Policy briefing

Supporting Internet Access and Security for Civil Society in Iran

What the US Government and Technology Companies Can Do

Center for
HUMAN
RIGHTS
in Iran

Supporting Internet Access and Security for Civil Society in Iran
What the US Government and Technology Companies Can Do

Center for Human Rights in Iran
New York
Tel: +1 -347-689-7782

www.iranhumanrights.org

Supporting Internet Access and Security for Civil Society in Iran

What the US Government and Technology Companies Can Do

April 2021

Center for HUMAN RIGHTS in Iran

www.iranhumanrights.org

ACKNOWLEDGMENTS

The Center for Human Rights in Iran gratefully acknowledge the extensive input of Amir Rashidi, Director of Digital Rights and Security at the New York-based human rights organization Miaan Group, in the preparation of this briefing, which was largely based on a conversation with Mr. Rashidi on January 15, 2021.

About us

Center for HUMAN RIGHTS in Iran

The **Center for Human Rights in Iran (CHRI)** is an independent, nonpartisan, nonprofit organization dedicated to the protection and promotion of human rights in Iran. CHRI investigates and documents rights violations occurring throughout Iran, relying on first-hand accounts to expose abuses that would otherwise go unreported. We bring these violations to the attention of the international community through news articles, briefings, in-depth reports and videos, and work to build support for human rights inside Iran as well. CHRI engages in intensive outreach and international advocacy aimed at defending the fundamental rights and freedoms of the Iranian people and holding the Iranian government accountable to its human rights obligations.

EXECUTIVE SUMMARY

The context

The US Treasury's Office of Foreign Assets Control (OFAC) has exempted the sale of personal communications tools and services from its sanctions on Iran.[1] This exemption, articulated in General License D1, is in recognition of the critical role such tools play in access to information and freedom of expression in repressive societies.[2] Yet access to international communications products by the people of Iran continues to be hampered by companies' reluctance to sell their goods and services to them.

This reluctance is largely due to companies' concerns regarding sanctions violations, arising from the lack of clarity in the D1 license, D1's lack of inclusion of newer technologies that have come to be central to personal communications, and companies' reluctance to undergo the cost of the OFAC application process for licenses to sell goods not covered by D1.

The problem

As a result, Iranians rely largely on personal communications tools and services produced in Iran, which are accessible to state surveillance and censorship. This poses significant security risks for users, who are operating in a context where the authorities openly acknowledge their monitoring of online content, and where online content disapproved of by the state can land one in prison. The effect has been especially harmful for the activist and dissident communities, for whom internet security is essential.

What can be done

The US government should clarify and update D1; encourage companies to pursue the sale of personal communications tools and services to Iranians and to make their free services available to them; streamline the OFAC license application process; and establish OFAC-approved financial channels to handle payments for these goods by Iranians.

Companies, for their part, should actively pursue sales of personal communications tools and services under D1; make their free services available to Iranians, and devote the legal and technical resources to apply for OFAC licenses to sell additional goods and services as needed.

Why it matters

Supporting Iranians' access to international communications tools and services will strengthen access to information and safe online communication for Iranian civil society. This *requires no changes to current sanctions legislation*, but rather more effective implementation of existing sanctions law to meet the stated aim of D1, which is to support freedom of expression in repressive societies.

RECOMMENDATIONS

To the US Government:

1. **Update and expand** OFAC's General License D1 so that "personal communications tools and services" that are exempt from sanctions on Iran explicitly include current internet technologies that have become central to communications. The US Treasury should **consult with tech and digital rights experts** to determine those technologies.

2. **Clarify**, with specificity and detailed guidance, exactly what D1 includes under "personal communications," as uncertainty regarding the scope of the exemptions has created fear among companies of sanctions violations and overcompliance.

3. **Encourage companies** to sell these tools and services to Iranians and to make free services available to them, through public assurances and comfort letters, and encourage companies to apply for OFAC licenses for further sales.

4. **Streamline the OFAC license application process** so that companies do not need to allocate years' worth of time by their legal and technical teams in order to apply for licenses.

5. **Designate OFAC-approved financial channels** for payment by Iranians for personal communications tools and services, as financial institutions remain reluctant to process even permissible transactions with Iranians due to fears of violating US banking sanctions.

To technology companies:

1. **Pursue sales** of personal communications tools and services to Iranians under OFAC's General License D1, and **make free services available** as well.

