention, and users access and control over their information	P3, P9, P4, P5, P6, P7, P8
Disclosures about the process of enforcing terms of service and the data associated to it	F3, F4
Disclosures about companies' policies and practices in relation to governments and third-party requests to access users' information, demand content takedowns, and restricting accounts	P10, P11, P12, F5, F6, F7, F8
Disclosure about applying industry best practices for securing privacy and users' identity	P13, P14, P15, P16, F11
Companies' efforts in educating users about online risks and ways to keep themselves safe	P17, P18

[Fig 5]

Summary of Findings



Asked Questions (FAQ) pages and other publicly available documents on companies' websites as opposed to a specific page for privacy policies or ToS. Telegram and WhatsApp both receive partial scores for not providing fully translated and understandable ToS and Privacy Policy in Persian. It is important that this information be easily findable and understandable by users before signing up to use a service, a process that is called receiving an "informed consent."

- ✦ Among Iranian companies, all except Gap list categories of content and activities that are not permitted on their platform. However, some definitions are vague or open to interpretation, such as "immoral" (*gheyre-akhlaghī*) or actions against national security (*eghdam alayhe amniate melli*). Bale notes that "the application [Bale] is part of the realm of the rule of law of the Islamic Republic of Iran, and all current laws of the country in the virtual environment must be followed." The application further continues that users can report issues directly to judiciary officials.⁴⁸

- ✦ None of the Iranian companies publish transparency reports to include details about their terms of service enforcement

such as the number of restricted accounts, instances of censored and taken down content, or governmental and other third parties' requests for access to users' information. WhatsApp's parent company, Facebook, publishes transparency reports. However, Facebook's transparency portal doesn't disaggregate data based on the type of service. Telegram has a transparency channel, but this channel has not yet published any data. However, the company publishes data about terrorist accounts suspension in its ISIS-Watch Telegram channel.⁴⁹

- ✦ Gap receives a zero score for its disclosure about enforcing its terms of service; BisPhone also receives no scores in its disclosure about governments and third-party requests to access users' information, demand content and accounts restriction.

In the following charts you can find more information about companies' scores and our findings with respect to certain category of indicators:

⁴⁸ [...] فضای اپلیکیشنهای رسمی بخشی از قلمرو حاکمیت قوانین جمهوری اسلامی ایران است و کلیه قوانین رایج کشور در محیط مجازی نیز لازم الاتباع است و مسئولیت حقوقی یا کیفری ناشی از نقض این قوانین با کاربر متخلف است. اعمال تروریستی، اقدامات علیه امنیتی ملی، اقدامات علیه تمامیت ارضی و استقلال کشور و نیز جاسوسی و سایر موارد که مطابق با مقررات موضوعه داخلی یا بین المللی جرم تلقی شده است و مسئولیت سوء استفاده از این اپلیکیشن در ارتباط با امور مجرمانه به هر شکل با کاربر است. کاربران محترم در خصوص این موارد باید نهایت دقت و جدیت را داشته باشند و البته می‌توانند هر یک از موارد نقض را به مقامات صالح یا ضابطین قضایی اطلاع رسانی نمایند.

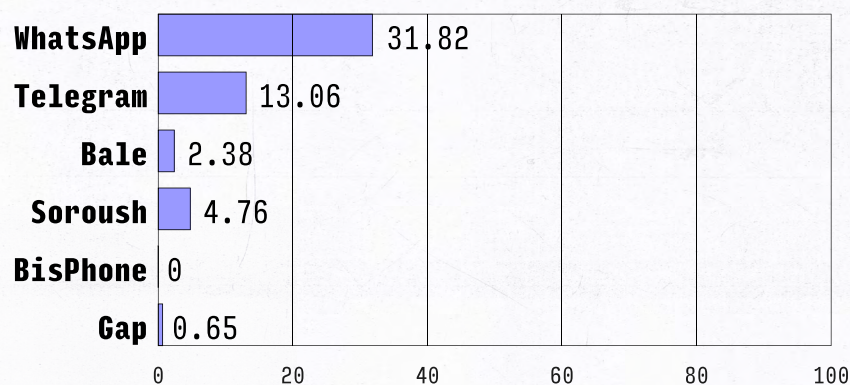
Bale, Terms of Use, <https://bale.ai/terms/>, Accessed in April 2020

⁴⁹ Telegram's ISIS Watch channel, <https://t.me/isiswatch>, Only a preview version of the channel exists for people who don't have a Telegram account. RDR assesses companies based on their public disclosure, without having to log-in or create an account. This affected our accoring about Telegram's transparency in publishing ToS enforcement data.

Government and Third Party Requests

[Fig 6]

Disclosures about governments and third-party requests for user information and account/content restriction



[Fig 7]

The score is the average of following indicators:

P10. Process for responding to third-party requests for user information The company should clearly disclose its process for responding to requests from governments and other third parties for user information.

P11. Data about third-party requests for user information The company should regularly publish data about government and other third-party requests for user information.

P12. User notification about third-party requests for user information The company should notify users to the extent legally possible when their user information has been requested by governments and other third parties.

F5. Process for responding to third-party requests for content or account restriction The company should clearly disclose its process for responding to government requests (including judicial orders) and private requests to remove, filter, or restrict content or accounts.

F6. Data about government requests for content or account restriction The company should regularly publish data about government requests (including judicial orders) to remove, filter, or restrict content or accounts.

F7. Data about private requests for content or account restriction

The company should regularly publish data about private requests to remove, filter, or restrict access to content or accounts.

F8. User notification about content and account restriction The company should clearly disclose that it notifies users when it restricts content or accounts.

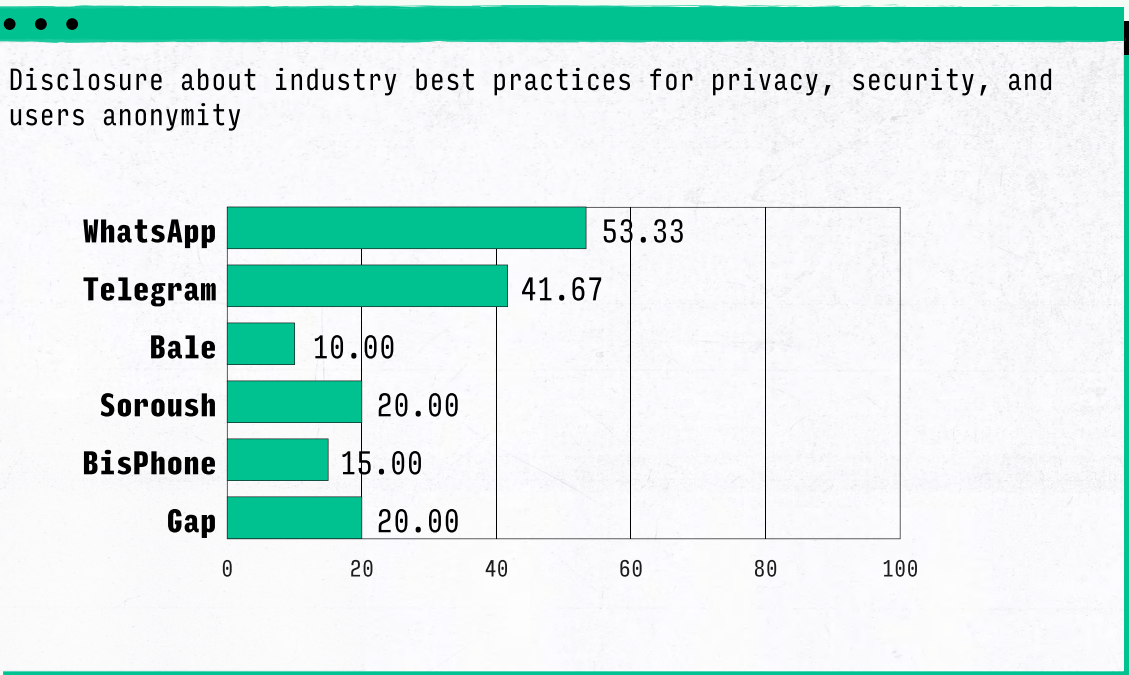
✦ **Iranian and foreign companies received the lowest scores in the ‘Government and Third Party Requests’ category.** Iranian companies are far behind their foreign counterparts in this regard.

✦ Among Iranian companies, Soroush received the highest score because it partially met P12 by disclosing that “under no circumstances will Soroush provide users’ information to any third party company/entity/organization without their permission.” Bale received a partial score for indicator F5, element 5, about the legal basis on which a company may comply with government requests.

✦ In the case of Telegram vs. WhatsApp, note that the WhatsApp score is calculated based on its parent company Facebook’s disclosure and transparency reporting; Facebook’s transparency portal does not disaggregate data based on the type of Facebook services (e.g. WhatsApp, Messenger, etc.)

Disclosure about industry best practices for privacy, security, and protecting users identity

[Fig 8]



[Fig 9]

The score is the average of following indicators:

P13. Security oversight The company should clearly disclose information about its institutional processes to ensure the security of its products and services.

P14. Addressing security vulnerabilities The company should address security vulnerabilities when they are discovered.

P15. Data breaches The company should publicly disclose information about its processes for responding to data breaches.

P16. Encryption of user communication and private content The company should encrypt user communication and private content so users can control who has access to it.

F11. Identity policy The company should not require users to verify their identity with their government-issued identification, or other forms of identification that could be connected to their offline identity.

✦ **None of the six companies disclose information about the ways they handle data breaches**, regardless of whether they notify users or relevant authorities about data breaches or not. In addition, no company discloses information about whether they have systems in place to limit employee access to user information. This is especially significant considering the multiple incidents related to employees snooping on users and, even worse, spying for governments.⁵⁰

✦ **Although they were both far from receiving perfect scores in this category, WhatsApp and Telegram**

disclose information about their end-to-end encryption practices. They provide technical specifications of their encryption protocol, MTPProto's 2.0. End-to-End encryption for Telegram (note that Telegram's source code is not fully open to review yet);⁵¹ the Signal Protocol for WhatsApp.⁵² Also note that WhatsApp's end-to-end encryption is set by default.

✦ **Iranian companies rank behind their foreign counterparts in the industry best practices category.** However, among them, BisPhone is the only company that received a partial score for P16: Encryption of user communication and

⁵⁰ Greg Bensinger Ellen Nakashima, "Former Twitter Employees Charged with Spying for Saudi Arabia by Digging into the Accounts of Kingdom Critics," The Washington Post, November 12, 2019, <https://wapo.st/2T280Y2> and "Facebook Has Fired Multiple Employees for Snooping on Users," Sources: Facebook Has Fired Multiple Employees for Snooping on Users, accessed September 18, 2020, <https://bit.ly/3j24cvx>

⁵¹ Telegram's FAQ, <https://bit.ly/3dVk4Wx>

⁵² End-to-End Encryption, Telegram, <https://bit.ly/3dVk4Wx> and WhatsApp Encryption Overview, WhatsApp, December 19, 2017, <https://bit.ly/2GVPfhV>

private content. BisPhone's disclosure claims that it provides end-to-end encryption, although it is not set by default. We could not find any information about the technical details of BisPhone's encryption on the company's website or GitHub page.⁵³

- ✦ **Bale received the lowest score among its Iranian counterparts in this category (Fig. 8)**; this is alarming considering the company's partnership with the Central Bank of Iran (a state-owned entity) to provide e-payment features and handle sensitive financial information.

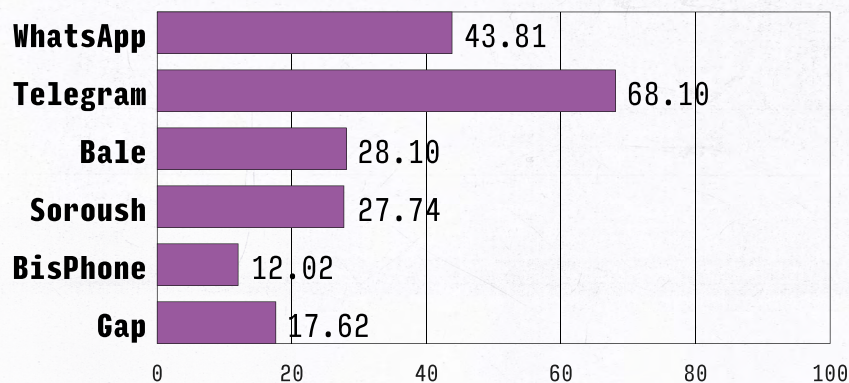
Disclosures about data collection, data sharing, data retention, and users access and control over their information

More details about companies' scores and our findings are as follows:

- ✦ **Telegram received the highest score in this category (Fig. 10).** Among all the assessed companies, Telegram was the most transparent about its data collection practices by emphasizing that it limits data collection to the point that is necessary for its service to work properly. One reason could be that, as opposed to WhatsApp's parent company, Facebook, Telegram's business model doesn't rely on targeted advertising, and the company clearly discloses this. In a paper entitled "It's the Business Model: How Big Tech's Profit

[Fig 10]

Data protection practices including disclosures about data collection, sharing, control, and access



⁵³ BisPhone, <https://bit.ly/31c1EaN> date accessed: June 5, 2020

[Fig 11]

The score is the average of following indicators:

P3. Collection of user information The company should clearly disclose what user information it collects and how

P4. Sharing of user information The company should clearly disclose what user information it shares and with whom.

P5. Purpose for collecting and sharing user information The company should clearly disclose why it collects and shares user information.

P6. Retention of user information The company should clearly disclose how long it retains user information.

P7. Users' control over their own user information The company should clearly disclose to users what options they have to control the company's collection, retention, and use of their user information.

P8. Users' access to their own user information Companies should allow users to obtain all of their user information the company holds.

P9. Collection of user information from third parties The company should clearly disclose its practices with regard to user information it collects from third-party websites or apps through technical means.

Machine is Distorting the Public Sphere and Threatening Democracy,” RDR researchers have shown that relying on targeted advertising creates incentives for companies to apply privacy-invasive methods to collect more and more information about users.⁵⁴ Another reason could be that as a parent company, Facebook offers multiple, often interconnected, services (Instagram, WhatsApp, Facebook Messenger, etc.) and there is not sufficient transparency about data sharing practices between Facebook's own services.

✦ **We couldn't find any information about Iranian companies' targeted advertising practices,**⁵⁵ nor could we find any disclosed information about data sharing practices within messaging apps' parent companies, and among different services offered by a certain parent company.

✦ **On the other hand, Iranian messaging services were relatively transparent about users' ability to delete their data;** all four Iranian companies received scores for disclosing that they delete user information after users terminate their

⁵⁴ “It's the Business Model: How Big Tech's Profit Machine Is Distorting the Public Sphere and Threatening Democracy,” Ranking Digital Rights, August 24, 2020, <https://bit.ly/3jFrg3u>

⁵⁵ Note that Soroush hinted at using cookies to gain information about the patterns of using Soroush in order to provide relevant support/services. It's not clear what those services are and if they are related to targeted advertising: <https://hi.sapp.ir/privacy>

account. **However, none of them disclose information about whether or how they de-identify user information that they retain.** Furthermore, Bale is the only company that discloses that it may share users information with government or legal authorities; the rest don't disclose anything about this aspect.

Disclosure about Governance

The 2019 RDR Index includes six indicators to assess companies' governance and oversight mechanisms with respect to privacy and freedom of expression. This category evaluates companies' commitment to UNGP's principles to respect and protect human rights, and how they implement these commitments across their

operations, including whether they conduct human rights due diligence, engage with civil society groups and other stakeholders, and provide grievance mechanisms to address human rights harms. Issues of particular note included:

- ✦ **All of the Iranian companies received scores of zero in the 'Governance' category.** In part, this is because none of the assessed companies took part in multi-stakeholder initiatives (MSI) that enable collective governance and partnerships between companies, civil society organizations, academic institutions, investors, governments, and other stakeholders. Among the assessed companies, WhatsApp's parent company, Facebook, is the only one that is a member of Global Network Initiative (an MSI that

[Fig 12]

- G1. Policy commitment** The company should publicly commit to respect users' human rights to freedom of expression and privacy.
- G2. Governance and management oversight** The company's senior leadership should exercise oversight over how its policies and practices affect freedom of expression and privacy.
- G3. Internal implementation** The company should have mechanisms in place to implement its commitments to freedom of expression and privacy within the company.
- G4. Impact assessment** The company should conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of its business affect freedom of expression and privacy and to mitigate any risks posed by those impacts.
- G5. Stakeholder engagement** The company should engage with a range of stakeholders on freedom of expression and privacy issues.
- G6. Remedy** The company should have grievance and remedy mechanisms to address users' freedom of expression and privacy concerns.

“help[s] companies respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications.”⁵⁶ We tried to identify Iranian or regional alternatives to such multi-stakeholder initiatives but were unable to find existing examples in Iran.

✦ In regards to the G4 indicator (‘Impact assessment’) it is concerning that all of the Iranian companies received scores of zero; due to the volatile nature of messaging services in terms of their feature set and fluctuating government partnerships, it is essential that human rights impact assessments be conducted regularly before adding new features or signing up for a new partnership.

For an example, one can look at the very recent example of Shad App, an e-learning service built on a domestic messaging app infrastructure, and its registration policy. In April 2020, the Iranian refugee protection NGO HAMI raised concerns about the accessibility of the app by Afghan refugee children, as the app requires national ID

numbers to be entered upon registration, which refugee children often lack.⁵⁷ The app developers and the Ministry of Education resolved the problem; however, such issues show the lack of awareness about the importance of conducting human rights impact assessment, and other Governance indicators such as active engagement with civil society organizations, and the provision of access to remedy.

It is our hope that the assessed companies will use this report and the workbook to start internal conversations about the UNGP, and to meet the Governance indicators in future iterations. Companies can also use other toolkits such as the “Human Rights Baseline Assessment for Small and Medium Sized Technology Companies” to start fulfilling their responsibilities with respect to the Governance indicators.⁵⁸



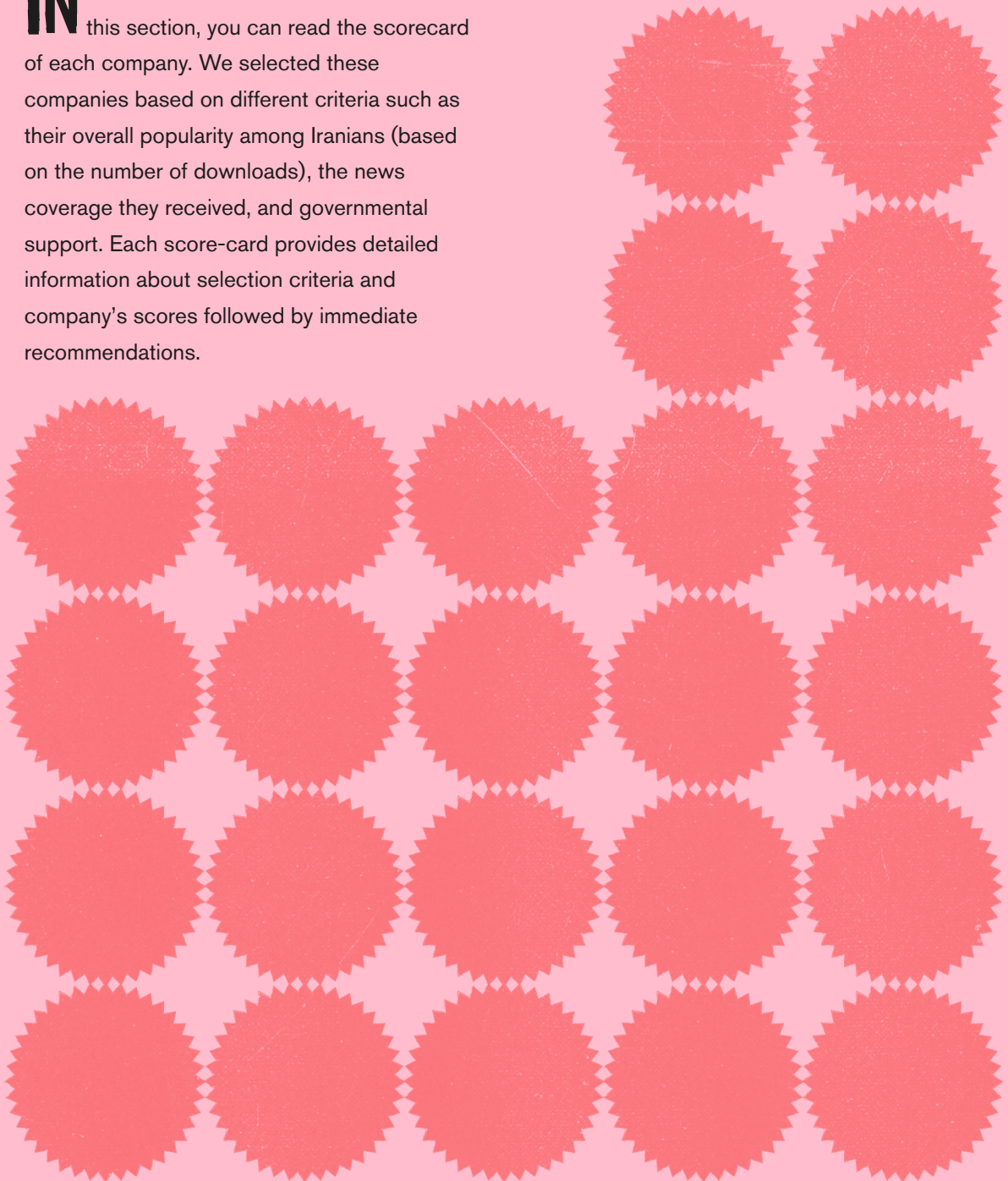
⁵⁶ Global Network Initiative, <https://globalnetworkinitiative.org/>