2. **Ask the US government** to clarify, update and expand General License D1 to explicitly include current digital technologies that have become central to online communications, and **consult with digital rights experts** to identify those technologies that are most critical to target.

3. **Advocate with the US Treasury** for streamlining OFAC's license application process.

4. **Devote the legal and technical resources** to apply for OFAC licenses.

5. **Advocate with the US government** for the establishment of designated payment channels so Iranians can pay for these tools and services.

INTRODUCTION

While US sanctions prohibit companies from doing business with Iran, the US Treasury's Office of Foreign Assets Control (OFAC), under General License D1, permits the sale of personal communications tools and services to Iranians, in recognition of the vital role such items play in assisting civil society and freedom of expression in repressive countries.[3] OFAC also considers requests for specific licenses to sell or make accessible other types of communications tools and services not clearly covered under D1.[4]

Despite D1, access to international communications tools and services by people in Iran has been undermined by companies' reluctance to sell their goods and services to Iranians or to allow Iranians access to their free services. This is largely due to companies' concerns regarding sanctions violations, arising from the lack of specificity, clarity and inclusiveness in the D1 license. Applying for specific OFAC licenses to sell products not clearly covered under D1 has also been avoided by companies due to the costly and time-consuming process that the application process typically requires. The lack of financial channels for Iranians to pay for such goods and services, irrespective of their permissibility, has compounded the problem.

As a result, Iranians still do not have access to a broad range of international communication tools and services. This has negatively impacted access to information and digital security throughout Iranian society, because it means Iranians must largely rely on communication tools and services produced in Iran, which are accessible to state surveillance and censorship. This poses serious security risks for users, who must operate in a repressive context where online content disapproved of by the state can land one in prison. The effect has been particularly harmful for the activist and dissident communities, for whom internet security is of vital importance.

This policy briefing by the Center for Human Rights in Iran details actions the Biden administration and technology companies could take to facilitate Iranians' access to international communications tools and services. Such actions would not require any new sanctions legislation or the lifting of any current sanctions, but rather more effective clarification and implementation of existing sanctions—as well as a commitment by both the government and companies to support the Iranian people's right to online access and digital security.

STRENGTHENING OFAC'S GENERAL LICENSE D1

The US Treasury's Office of Foreign Assets Control (OFAC) General License D1, allowing the sale of personal communications tools and services to Iranians, needs to be clarified and updated, so that:

1) The full range of tools and services necessary for personal communications is included in General License D1;

2) Companies know exactly what tools and services are permissible under D1.

Clarifying D1

There is an atmosphere of fear surrounding US sanctions on Iran amongst technology companies and uncertainty regarding permissible sales of personal communications tools and services, arising from a lack of specificity and clarity in D1's guidance. This has resulted in sanctions overcompliance and the unavailability for Iranians of international tools and services that should be exempt from sanctions because they are vital to personal communications.

To remedy this, OFAC should publish more specific guidelines, with clear and specific examples, making clear the full range of tools and services that are allowed, so that there is no ambiguity and no reason for companies to overcomply.

Updating D1

Communications technology has evolved since D1 was established, and the license needs to be updated to reflect this. For example, cloud and hosting services are now essential infrastructure for safe online communications; if one cannot host a website with a secure service or put a website onto a secure data center then one will not be able to communicate effectively. Yet access to such international services has been highly problematic for Iranians, as major services such as Google Cloud, Amazon Web Services (AWS), DigitalOcean and GoDaddy still do not make their products available to Iranians.

D1 needs to explicitly reference cloud and hosting services and other technology infrastructure that have come to be central to online communication; only then will companies know these products are included under the sanctions exemptions and be willing to make them available to Iranians.

The recent success of the code hosting platform GitHub in securing an OFAC license to allow Iranians to use its paid and free services illustrates the importance of expanding the technologies included in D1.[5] The license allows Iranians to use GitHub's open source code to develop software, applications, online services and websites for any number of uses—business, educational, nonprofit—potentially freeing developers in Iran from Iranian-produced products that incur security risks because anything stored on state servers or state infrastructure can be accessed by the state and is therefore vulnerable to the Iranian authorities' surveillance and censorship.

There are also more direct human rights implications of the GitHub license: technology professionals in Iran can use GitHub to access codes that can help develop censorship circumvention tools, as well as tools such as firewalls and antivirus software that make websites or online communications more secure from state access, surveillance and hacking.