⁵⁷ Melody Kazemi, “Policy Monitor - April 2020,” Filterwatch, May 14 2020, <https://bit.ly/3dzeQZW>

⁵⁸ “Human Rights Baseline Assessment for Small and Medium Sized Technology Companies”, Global Partners Digital and Open Technology Institute, January 2020, <https://bit.ly/2H84vb2>

COMPANY SCORECARDS

IN this section, you can read the scorecard of each company. We selected these companies based on different criteria such as their overall popularity among Iranians (based on the number of downloads), the news coverage they received, and governmental support. Each score-card provides detailed information about selection criteria and company's scores followed by immediate recommendations.



SOROUSH/SOROUSH PLUS



With 3 million downloads on Cafe Bazaar, Soroush is a relatively widely used domestic messaging platforms in Iran.

In May 2019, the Supreme Council of Cyberspace named Soroush as one of the preferred domestic messaging apps.

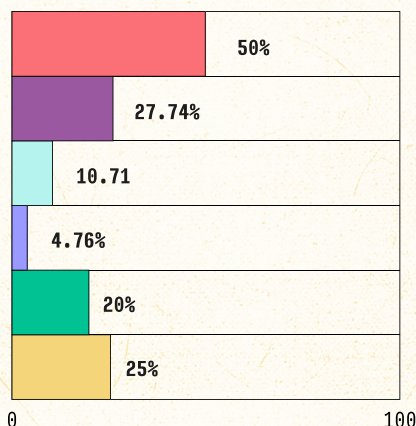
Soroush was owned by the Islamic Republic of Iran Broadcasting or IRIB (the Iranian state-controlled media agency). In April 2020, IRIB decided to sell the company to another public or private entity.

Privacy Policy ↗	✓
Terms of Service ↗	✓
INDUSTRY BEST PRACTICES	
Encryption	No information or technical paper found
Security audits	There is no information about the company's security audit and bug bounty programs
Does the company publish transparency reports?	No

OVERALL SCORES



- Access to Terms of Services and Privacy Policy and their updates
- Disclosures about data collection, data sharing, retention and users' control
- Disclosures about terms of service enforcement:
- Disclosures about governments and third-party requests:
- Disclosure about industry best practices:
- Companies' efforts in educating users about online risks and how to protect themselves:



IMMEDIATE RECOMMENDATIONS

- ▶ It's a good sign that the company has a community standards page with a list of allowed and not-allowed use cases. However, the enforcing mechanisms for applying these community standards are not clear. Soroush should disclose the methods, automated and/or manual, by which it enforces its community standards.
- ▶ Soroush does not disclose any information about the encryption protocol it uses. The company should immediately disclose whether and how it encrypts user data in transit and at storage.
- ▶ The company should publish transparency reports listing the number of both content takedowns and user takedowns disaggregated into categories of requests from third party non-governments, government, and judicial agencies.
- ▶ Soroush should clearly commit to the principle that any partnerships with government agencies will not provide those agencies with any special access to user information.

GAP MESSENGER



Gap Messenger is among the preferred messaging apps introduced by the Supreme Council of Cyberspace.

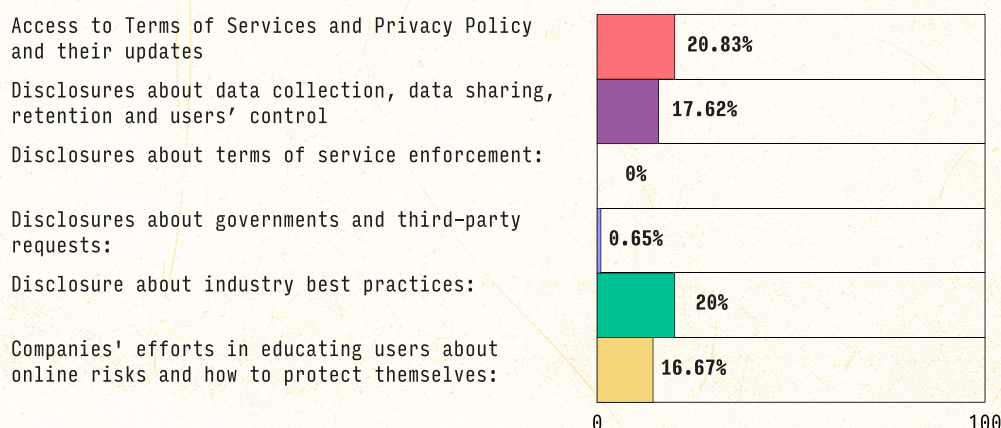
Owned by TS Information Technology Ltd (TSIT).

According to the company's blog, Gap Messenger has a presence in the international market. They have an office in the UK. The app is available as "Vida" for non-Iranian users and as "Gap" for users inside Iran. In the same blogspot, they highlighted their interest in securing partnership with South Africa's telecommunication company, MTN.⁵⁹

In January 2019, Gap announced its business partnership with the Telecommunication Company of Iran for facilitating online bill paying.⁶⁰

Privacy Policy EN FA AR	✓
Terms of Service	✗
INDUSTRY BEST PRACTICES	
Encryption	According to the company's information section on Iranian app stores, the company provides end-to-end encryption. We didn't find any information about the details of encryption algorithms used, nor did we find any technical paper. ⁶¹
Security audits	No information found about bug bounty programs.
Does the company publish transparency reports?	No

OVERALL SCORES



IMMEDIATE RECOMMENDATIONS

- ▶ Gap should add a separate Terms of Service page on its website's homepage.
- ▶ Gap should provide a Persian version of its FAQ page.
- ▶ The company should be transparent about the jurisdiction that it operates within and is legally held accountable to. This includes transparency about data sharing practice between Vida and Gap (and Ring), in addition to data storage practices within or outside Iran's borders.
- ▶ Gap's privacy policy in English is different from those in Persian and Arabic. The company should immediately address this inconsistency.
- ▶ To show its full commitment to users' security Gap should publish the technical details of its encryption protocol and officially post information about its security audits and bug bounty programs on its website.
- ▶ Gap should include terms of service for the use of APIs in its developer center.
- ▶ Gap should clearly commit to the principle that any partnerships with government agencies will not provide those agencies with any special access to user information.

⁵⁹ "Gap Messaging App Agrees to Expand International Services to Countries in the Region," Gap Blog, July 20, 2019, <https://bit.ly/319Jd83>, it is important to note that in August 2020, MTN South Africa decided to divest and leave Iran's market partly due to the sanctions.

⁶⁰ "Agreement Between Gap Messaging App and Telecommunication Company of Iran," Gap Blog, January 15, 2019, <https://bit.ly/2H8xbRn>

⁶¹ Cafe Bazaar, <https://bit.ly/31dyq97>, date accessed: Jun. 5, 2020

BALE

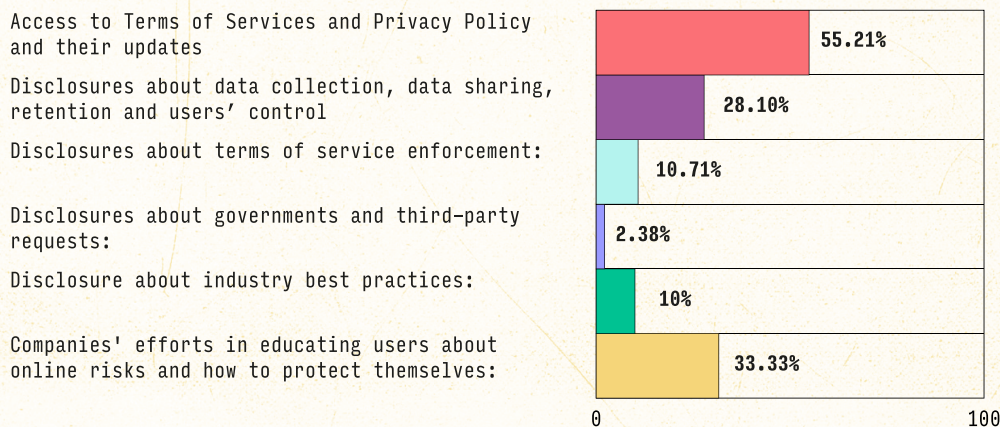


Bale is a combination of a messaging and e-payment app. The application provides social messaging features in addition to several e-banking and e-government features. Bale is supervised by the Central Bank of Iran.⁶²

The Supreme Council of Cyberspace named Bale as one of one of its preferred messaging apps.

Privacy Policy ↗	✓
Terms of Service ↗	✓
INDUSTRY BEST PRACTICES	
Encryption	No information or technical paper found
Security audits	There is no information about the company's security audit and bug bounty programs
Does the company publish transparency reports?	No

OVERALL SCORES



IMMEDIATE RECOMMENDATIONS

- ▶ The company should separate its privacy policy and from its terms of service and host them both on the homepage of its website.
- ▶ The platform should publish regular transparency reports at least once a year. Compared to other Iranian messaging apps that we assessed, Bale is more transparent about the details of terms of service and its privacy practices; however it doesn't publish transparency reports. Thus, publishing a transparency report is the natural next step.
- ▶ The app should be transparent about its governance structure, especially with respect to its partnership with the Central Bank of Iran (with regard to data and information sharing practices and data collection). Bale should clearly disclose that any partnership with the Central Bank of Iran or government agencies will not provide those agencies with any special access to user information.
- ▶ Because of the built-in e-payment features and highly sensitive financial data, Bale should disclose information about security measures it takes to secure data including information about encryption, internal and external security audits, and ways to remediate and inform users about data breaches.