The US Treasury should consult closely with technology and digital rights experts to determine which technologies, tools and services are now central to personal communications, and explicitly include these in the D1 General License.

Encouraging companies

US Treasury officials should talk to technology companies and provide explicit public and private assurances to them, for example through letters of comfort, that such sales are permissible, and encourage companies to make their goods and services, both paid and free, available to Iranians.

Access to the internet is not a luxury; it is an essential service—and a fundamental right. A major effort is needed to reach out to these companies and explain to them not only the permissibility of such sales but also the cost to civil society of sanctions overcompliance.

US officials should talk to technology and digital rights experts to ascertain the companies that should be prioritized for outreach efforts due to the centrality of their products for Iranian civil society.

There is an atmosphere of fear surrounding US sanctions on Iran…arising from a lack of specificity and clarity in D1's guidance.

Streamlining OFAC's license application process

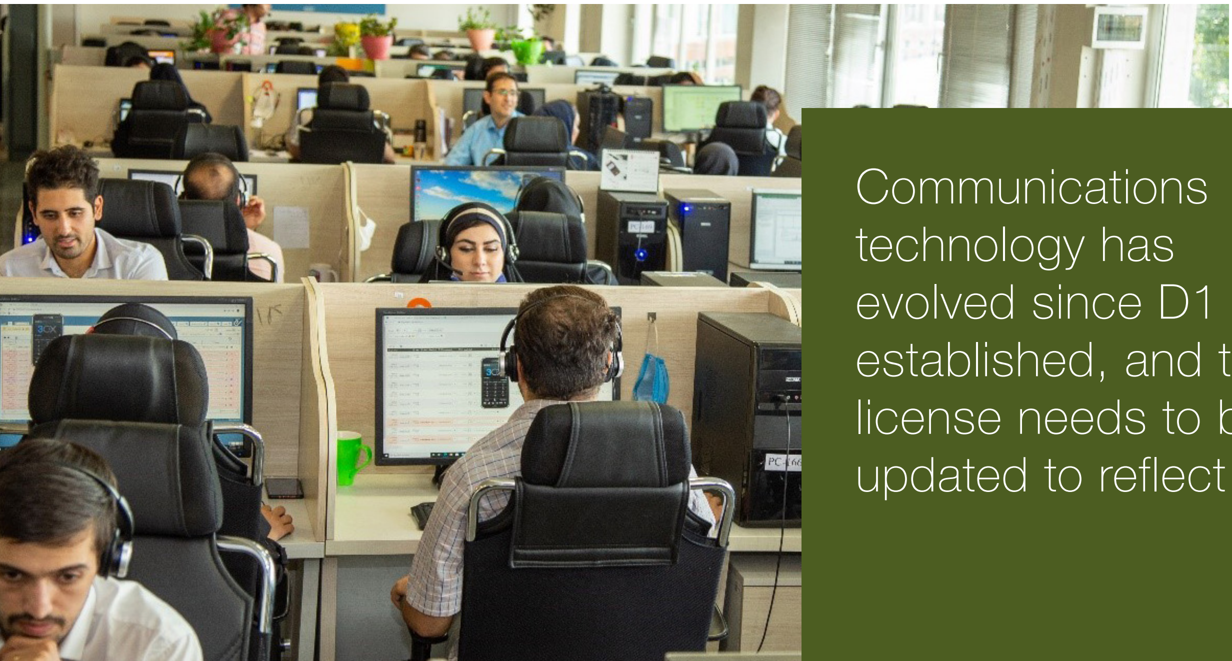
OFAC should streamline its process for applying for a specific license, so that companies do not have to devote years of time and the resources of their legal and technical teams to acquire such licenses. GitHub, for example, had to go through a two-year process to obtain its OFAC license.[6]

GitHub was a success only because there was close collaboration between the company's legal and technical teams, and the company was willing to devote the time and resources of these teams to make the case for the license. Yet that bar is high (for smaller companies, such expenditures are not even a possibility) and it has resulted in a reluctance amongst companies to seek OFAC licenses for tools and services that are central to safe online information access and communication.

Establishing viable payment channels

The Biden Administration also needs to address the need for safe, designated payment channels for trade in permissible goods and services to Iranians. Because of a fear of violating US secondary sanctions, banks are reluctant to proceed even with legal financial transactions with Iranians.[7] Irrespective of exemptions and licenses, if Iranians cannot find a way to pay for international tools and services, they will be unable to access them.