⁶² Sina Zakery, "Analysis of Bale Messaging App; Banking Replacement for Telegram," ITResan, April 16, 2018, <https://bit.ly/344jo7b>

BISPHONE

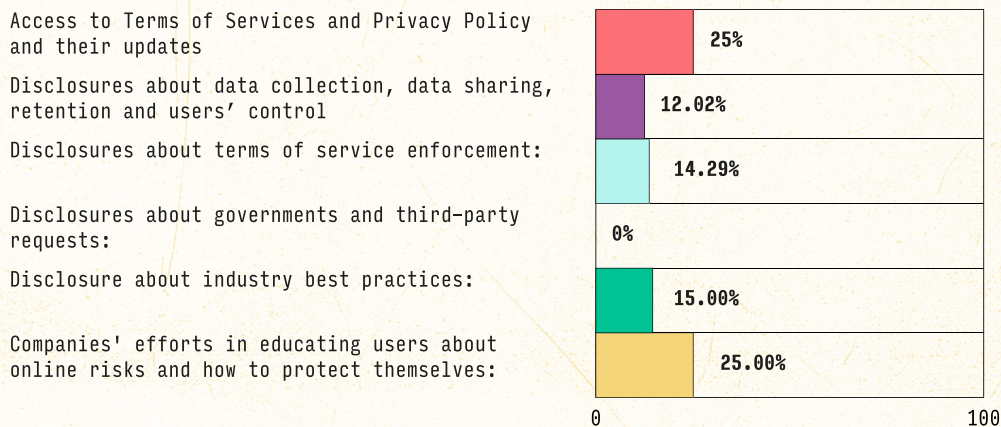


BisPhone is an Iranian messaging app that distinguishes itself from its other counterparts by claiming to provide end-to-end encryption. However, end-to-end encryption is not set by default. We also could not find any technical details about its encryption protocols.

BisPhone is owned by TSTonline co.

Privacy Policy	
Terms of Service	
INDUSTRY BEST PRACTICES	
Encryption	It provides an opt-in end-to-end encryption, we couldn't find a technical paper about details of the encryption algorithm.
Security audits	There is no information about the company's security audit and bug bounty programs
Does the company publish transparency reports?	No

OVERALL SCORES



IMMEDIATE RECOMMENDATIONS

- ▶ BisPhone should publish a privacy policy on the first page of its website.
- ▶ As the first messaging app in Iran that has promised to provide end-to-end encryption, the company should publish its technical paper disclosing the encryption algorithms they use.
- ▶ Encryption should be set by default rather than leaving it to users to opt in.
- ▶ BisPhone should clearly disclose that any partnerships and receiving direct or indirect financial support (such as free access to NIN data centers) from Iranian government agencies will not provide those agencies with any special access to user information.⁶³

⁶³ Massoumeh Bakhshipour, "Free Services for Domestic Messaging Apps from National Information Network's Primary Data Centre," August 29, 2020, Mehr News, <https://bit.ly/3duHdZ8>

Other Messaging Apps

Despite Iranian leaders' effort to support domestic messaging services, they are still not as popular as their non-Iranian counterparts. Telegram — with approximately 40 million users— and WhatsApp — with approximately 33 million users — are among the most popular apps among Iranians.⁶⁴ In addition, domestic messaging apps often compare themselves, in terms of an app's design features, reliability, and security, to their non-Iranian counterparts. Therefore, we decided to include WhatsApp and Telegram in our assessment. It is important to note that due to different factors, such as the jurisdiction a company conducts business under and language, those apps cannot be compared with the Iranian apps in a similar manner. However, because millions of Iranians use them, they too have responsibilities to respect their Iranian users' digital rights.

⁶⁴ "How Many Iranian Telegram and Domestic Messaging App Users are There," IRNA , May 22, 2019, <https://bit.ly/2T2jRk9> and WhatsApp Search on Cafe Bazaar, Cafe Bazaar, accessed Jul. 5, 2020 <https://bit.ly/35Mfpcf>

WHATSAPP ⁶⁵



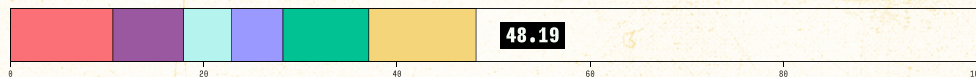
WhatsApp, a messaging and VoIP service, has 33 million downloads on Cafe Bazaar, an Iranian marketplace for Android apps.

The US-based company is owned by Facebook, Inc.

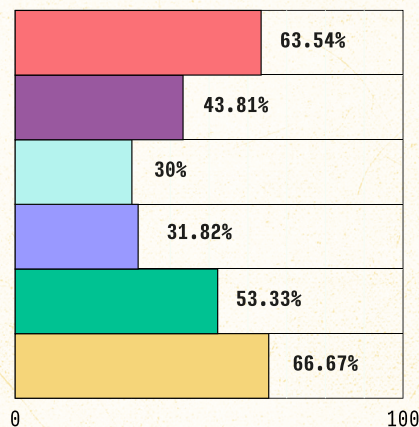
Privacy Policy ↗	✓
Terms of Service ↗	✓
INDUSTRY BEST PRACTICES	
Encryption	WhatsApp is end-to-end encrypted by default
Security audits	WhatsApp has bug bounty programs. However, the source code is not open for reviews.
Does the company publish transparency reports?	
↗ Facebook, as a parent company of WhatsApp publishes transparency reports but the reports are not divided by each service.	

[↗](#) The company has a legal page in Persian however not everything about the privacy policy and terms of service is translated into the Persian language.

OVERALL SCORES



- Access to Terms of Services and Privacy Policy and their updates
- Disclosures about data collection, data sharing, retention and users' control
- Disclosures about terms of service enforcement:
- Disclosures about governments and third-party requests:
- Disclosure about industry best practices:
- Companies' efforts in educating users about online risks and how to protect themselves:



IMMEDIATE RECOMMENDATIONS (PARTICULAR FOR IRANIAN USERS)

- ▶ WhatsApp should provide full and understandable versions of its privacy policy and terms of service pages in Persian. It is a good sign that فارسی (Persian) is one of the supported languages. However, the current information in Persian is limited to basic information about privacy, the app's features, and a general FAQ.
- ▶ E2EE nature of WhatsApp doesn't immune the service from malicious uses such as deploying (spear)-phishing tactics to spy on human rights activists and journalists.⁶⁶
- ▶ WhatsApp should disclose more about its prevention and remediation process in the case of such malicious incidents targeting users. In addition, it should provide more practical material in Persian to educate users – with various levels of digital literacy – about such risks.
- ▶ WhatsApp should disclose more information about its country/regional-based stakeholder initiatives and how it ensures that such engagements are inclusive and effective.
- ▶ Facebook (WhatsApp's parent company) should disclose information about the ways it handles Iranian government and third-party requests that involve information from/about Iranian users. According to the company's Transparency Portal, the Iranian government has been requesting information about users but there is no clarity about the platform/s they requested data from and the nature of those requests.⁶⁷

TELEGRAM



Despite being blocked since 2018, with around 40 million users, Telegram is still one of the most popular apps in Iran. By providing various APIs such as bot APIs, TDLib, and Telegram API, Telegram gives this option to Iranian developers to build various bots and even their own customized Telegram clients such as Telegram Talayi, Talagram, HotGram.

Telegram is registered by Telegram FZ LLC in the UK and the team is currently based in Dubai, UAE.⁶⁹

Privacy Policy ↗	✓
Terms of Service ↗	✓
INDUSTRY BEST PRACTICES	
Encryption	Telegram channels and groups are not end-to-end encrypted. However users can choose "Secret Chats" if they want to have end-to-end encrypted communication.
Security audits	Telegram does not provide bug bounty programs. However source codes and technical documents are available. The company also provides prizes for researchers who can find any security vulnerabilities in Telegram. ⁷⁰
Does the company publish transparency reports?	<p>✗ It has a transparency channel but there is no data in that channel.</p>

✗ Telegram's FAQ, which has more information about privacy and terms of service than its actual privacy policy and terms of service pages, is available in Persian.

OVERALL SCORES



Access to Terms of Services and Privacy Policy and their updates

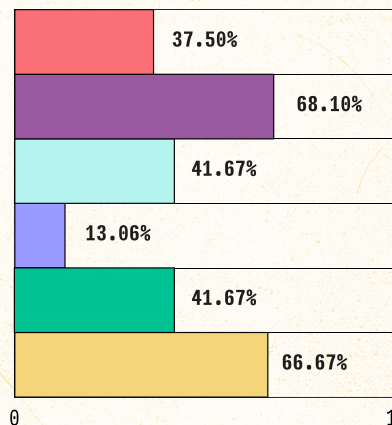
Disclosures about data collection, data sharing, retention and users' control

Disclosures about terms of service enforcement:

Disclosures about governments and third-party requests:

Disclosure about industry best practices:

Companies' efforts in educating users about online risks and how to protect themselves:



IMMEDIATE RECOMMENDATIONS

(PARTICULAR FOR IRANIAN USERS)

- ▶ Telegram's privacy policy and terms of service should be available on its homepage.
- ▶ At the time of writing this report, Telegram's Persian UI was in its beta version. Except for the basic FAQ page, the other documents such as advanced FAQ, privacy policy and terms of service are not available in Persian. The company should provide Persian versions of those documents.
- ▶ Telegram should add information about content and account takedowns/restrictions, third party requests, appeal requests in its transparency portal on its website so everyone can access it without having to create an account on Telegram.⁷¹ The company has a transparency channel but there is no data published in it. There is also another channel called ISIS-Watch that discloses the number of terrorist account suspensions. However, there is no information about other types of account and content restrictions.
- ▶ In its APIs page, Telegram should add terms of service to define its policies and practices regarding misuses of its APIs and its bots policies (check RDR's 2020 pilot study for bots policy).

General Recommendations

We divided our recommendations into two categories: recommendations for Iranian technology companies and recommendations for the Iranian government.

Recommendations for companies

Despite the fact that we only assessed a few messaging apps, the following recommendations are applicable to most companies whose main activity is to develop web-based and mobile apps and services:

Clarity in privacy policy

- ✦ Privacy policies should be written in simple, non-lawyerly language. They should be available on companies' websites and on app stores.
- ✦ Whenever companies update their privacy policies, they should notify users about the updates and keep the history of changes on their website.

- ✦ Companies should disclose the category of data they collect, why they are collected, the way they are stored, and for how long they are kept.
- ✦ In their data and privacy policies, companies should be transparent about their data sharing practices with third-party advertising companies and data brokers; use of cookies; and their API policies.

Clarity in terms of service and its enforcement

- ✦ By developing clear terms of services and community standards, companies should disclose types of content and activities that are allowed and not allowed on their services.
- ✦ Companies should clearly disclose how they enforce their terms of service and community standards. They should disclose what manual and/or automated techniques they use to govern activities (and content) and what actions they take if that activity violates their terms of services. In the case of messaging services, depending on a service's functionality, they should clearly disclose the differences of their terms of services for public and private features, such as one-on-one chats, groups, and

⁶⁵ WhatsApp scores are from RDR's 2019 assessment. We used the assessment to ensure our scoring is consistent with the RDR's internal scoring system. You can find it on <https://bit.ly/3j62Kby>

⁶⁶ Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab Research Report No. 113, University of Toronto, Sep. 2018, <https://bit.ly/34Af3Jk>

⁶⁷ Facebook Transparency page for Iran, accessed on Jul. 5, 2020, <https://transparency.facebook.com/government-data-requests/country/IR>

channels and the ways they enforce their ToS for each category.

- ✦ Due to the violation of terms of service or community standards, If they decide to flag or take down users content or limit users access to company's services, they should notify users and clearly disclose why they decided to take that action.
- ✦ Companies should disclose their APIs' and bots' terms of service clearly for developers and provide information about safeguards they put in place to avoid misuses.

Transparency reporting

- ✦ Companies have to add a transparency portal to their website. At minimum, companies should follow the **Santa Clara Principles on Transparency and Accountability**.
- ✦ In the transparency portal, they have to publish their periodic (six-monthly or yearly) transparency reports and be transparent about their enforcement mechanisms by disclosing:
 - The number of posts and accounts they took down and whether they did so automatically or manually.

- How many requests they received from government and judicial authorities to take actions on users' accounts or content. How many of those requests have been accepted and how many have been rejected.
- How many requests they received from non-governmental bodies (third-parties including other companies, other users, etc.) to take actions on users' accounts or connect. How many of those requests have been accepted and how many have been rejected.
- Categories of content and account takedowns based on the type of violations of terms of services and community standards (for example: child sexual abuse material, copy right violation, pornography, etc.)
- Add a new portal for government and judicial bodies who request users' information. In that portal, companies should disclose their step-by-step process for receiving requests from those bodies and how they process it. They should include hypothetical examples of legitimate vs. non-legitimate requests.

68 See the search for Telegram on Cafe Bazaar, accessed July 5, 2020, <https://bit.ly/37ctuVF> and Telegram APIs, Telegram, accessed Jul. 5, 2020, <https://core.telegram.org/>

69 Telegram FAQ, Telegram, accessed on Jul. 8, 2020, <https://bit.ly/3nWof29>

70 "\$300,000 for Cracking Telegram Encryption," Telegram, Nov. 4, 2014, <https://bit.ly/31aU8KU>

71 Pavel Durov, "Telegram and the Freedom of Speech," October 29, 2017, <https://bit.ly/2IyUpAF>

Privacy and security by design

- ✦ Companies should implement internationally-recognised and robust encryption algorithms to protect users' information in transit and as well as where it is stored. Strong encryptions should be set by default. Where applicable, including for messaging apps and VoIP services, end-to-end encryption should be in place. Technical papers that describe the encryption algorithms should be publicly available on the company's official online pages.
- ✦ For services which involve the creation of user accounts, companies should require users to make strong passwords. If the company handles sensitive information such as a user's name, phone number, address, etc. it should provide multi-factor authentication options.
- ✦ Companies should minimize their collection of user data only to the level that is required for a given service to operate. Where collecting and processing of users' sensitive information is required for maintaining a service, companies should apply de-identification techniques, such as pseudonymization, anonymization, etc. to protect users' privacy.
- ✦ UX/UI designers should apply human rights-centric design principles when designing an app's interfaces. They should make access to privacy and security settings simple enough so people with different levels of digital literacy and differently-abled people can fully understand and use them.

- ✦ Companies should have an internal cybersecurity team – which could include practices such as red and blue teaming or threat modeling – to conduct security testing before releasing their products. In addition, companies should be open to receiving reports from outside cybersecurity and privacy researchers who find vulnerabilities and security bugs in their software, a practice commonly known as bug bounty programs. In addition, in designing and developing their software, companies should use best security practices including avoiding the use of unsafe functions and libraries. For further instructions on applying best privacy and security practices in design and development of your services, check out resources such [the Digital Standards](#) and [OWASP Security Testing Guide](#) (see the appendix).

Information about a company's privacy and security by design practices should be publicly available — as white papers, technical specifications, code pieces — on the company's website such as official blog pages, multi-media channels, software hosting platforms such as GitHub, developers pages, and FAQ pages.

Appeal process and feedback channels

- ✦ Companies should provide a simple and easy to understand appeal process. A user whose content is taken down or account is banned must have a channel to question a company's decisions and appeal the process.

- ✦ Companies should provide functioning email addresses, customer service phone lines, social media channels, online forms, questionnaires to create communication and feedback channels between themselves, users, and other stakeholders.

Transparency in company's governance structure

- ✦ Companies should have an 'About' page on their website. In this page, companies should be transparent about who owns the company and if it is owned by a parent company, what the name of that parent company is, whether the company is state-owned, partially state-owned or is a fully privately-owned company.
- ✦ Companies should inform the public about any data breach or security incidents by publishing a public statement and sending emails to their users. In addition, companies should include this information in the periodic transparency reports.
- ✦ Companies should use the UNGPs to conduct human rights due diligence. They have to publicly disclose that they respect human rights and that they conduct human rights impact assessment regularly by engaging in multi-stakeholder initiatives and civil society organizations who work with vulnerable communities including children, ethnic, gender and sexual, religious minorities, and refugees. Use the workbook attached to this report to start the conversation internally ([link to the workbook](#)).

- ✦ To ensure that companies employees are familiar with digital rights issues, the company should organize internal training and workshops for its employees (from high level executives to technologists, legal, human resource, sales and marketing teams) to understand how each team can prevent and mitigate potential human rights harms in their day to day practices.

- ✦ Companies should engage with government policy-making processes, raise their concerns and stand up for users' digital rights. Some of these strategies include creating cross-company collaboration and standards, sending out open letters to authorities, engaging with press, etc.

Recommendations for the Iranian government

- ✦ The Iranian government should stop its unchecked and mandatory digital localization plans that massively compromise net neutrality principles. These plans, which are mainly carried out by blocking access to international services, either through filtering or preferential tariffs for domestic services, have been undermining users' freedom of choice and freedom of access to information, with a disproportionate negative impact on vulnerable groups and Iranians of lower socio-economic status. Adding e-government features into private messaging services, providing short-sighted economic incentives for using local internet services vs international ones, or

providing free state-backed services for technology start-ups such as data centers should not be simply publicized as the government's well-meaning plans for "supporting" domestic start-ups. In the absence of oversight mechanisms, these ambiguous partnerships jeopardize users' trust in those companies, result in the over-regulation of these companies, the creation of a culture of favoritism and unfair competition among private technology companies in Iran, and their alienation from the international market.

- ✦ The Iranian government should implement a robust and comprehensive data protection legal framework in line with internationally recognised human rights standards. They should set requirements for companies on their privacy and security practices. Until having a comprehensive rights-respecting data protection legal framework, they should halt the progress of the "Managing Social Messaging Apps" bill which restricts Iranians' online freedoms and gives the Armed Forces control over internet gateways.

A few words for civil society groups and technology researchers

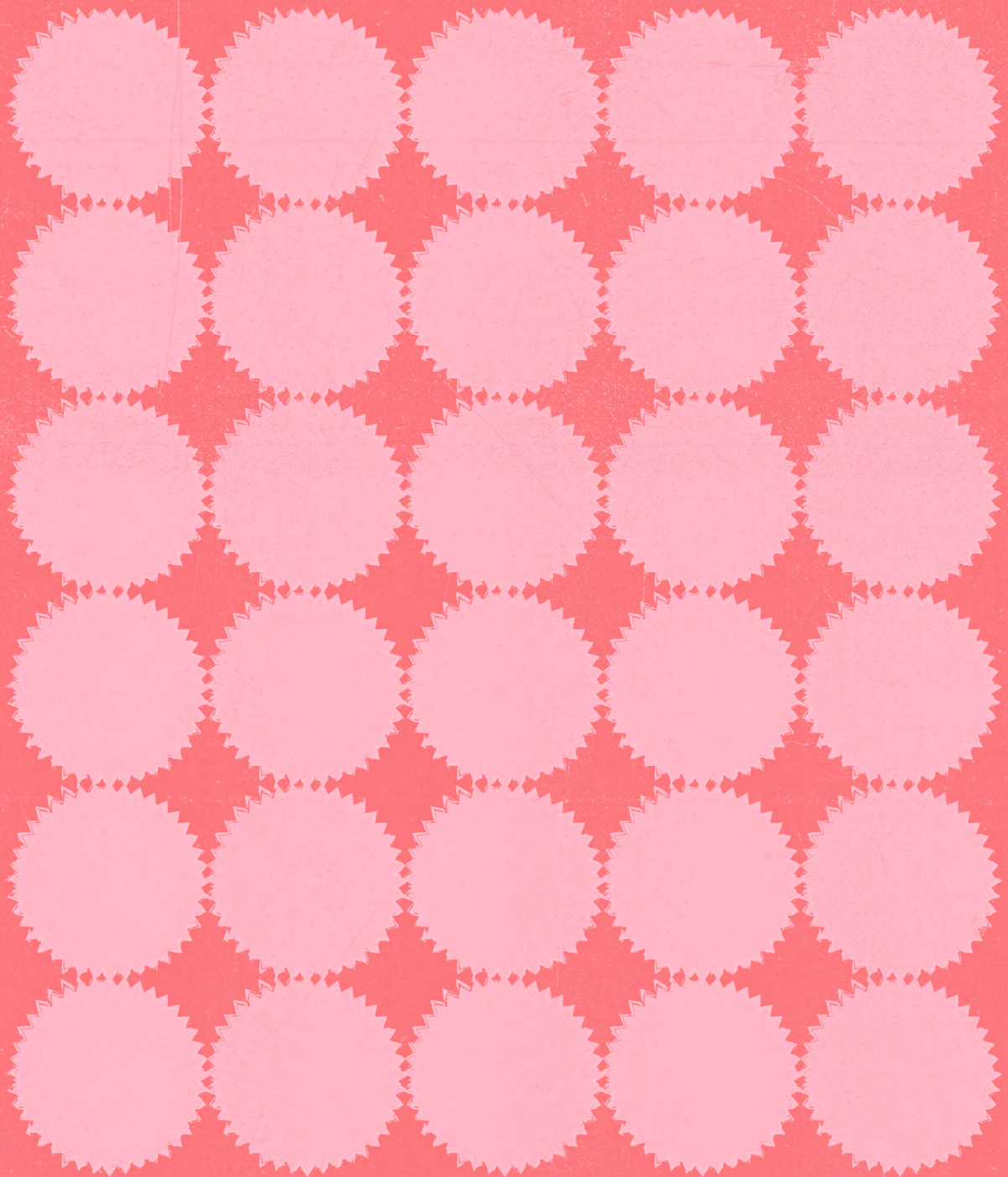
It should be emphasised again that this report highlights the harms posed to the digital rights of internet users inside Iran by a lack of transparency, or inappropriate policies set by technology companies.