A similar problem has been experienced with the sale of humanitarian goods to Iran, which are also exempt from US sanctions.[8] The Swiss Humanitarian Trade Agreement (SHTA), a financial channel established by the Swiss government in collaboration with Washington, has sought to address this problem by establishing an OFAC-approved financial channel for handling medical and other humanitarian sales to Iran.[9] SHTA is limited; only Swiss companies can use it. Yet even this kind of limited channel has not yet been established for communications products, rendering trade in this sector, irrespective of D1 exemptions, difficult.



Communications technology has evolved since D1 was established, and the license needs to be updated to reflect this.

WHAT TECHNOLOGY COMPANIES CAN DO

Actions by technology companies are also necessary for the people of Iran to have access to the international communication tools and services they need to fully access information and communicate safely.

Pursue sales to Iranians and make free services available

Technology companies should seek to avoid overcompliance with sanctions and pursue sales of personal communications tools and services to Iranians, as these products are exempt from sanctions under OFAC's General License D1. Services that are free should also be made available to Iranians. While there are numerous companies involved in products pertinent to personal communications, a few companies stand out as particularly important in the Iranian context.

Google is highly popular in Iran, and Android, which is owned by Google, is the most popular operating system in the country. A decision by Google to unlock Android Developers and the many tools and services that are linked to Android would be a significant advance for digital access and security in Iran, replacing many domestically-produced services that pose security risks to users.

Cloud and hosting services, such as Google Cloud Platform (GCP), Amazon Web Services (AWS), DigitalOcean and GoDaddy have also become central to digital communications and their sale to Iranians should be pursued.

Access to Apple services is needed as well. Creating an Apple ID, which is necessary for downloading Apple applications, requires a phone number but Iranian phone numbers are not accepted by Apple. This means, for example, that instead of putting their apps on the Apple Store Iranians use their local app store, Cafe Bazaar, which is banned from offering applications to the public that are blocked in Iran and where anything on the phone (including such things as circumvention tools) can be viewed by the store and passed along to the government. Not only does this pose a severe risk to the individual users, it also alerts the Iranian authorities to the tools they should block.

Technology companies should consult with digital rights experts to better understand the critical uses of these tools and services and the implications of their inaccessibility to citizens of repressive countries such as Iran. This consultation should be part of an ongoing collaborative engagement process so that discussions continue to reflect current technologies.

Iranians must rely on communication tools and services produced in Iran, which are accessible to state surveillance and censorship.

Apply for OFAC licenses

If technology companies believe in supporting online access and security—especially in repressive country contexts—then they should allocate the legal and technical resources to apply for specific OFAC licenses. Such licenses are needed to pursue sales beyond those tools and services that are clearly covered by D1, so that other products needed for information access and safe online communication, whose permissibility may be unclear, are made available to the people of Iran. And companies need to engage with the US government until they get those licenses.

The OFAC license for GitHub was issued only because the company devoted the time and resources, there was close collaboration between the company's legal and technical teams, and the company was willing to make the case for the license with the US government. That kind of commitment is needed by other companies. GitHub demonstrated that licenses to sell communication tools and services to Iranians can be obtained, but only if a decision is made by the company to allocate the resources.

Advocate with the US Government

Technology companies should make their views regarding what they need in order to sell personal communications tools and services to Iranians clear to the Biden administration.

Companies should ask OFAC to clarify, update and expand General License D1 so that it is clear what is permissible and what is not, and so that it reflects the current state of information and communications technology and explicitly includes tools and services that have become central to communications.

They should also ask the US Treasury to streamline OFAC's license application process. The two-year process GitHub went through to obtain its OFAC license is not an option for smaller companies.

Technology companies also need to address the lack of payment channels for Iranians with the Biden Administration, advocating with the Treasury Department for designated channels so that Iranians can pay for these tools and services. Sales are impossible if Iranians cannot pay for them, whether or not they are licensed.

IMPACT ON FREEDOM OF EXPRESSION

The inability to access international communications tools and services has direct consequences for the people of Iran—as it does for the citizens of any repressive country.

Compromised digital security

Without access to international tools and services, any online communication or activity is accessible to the state because all these communications travel over state infrastructure using state tools and services.

The Iranian government has openly boasted of its online surveillance activities. It uses information thus retrieved to convict individuals whose political or cultural views depart from those of the authorities, under manufactured charges that typically include espionage, threats to national security, propaganda against the state, collaboration with an enemy state, and *mohabereh* (enmity against God), which can carry the death penalty.