The report does not aim to assess the veracity of any of these companies' claims, or the human rights implications of any other aspects of these companies' practices, including their technical infrastructure, their practices outside of the remit of this report, or their influence on the formation of digital policies in Iran.

There remains, therefore, a need for civil society to provide further analysis about these aspects of technology companies' practices, and to hold them accountable where they threaten the fundamental rights of their users.



METHODOLOGY APPENDIX



Challenges and Lessons Learned

- ✦ The Ranking Digital Rights Index methodology applies to telecommunications and multi-service mobile and internet service companies. We started our research by examining Iranian telecommunications companies. However, early on, we noticed that most of these companies don't even have basic privacy policies or terms of services on their websites. In addition, most telecom companies are directly or indirectly owned by state actors and thus cannot be counted under a standard definition of "private sector."
- ✦ The RDR Index methodology includes a system for companies to provide feedback on preliminary results before publication;⁷² however not all companies provide feedback and companies are evaluated whether or not they choose to interact with RDR. For various reasons, we were not able to engage in this practice with Iranian technology companies during the course of our research, primarily due to concerns for the potential safety of the study's authors as well as that of participants. In the next iteration, we hope to provide a survey for companies to be able to share feedback in an anonymous manner. We also hope to engage with other RDR researchers to assess possible ways to incorporate this practice in future iteration of the report.
- ✦ None of the Iranian companies in this report satisfy any of the Governance indicators. This affected our decision about how to visually communicate the comparative scores. We decided not to give a combined score (privacy score + freedom of expression score + governance score) to each company, and instead visualized scores via six categories of indicators assessed in the report.
- ✦ In closed and semi-closed political systems, often there is not enough transparency, or clear boundaries between states' involvement in financial and managerial decisions of private tech companies. This lack of clarity — especially in data sharing practices — has severe impacts on users' human rights. Therefore, adding simple indicators related to companies' ownership such as the existence of "About" pages, annual meetings, financial reports, board members' roles, functioning email addresses and social media channels is

72 "2019 Research Process", Ranking Digital Rights, 2019, <https://bit.ly/3nQUBeK>

helpful in furthering transparency and accountability. In addition, in future iterations of tech accountability reports, we aim to assess and propose possible options for Iranian companies to engage with civil society organizations and other stakeholders in a safe and productive manner if joining regional and international MSIs is not viable for various political and financial reasons.

✦ It is important to acknowledge that authoritarian states have excessive power in controlling, over-regulating, and punishing private companies. From a practical standpoint, it is very idealistic to expect companies to fully resist and not comply with governments' illegitimate requests that undermine digital rights. Therefore, in these countries, proactive measures such as applying privacy by design principles, security by default, human-rights centric UX/UI design, and digital literacy play a crucial role in protecting users. This is the reason we added a section about human rights by design in our recommendations.

✦ During our research, we noticed that companies' developers policies and terms of use (including uses of Application Programming Interfaces (API), which enable the creation of bots, make digital services interoperable, and help create forked versions of a certain service) have unlocked new forms of potential misuse. It is important to note that RDR's 2020 pilot methodology includes indicators about "bot policy" that partially cover our concerns around the use of APIs.

Data sharing and data collection practices between third-party developers and companies through the use of APIs have made our assessment challenging. Information about developers policies and terms of use can be examined in detail by adding "research guidance" to third-party data collection and data sharing indicators such as P3, P4, P9. It is also worth exploring how companies respond to misuse of APIs by going beyond companies' "bot" policies (indicator F13, RDR 2020 pilot study) and assessing disclosures about providing secure APIs. Likewise, there is a need for more transparency about companies' enforcement of developers' terms of use, especially in response to malicious uses of source codes, creating privacy-invasive forked-versions of the service, etc. We anticipate that in the future, due to the demand for the further interoperability of digital services, we will hear more about the digital rights implications of the relationships between third-party developers and companies.

✦ There are unique human rights concerns that relate to messaging apps. Some of these concerns include: online harassment, the virality of dis- and misinformative content, doxxing, and more. To assess companies' responses to these concerns we may need unique indicators. However, we decided not to add those specific indicators because one of the main goals of this report is to be used by other tech companies that provide a wide range of digital services including online publishing platforms, search engines, email services, e-commerce, social networks, etc. In

addition, despite numerous concerns with the use of machine learning solutions for automated content moderation, personalizations, etc. we decided not to focus on those issues in this iteration. We may investigate these issues in future iterations. For more information about indicators related to targeted advertising and algorithmic systems check out RDR's 2020 pilot study and new indicators that will be a basis for the RDR Corporate Accountability Index 2021 report.⁷³

Indicators

We adapted the 2019 RDR Corporate Accountability Index indicators. Several indicators were not applicable to messaging services (F9, F10). Elements F6.3, F7.3, F3.4, and F3.5 do not apply to WhatsApp because the company does not have access to the content of the messages. P7.3 does not apply to Telegram because the company does not use targeted advertising. For P1.2 and F1.2 we scored all companies based on availability of privacy policy and terms of service in the Persian language.



⁷³ "RDR pilot study underscores the need for rights-based standards in targeted advertising and algorithmic systems," Ranking Digital Rights, March 16, 2020, <https://bit.ly/34671aZ>

Freedom of Expression Indicators

F1. Access to terms of service

- F1.1 Are the company's terms of service easy to find?
- F1.2 Are the terms of service available in the language(s) most commonly spoken by the company's users?
- F1.3 Are the terms of service presented in an understandable manner?

F2. Changes to terms of service

- F2.1 Does the company clearly disclose that it notifies users about changes to its terms of service?
- F2.2 Does the company clearly disclose how it will directly notify users of changes?
- F2.3 Does the company clearly disclose the timeframe within which it provides notification prior to changes coming into effect?
- F2.4 Does the company maintain a public archive or change log?

F3. Process for terms of service enforcement

- F3.1 Does the company clearly disclose what types of content or activities it does not permit?
- F3.2 Does the company clearly disclose why it may restrict a user's account?
- F3.3 Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?
- F3.4 Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?
- F3.5 Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?
- F3.6 Does the company clearly disclose its process for enforcing its rules?
- F3.7 Does the company provide clear examples to help the user understand what the rules are and how they are enforced?

F4. Data about terms of service enforcement

- F4.1 Does the company clearly disclose data about the volume and nature of content and accounts restricted for violating the company's rules?
- F4.2 Does the company publish this data at least once a year?
- F4.3 Can the data published by the company be exported as a structured data file?

F5. Process for responding to third-party requests for content or account restriction

- F 5.1 Does the company clearly disclose its process for responding to non-judicial government requests?
- F 5.2 Does the company clearly disclose its process for responding to court orders?
- F 5.3 Does the company clearly disclose its process for responding to government requests from foreign jurisdictions?
- F 5.4 Does the company clearly disclose its process for responding to private requests?
- F 5.5 Do the company's explanations clearly disclose the legal basis under which it may comply with government requests?
- F 5.6 Do the company's explanations clearly disclose the basis under which it may comply with private requests?
- F 5.7 Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond?
- F 5.8 Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?
- F 5.9 Does the company commit to push back on inappropriate or overbroad requests made by governments?

F 5.10 Does the company commit to push back on inappropriate or overbroad private requests?

F 5.11 Does the company provide clear guidance or examples of implementation of its process of responding to government requests?

F 5.12 Does the company provide clear guidance or examples of implementation of its process of responding to private requests?

F6. Data about government requests for content or account restriction

F6.1 Does the company break out the number of requests it receives by country?

F6.2 Does the company list the number of accounts affected?

F6.3 Does the company list the number of pieces of content or URLs affected?

F6.4 Does the company list the types of subject matter associated with the requests it receives?

F6.5 Does the company list the number of requests that come from different legal authorities?

F6.6 Does the company list the number of requests it knowingly receives from government officials to restrict content or accounts through unofficial processes?

F6.7 Does the company list the number of requests with which it complied?

F6.8 Does the company publish the original requests or disclose that it provides copies to a public third-party archive?

F6.9 Does the company report this data at least once a year?

F6.10 Can the data be exported as a structured data file?

F7. Data about private requests for content or account restriction

F7.1 Does the company break out the number of requests it receives by country?

F7.2 Does the company list the number of accounts affected?

F7.3 Does the company list the number of pieces of content or URLs affected?

F7.4 Does the company list the reasons for removal associated with the requests it receives?

F7.5 Does the company describe the types of parties from which it receives requests?

F7.6 Does the company list the number of requests it complied with?

F7.7 Does the company publish the original requests or disclose that it provides copies to a public third-party archive?

F7.8 Does the company report this data at least once a year?

F7.9 Can the data be exported as a structured data file?

F7.10 Does the company clearly disclose that its reporting covers all types of private requests that it receives?

F8. User notification about content and account restriction. The company should clearly disclose that it notifies users when it restricts content or accounts.

F8.1 If the company hosts user-generated content, does the company clearly disclose that it notifies users who generated the content when it is restricted?

F8.2 Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?

F8.3 In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)?

F8.4 Does the company clearly disclose that it notifies users when it restricts their account?

F11. Identity policy. The company should not require users to verify their identity with their government-issued identification, or other forms of identification that could be connected to their offline identity.

F11.1 Does the company require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity?

Privacy Indicators

P1. Access to privacy policies The company should offer privacy policies that are easy to find and easy to understand.