The Iranian government is moving aggressively to fill the space left by the absence of these international companies' products with its own versions of these tools and services. The Iranian government's home-grown services now include operating systems, data centers, search engines, email services, social media networks, messaging apps, and so forth, and the government is investing significant resources to create a cloud and hosting service.

This poses serious security risks for users, who operate in a repressive context where online content disapproved of by the state can land one in prison.

Without the latest tools and services… communication between the citizens of Iran and to the outside world will be increasingly at the state's discretion.

If Iranians cannot use international communication tools and services, they will use these locally-made products, which are not equivalent or safe for users. The ramifications will include:

- More convictions of activists, dissidents, independent journalists and human rights lawyers for online content.
- The inability of Iranian civil society—especially the activist and dissident communities—to safely and effectively share information domestically or with international sources such as global media or the UN.

Increased censorship

State censorship is also facilitated by the loss of access to international tools and services. While millions of websites (especially international news sites and the websites of rights-based organizations) and major social media platforms have long been blocked in Iran, the state has increasingly focused on blocking VPNs and other censorship circumvention tools, as well as messaging applications that employ end-to-end encryption.[10]

Without the ability to access—or develop—new tools and services that allow an end-run around state censors, Iranians have less access to:

- Independent news sources
- NGOs and other civil society organizations in Iran
- Human rights organizations, both domestic and international
- Foreign and independent media

Internet shut-downs

Being forced to use local services also means Iranians are more vulnerable to state shutdowns of the global internet inside Iran.

The authorities in Iran shut down access to the global internet when they want to prevent news from getting in or out of the country—which typically occurs during the violent state suppression of protests and other egregious human rights violations by the government.[11] For example, internet access was briefly cut off during protests in Iran in December 2017; fully blocked for roughly a week during the state's violent crushing of the 2019 street protests (when hundreds of civilians were killed by state security forces); disrupted again in Khuzestan province in July 2020; and most recently, again blocked during unrest in Sistan and Baluchistan province in March 2021.[12]

When Iran did not have its own domestic versions of communications tools and services that it could run on the country's national internet project, the National Information Network (NIN), the cost of cutting off access to the global internet was high. For example, the functions of banks and government services, which use online services, would be affected. Yet with the expansion of domestic services run on the country's national internet, cutting off access to the global internet no longer means disruption to key services. Internet cut-offs thus become less costly—and more likely—as evidenced by Iran's growing use of this technique, enabling the authorities to impose "news blackouts" that prevent state repression from being broadcast to the outside world.

Without the latest tools and services to allow Iranians to bypass these blockages and shutdowns, communication between the citizens of Iran and to the outside world will be increasingly at the state's discretion.

Internet freedom globally

Beyond Iran, limiting access to international communications tools and services also hurts the global internet. It is contributing to the localization of the internet, where national networks like Iran's NIN, which make users vulnerable to state surveillance, hacking and censorship, proliferate.

This is not only an Iranian issue; repressive countries around the world are models for each other, sharing tools and techniques and learning from one another. Addressing the growing localization of the internet and the threat to information access and security it represents should be a global priority.

Access to the internet is a fundamental right—and access to international communications tools and services is key to protect it. These products are essential to the ability to effectively counter efforts by repressive states to control cyberspace. As part and parcel of a commitment and indeed obligation to uphold freedom of expression and fundamental human rights, the Biden administration and technology companies should do all in their power to support access to critical communication tools and services for the people of Iran.

Center for HUMAN RIGHTS in Iran

Supporting Internet Access and Security for Civil Society in Iran

What the US Government and Technology Companies Can Do

ENDNOTES

1 “Iran Sanctions,” U.S. Department of the Treasury https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/iran-sanctions

2 “Treasury Department Reaffirms Commitment to Fostering Internet Freedom and Supporting the Iranian People,” U.S. Department of the Treasury https://home.treasury.gov/news/press-releases/sm0322

3 Ibid.

4 “OFAC License Application Page,” U.S. Department of the Treasury https://home.treasury.gov/policy-issues/financial-sanctions/ofac-license-application-page

5 Nat Friedman, “Advancing developer freedom: GitHub is fully available in Iran,” The GitHub blog, January 5, 2021, https://github.blog/2021-01-05-advancing-developer-freedom-github-is-fully-available-in-iran/