- P1.1 Are the company's privacy policies easy to find?
- P1.2 Are the privacy policies available in the language(s) most commonly spoken by the company's users?
- P1.3 Are the policies presented in an understandable manner?

P2. Changes to privacy policies The company should clearly disclose that it provides notice and documentation to users when it changes its privacy policies.

- P2.1 Does the company clearly disclose that it notifies users about changes to its privacy policies?
- P2.2 Does the company clearly disclose how it will directly notify users of changes?
- P2.3 Does the company clearly disclose the time frame within which it provides notification prior to changes coming into effect?
- P2.4 Does the company maintain a public archive or change log?

P3. Collection of user information The company should clearly disclose what user information it collects and how.

- P3.1 Does the company clearly disclose what types of user information it collects?
- P3.2 For each type of user information the company collects, does the company clearly disclose how it collects that user information?
- P3.3 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?

P4. Sharing of user information The company should clearly disclose what user information it shares and with whom.

- P4.1 For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
- P4.2 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?
- P4.3 Does the company clearly disclose that it may share user information with government(s) or legal authorities?
- P4.4 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 and sharing user information The company should clearly disclose why it collects and shares user information.

- P5.1 For each type of user information the company collects, does the company clearly disclose its purpose for collection?
- P5.2 Does the company clearly disclose whether it combines user information from various company services and if so, why?
- P5.3 For each type of user information the company shares, does the company clearly disclose its purpose for sharing?
- P5.4 Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected?

P6. Retention of user information The company should clearly disclose how long it retains user information.

- P6.1 For each type of user information the company collects, does the company clearly disclose how long it retains that user information?
- P6.2 Does the company clearly disclose what de-identified user information it retains?
- P6.3 Does the company clearly disclose the process for de-identifying user information?

P6.4 Does the company clearly disclose that it deletes all user information after users terminate their account?

P6.5 Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?

P7. Users' control over their own user information The company should clearly disclose to users what options they have to control the company's collection, retention, and use of their user information.

P7.1 For each type of user information the company collects, does the company clearly disclose whether users can control the company's collection of this user information?

P7.2 For each type of user information the company collects, does the company clearly disclose whether users can delete this user information?

P7.3 Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?

P7.4 Does the company clearly disclose that targeted advertising is off by default?

P8. Users' access to their own user information. Companies should allow users to obtain all of their user information the company holds.

P8.1 Does the company clearly disclose that users can obtain a copy of their user information?

P8.2 Does the company clearly disclose what user information users can obtain?

P8.3 Does the company clearly disclose that users can obtain their user information in a structured data format?

P8.4 Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?

P9. Collection of user information from third parties (Internet companies) The company should clearly disclose its practices with regard to user information it collects from third-party websites or apps through technical means.

P9.1 Does the company clearly disclose what user information it collects from third-party websites through technical means?

P9.2 Does the company clearly explain how it collects user information from third parties through technical means?

P9.3 Does the company clearly disclose its purpose for collecting user information from third parties through technical means?

P9.4 Does the company clearly disclose how long it retains the user information it collects from third parties through technical means?

P9.5 Does the company clearly disclose that it respects user-generated signals to opt-out of data collection?

P10. Process for responding to third-party requests for user information The company should clearly disclose its process for responding to requests from governments and other third parties for user information.

P10.1 Does the company clearly disclose its process for responding to non-judicial government requests?

P10.2 Does the company clearly disclose its process for responding to court orders?

P10.3 Does the company clearly disclose its process for responding to government requests from foreign jurisdictions?

P10.4 Does the company clearly disclose its process for responding to requests made by private parties?

P10.5 Do the company's explanations clearly disclose the legal basis under which it may comply with government requests?

P10.6 Do the company's explanations clearly disclose the basis under which it may comply with requests from private parties?

P10.7 Does the company clearly disclose that it carries out due diligence on government

requests before deciding how to respond?

P10.8 Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?

P10.9 Does the company commit to push back on inappropriate or overbroad government requests?

P10.10 Does the company commit to push back on inappropriate or overbroad private requests?

P10.11 Does the company provide clear guidance or examples of implementation of its process for government requests?

P10.12 Does the company provide clear guidance or examples of implementation of its process for private requests?

P11. Data about third-party requests for user information The company should regularly publish data about government and other third-party requests for user information.

P11.1 Does the company list the number of requests it receives by country?

P11.2 Does the company list the number of requests it receives for stored user information and for real-time communications access?

P11.3 Does the company list the number of accounts affected?

P11.4 Does the company list whether a demand sought communications content or non-content or both?

P11.5 Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?

P11.6 Does the company include requests that come from court orders?

P11.7 Does the company list the number of requests it receives from private parties?

P11.8 Does the company list the number of requests it complied with, broken down by category of demand?

P11.9 Does the company list what types of government requests it is prohibited by law from disclosing?

P11.10 Does the company report this data at least once per year?

P11.11 Can the data reported by the company be exported as a structured data file?

P12. User notification about third-party requests for user information The company should notify users to the extent legally possible when their user information has been requested by governments and other third parties.

P12.1 Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) request their user information?

P12.2 Does the company clearly disclose that it notifies users when private parties request their user information?

P12.3 Does the company clearly disclose situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users?

P13. Security oversight The company should clearly disclose information about its institutional processes to ensure the security of its products and services.

P13.1 Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information?

P13.2 Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services?

P13.3 Does the company clearly disclose that it commissions third-party security audits on its products and services?

P14. Addressing security vulnerabilities The company should address security vulnerabilities when they are discovered.

P14.1 Does the company clearly disclose that it has a mechanism through which security

researchers can submit vulnerabilities they discover?

P14.2 Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities?

P14.3 Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?

P15. Data breaches The company should publicly disclose information about its processes for responding to data breaches.

P15.1 Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?

P15.2 Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?

P15.3 Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?

P16. Encryption of user communication and private content (Internet, software, and device companies) The company should encrypt user communication and private content so users can control who has access to it.

P16.1 Does the company clearly disclose that the transmission of user communications is encrypted by default?

P16.2 Does the company clearly disclose that transmissions of user communications are encrypted using unique keys?

P16.3 Does the company clearly disclose that users can secure their private content using end-to-end encryption, or full-disk encryption (where applicable)?

P16.4 Does the company clearly disclose that end-to-end encryption, or full-disk encryption, is enabled by default?

P17. Account Security (Internet, software, and device companies) The company should help users keep their accounts secure.

P17.1 Does the company clearly disclose that it deploys advanced authentication methods to prevent fraudulent access?

P17.2 Does the company clearly disclose that users can view their recent account activity?

P17.3 Does the company clearly disclose that it notifies users about unusual account activity and possible unauthorized access to their accounts?

P18. Inform and educate users about potential risks The company should publish information to help users defend themselves against cyber risks.

P18.1 Does the company publish practical materials that educate users on how to protect themselves from cyber risks relevant to their products or services?

Governance Indicators

G1. Policy Commitment

G1.1 Does the company make an explicit, clearly articulated policy commitment to human rights, including freedom of expression and privacy?

G2. Governance and management oversight

G2.1 Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect freedom of expression and privacy?

G2.2 Does the company clearly disclose that an executive-level committee, team, program, or officer oversees how company practices affect freedom of expression and privacy?

G2.3 Does the company clearly disclose that a management-level committee, team, program, or officer oversees how company practices affect freedom of expression and privacy?

G3. Internal implementation

G3.1 Does the company clearly disclose that it provides employee training on freedom of expression and privacy issues?

G3.2 Does the company clearly disclose that it maintains an employee whistleblower program through which employees can report concerns related to how the company treats its users' freedom of expression and privacy rights?

G4. Impact assessment

G4.1 As part of its decision-making, does the company consider how laws affect freedom of expression and privacy in jurisdictions where it operates?

G4.2 Does the company regularly assess freedom of expression and privacy risks associated with existing products and services?

G4.3 Does the company assess freedom of expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies or entry into new markets?

G4.4 Does the company assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service?

G4.5 Does the company disclose that it assesses freedom of expression and privacy risks associated with its use of automated decision-making, such as through the use of algorithms and/or artificial intelligence?

G4.6 Does the company assess freedom of expression and privacy risks associated with its targeted advertising policies and practices?

G4.7 Does the company conduct additional evaluation wherever the company's risk assessments identify concerns?

G4.8 Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?

G4.9 Does the company conduct assessments on a regular schedule?

G4.10 Are the company's assessments assured by an external third party?

G4.11 Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?

G5. Stakeholder engagement

G5.1 Is the company a member of a multi-stakeholder initiative whose focus includes a commitment to uphold freedom of expression and privacy based on international human rights principles?

G5.2 If the company is not a member of a multi-stakeholder initiative, is the company a member of an organization that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy?

65.3 If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly impacted by the company's business?

66. Remedy

66.1 Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their freedom of expression or privacy has been adversely affected by the company's policies or practices?

66.2 Does the company clearly disclose its procedures for providing remedy for freedom of expression- or privacy-related grievances?

66.3 Does the company clearly disclose timeframes for its grievance and remedy procedures?

66.4 Does the company clearly disclose the number of complaints received related to freedom of expression and privacy?

66.5 Does the company clearly disclose evidence that it is providing remedy for freedom of expression and privacy grievances?



Disclosure vs. Practice

Following the RDR Index methodology, we scored companies based on their official public disclosure of policies and practices that affect privacy and freedom of expression. We did not test companies' products. We encourage cybersecurity researchers, privacy engineers, Open Source Investigation (OSINT) experts, and other technology and human rights researchers to develop their own methods, or use other widely used methodologies, to test companies' products in order to understand to what extent companies' disclosures and claims match actual practice. These resources are also helpful for companies to apply best practices in their product design and development.