6 Ibid.

7 Kenneth Katzman, “Iran Sanctions, Updated November 18, 2020,” Congressional Research Service https://fas.org/sgp/crs/mideast/RS20871.pdf

8 See “Clarifying Guidance: Humanitarian Assistance and Related Exports to the Iranian People,” Office of Foreign Assets Control, US Department of the Treasury, February 6, 2012 https://home.treasury.gov/system/files/126/hum_exp_iran.pdf and “Guidance on the Sale of Food, Agricultural Commodities, Medicine, and Medical Devices by Non-U.S. Persons to Iran,” US Department of the Treasury, July 25, 2012 https://home.treasury.gov/system/files/126/iran_guidance_med.pdf and “Financial Channels to Facilitate Humanitarian Trade with Iran and Related Due Diligence and Reporting Expectations,” US Department of the Treasury https://home.treasury.gov/system/files/126/iran_humanitarian_20191025.pdf

9 “United States and Switzerland Finalize the Swiss Humanitarian Trade Arrangement,” US Department of the Treasury, February 27, 2020 https://home.treasury.gov/news/press-releases/sm919

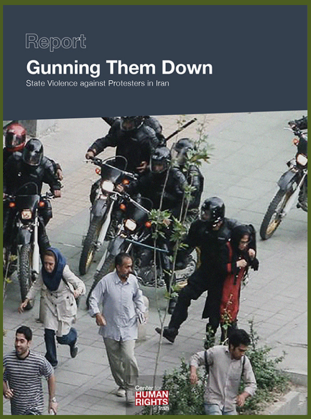
10 See “Guards at the Gate: The Expanding State Control Over the Internet in Iran,” Center for Human Rights in Iran, January 2018 https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf and “Closing of the Gates: Implications of Iran’s Ban on the Telegram Messaging App,” Center for Human Rights in Iran, June 2018 https://www.iranhumanrights.org/wp-content/uploads/Closing-the-gates-3-online.pdf

[11] Matt Burgess, “Iran’s Total Internet Shutdown Is a Blueprint for Breaking the Web,” Wired, October 7, 2020 https://www.wired.co.uk/article/iran-news-internet-shutdown

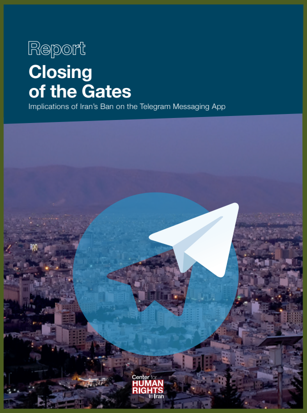
[12] See “Silencing the Streets; Deaths in Prison,” Center for Human Rights in Iran, February 2018 https://www.iranhumanrights.org/wp-content/uploads/Silencing-the-streets-6.pdf and “Gunning Them Down: State Violence against Protesters in Iran,” Center for Human Rights in Iran, May 2020 https://iranhumanrights.org/wp-content/uploads/Iran-Human-Rights-November-2019-January-2020-Protests.pdf and “Internet Disrupted in Iran amid Regional Protest,” Netblocks, July 16, 2020 https://netblocks.org/reports/internet-disrupted-in-iran-amid-regional-protests-xyMkjXAZ and “Deaths Rising in Sistan and Baluchistan as Unrest Continues Amidst Internet Shutdown,” Center for Human Rights in Iran, March 1, 2021 https://www.iranhumanrights.org/2021/03/deaths-rising-in-sistan-and-baluchistan-as-unrest-continues-amid-internet-shutdown/

Recent reports

by the Center for Human Rights in Iran


Report
Gunning Them Down
State Violence against Protesters in Iran
Center for HUMAN RIGHTS in Iran

Gunning Them Down
State Violence against Protesters in Iran
May 2020


Report
Closing of the Gates
Implications of Iran's Ban on the Telegram Messaging App
Center for HUMAN RIGHTS in Iran

Closing of the Gates
Implications of Iran's Ban on the Telegram Messaging App
June 2018

Report
Guards at the Gate
The Expanding State Control Over the Internet in Iran
Center for HUMAN RIGHTS in Iran

Guards at the Gate
The Expanding State Control Over the Internet in Iran
January 2018

Center for HUMAN RIGHTS in Iran

Supporting Internet Access and Security for Civil Society in Iran
What the US Government and Technology Companies Can Do