The following, although not exhaustive, may be helpful:

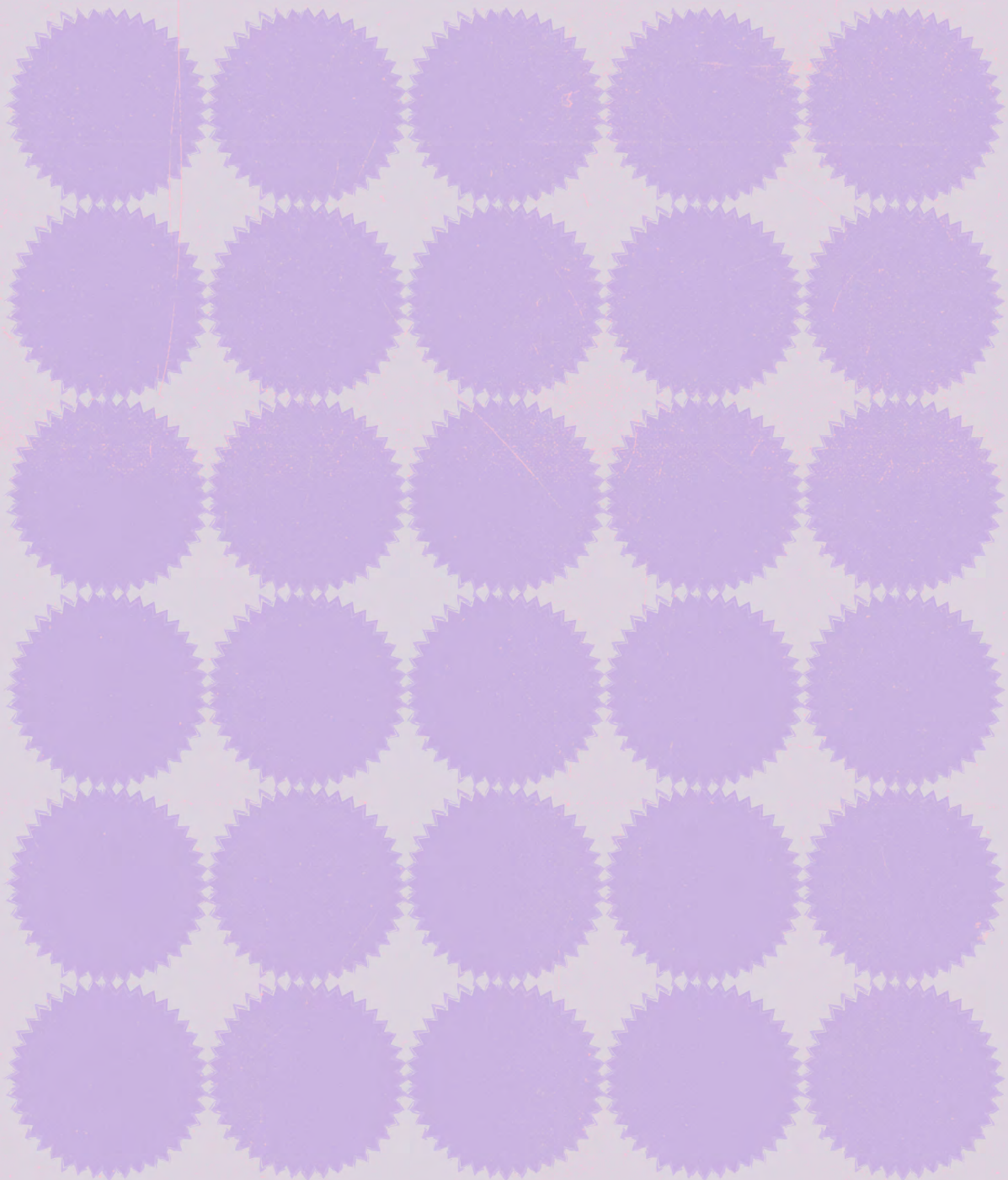
Resources on testing products for security and privacy measures:

- ✦ The Open Web Application Security Project or OWASP's Mobile Security Testing Guide is an instruction manual for reverse engineering and testing mobile apps for privacy and security.
<https://mobile-security.gitbook.io/mobile-security-testing-guide/overview/0x03-overview>
- ✦ The OWASP's Testing for Weak Encryption
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption
- ✦ The Digital Standard is "a digital privacy and security standard to help guide the future design of consumer software, digital platforms and services, and Internet-connected products." The Digital standard is a collective effort by Consumer Reports, Disconnect, Ranking Digital Rights, and The Cyber Independent Testing Lab.
<https://www.thedigitalstandard.org/the-standard>
- ✦ The Mozilla Observatory is a tool for testing websites' security
<https://observatory.mozilla.org/>
- ✦ Digital Security and Privacy Protection UX Checklist
<https://static1.squarespace.com/static/5e28cfb6752be803fc51f907/t/5eaa5b-9f4f2f3e5a01d381ba/1588222879354/Secure+UX+Checklist.pdf>

DIGITAL RIGHTS WORKBOOK

START THE CONVERSATION IN YOUR COMPANY

BY **TARAAZ** AND **FILTERWATCH**





Digital Rights Workbook: Start the Conversation in Your Company

Applying the **Ranking Digital Rights Corporate Accountability Index** methodology to guide Iranian technology companies toward greater transparency and better digital rights practices

Who is this workbook for?

This workbook is designed to help companies in their self-assessment process. In particular, it is targeted toward small start-up companies in Iran who want to instill digital rights values from the earliest stages of their activities.

How can you use this workbook?

We suggest organizing a one or two day workshop to go through different elements of the workbook.

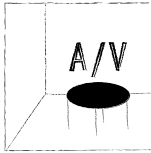
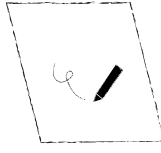
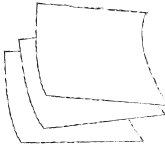
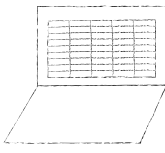
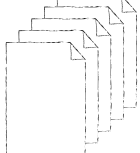
☀ Workshop preparation

A member of the executive/management team should take the lead on organizing a workshop. Beforehand, the organizer should read **this report** and other resources such as **the UN Guiding Principles on Business and Human Rights**, then circulate the resources among team members.

The organizer should invite members of the following teams to participate at the workshop:

- ☀ **Member(s) of executive and management team**
- ☀ **Member(s) of CS and Engineering team**
(e.g. developers, system administrator, etc.)
- ☀ **Member(s) of UX/UI research and design**
- ☀ **Member(s) of legal and policy team**
- ☀ **Member(s) of Public Relations and communications team**

You will also need:

-  ☀ **A conference room with an AV system**
-  ☀ **White board**
-  ☀ **Sticky notes**
-  ☀ **A laptop for working on the workbook**
-  ☀ **Printouts of privacy policy and ToS if available**

☀ Workshop activity

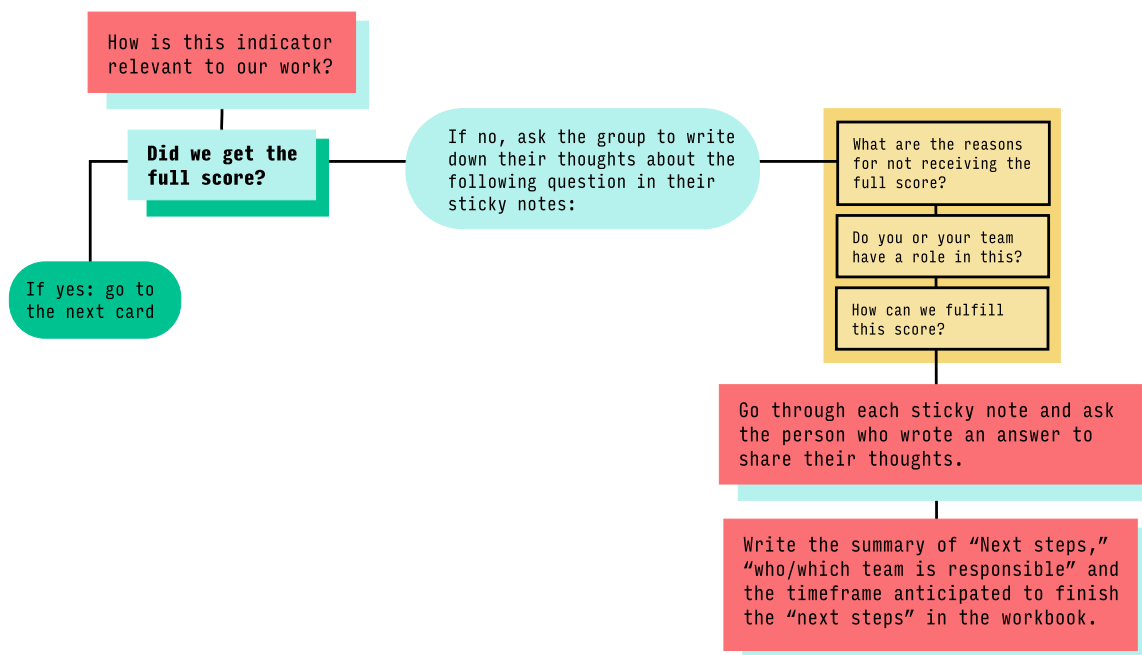
The organizer will open the workshop by providing a brief presentation about the UNGP and Ranking Digital Rights Index, followed by describing the reasons and goals of the workshop. The person should also explain the workshop activities and assign a note taker for the workshop and a volunteer to collect the notes and help the lead in facilitating the discussion.

☀ Indicator cards

You can download the Excel workbooks for privacy, freedom of expression, and governance on the [Filterwatch website](#).

☀ Group discussion

The organizer reads each indicator (**in the workbook**) and the group starts a discussion by answering the following questions:



Acronyms and Glossary of Terms

API

Application Programming Interface

Bot

Automated programs designed to perform a specific task

Bug Bounty

An initiative, often by websites or developers that rewards individuals for discovering and reporting software

CDICC

The Committee for Determining Instances of Criminal Content (CDICC)

Digital Rights

Human rights in the digital age, referring to the extension of the enjoyment of fundamental human rights, such as those recognised by the Universal Declaration of Human Rights (UDHR) to digital technologies and the internet.

Encryption

Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

End-to-End Encryption (E2EE)

System of communication that ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient.

ICCPR

International Covenant on Civil and Political Rights.

ICESCR

International Covenant on Economic, Social and Cultural Rights.

The Right to Privacy

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” (UDHR, Article 12).

ICT

Information and Communications Technology

IRIB

Islamic Republic of Iran Broadcasting

Multi-Stakeholder Initiatives (MSIs)

Voluntary partnerships between companies, civil society organizations, academic institutions, investors, governments, and other stakeholder to enable collective governance. Global Network Initiative (GNI) is an example of a Multi-Stakeholder Initiative.

RDR

Ranking Digital Rights

The Right to Freedom of Expression

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” (UDHR, Article 19)

UDHR

Universal Declaration of Human Rights

UN

United Nations

UNGP

United Nations Guiding Principles on Business
and Human Rights

2FA

Two Factor Authentication





**DIGITAL RIGHTS &
TECHNOLOGY SECTOR
ACCOUNTABILITY IN IRAN:**
THE CASE OF MESSAGING APPS