Freedom
House

Methodology Questions

❖ *Freedom on the Net* scores have been inverted to align with *Freedom in the World*, Freedom House's flagship report on political rights and civil liberties.
❖ Each country is ranked on a scale of 100 to 0, with 100 representing the most free conditions and 0 the least free.
❖ A combined score of 100-70 = Free, 69-40 = Partly Free, and 39-0 = Not Free.

A. OBSTACLES TO ACCESS (0–25 POINTS)

1. **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections? (0–6 points)**

   ● Do individuals have access to high-speed internet services at their home, place of work, internet cafés, libraries, schools, and other venues, as well as on mobile devices?
   ● Does poor infrastructure (including unreliable electricity) or catastrophic damage to infrastructure (caused by events such as natural disasters or armed conflicts) limit citizens' ability to access the internet?

2. **Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons? (0–3 points)**

   ● Do financial constraints—such as high prices for internet services, excessive taxes imposed on such services, or state manipulation of the relevant markets—make internet access prohibitively expensive for large segments of the population?
   ● Are there significant differences in internet penetration and access based on geographical area, or for certain ethnic, religious, gender, LGBT, and other relevant groups?
   ● Do zero-rating plans or other pricing practices by service providers create a digital divide in terms of what types of content individuals with different financial means can access?

3. **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity? (0–6 points)**

   ● Does the government restrict, or compel service providers to restrict, internet connectivity by slowing or shutting down internet connections during specific events (such as protests or elections), either locally or nationally?
   ● Does the government centralize internet infrastructure in a manner that could facilitate restrictions on connectivity?
   ● Does the government block, or compel service providers to block, social media platforms and communication apps that serve in practice as major conduits for online information?
   ● Does the government block, or compel service providers to block, certain protocols, ports, and functionalities within such platforms and apps (e.g., Voice-over-Internet-Protocol or VoIP, video streaming, multimedia messaging, Secure Sockets Layer or SSL), either permanently or during specific events?

- Do restrictions on connectivity disproportionately affect marginalized communities, such as inhabitants of certain regions or those belonging to different ethnic, religious, gender, LGBT, and other relevant groups?

4. **Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers? (0–6 points)**

- Is there a legal or de facto monopoly on the provision of fixed-line, mobile, and public internet access?
- Does the state place extensive legal or regulatory controls on the establishment of service providers?
- Are operating licenses approved or rejected on partisan or prejudicial grounds?
- Do licensing requirements, such as retaining customer data or preventing access to certain content, place an onerous financial burden on service providers?
- Does the state place prohibitively high fees on the establishment and operation of service providers?
- Are favorable informal connections with government officials necessary for service providers to establish operations or remain viable?

5. **Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner? (0–4 points)**

- Are there explicit legal guarantees that protect the independence and autonomy of any regulatory body overseeing the internet (exclusively or as part of a broader mandate) from political or commercial interference?
- Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' legitimate interests?
- Are decisions taken by regulatory bodies, particularly those relating to the internet, seen to be fair and to take meaningful notice of comments from stakeholders in society?
- Are decisions taken by regulatory bodies seen to be apolitical and independent from changes in government?
- Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?

B. LIMITS ON CONTENT (0–35 POINTS)

1. **Does the state block or filter, or compel service providers to block or filter, internet content? (0–6 points)**

- Does the state use, or compel service providers to use, technical means to restrict freedom of opinion and expression, for example by blocking websites and online content featuring journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression?

- Does the state use, or compel service providers to use, technical means to restrict access to websites that may be socially or legally problematic (e.g., those related to gambling, pornography, copyright violations, illegal drugs) in lieu of more effective remedies, or in a manner that inflicts significant collateral damage on content and activities that are protected under international human rights standards?
- Does the state block or order the blocking of entire social media platforms, communication apps, blog-hosting platforms, discussion forums, and other web domains for the purpose of censoring the content that appears on them?
- Is there blocking of tools that enable users to bypass censorship?
- Does the state procure, or compel services providers to procure, advanced technology to automate censorship or increase its scope?

2. **Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content? (0–4 points)**

- Are nontechnical measures—administrative, judicial, or extralegal—used to order the deletion of content from the internet, either prior to or after its publication?
- Do government officials or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
- Do digital platforms and content hosts remove content in order to avoid being prosecuted for opinions expressed by third parties via the technology they supply?
- Are access providers, content hosts, and third parties free from excessive or improper legal responsibility for information transmitted via the technology they supply?

3. **Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process? (0–4 points)**

- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
- Are those that restrict content—including state authorities, ISPs, and content hosts—transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?
- Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?

4. **Do online journalists, commentators, and ordinary users practice self-censorship? (0–4 points)**

- Do internet users in the country engage in self-censorship on important political, social, or religious issues?
- Are there unspoken rules that prevent users from expressing certain opinions via local news sites, blogs, social media platforms, or private messages?
- Do users avoid discussion of subjects that are likely to lead to retribution or result in censorship?
- Do state surveillance or data collection practices have a chilling effect on online speech or cause users to avoid certain online activities of a civic nature?

- Where widespread self-censorship exists, do some journalists, commentators, or ordinary users continue to test the boundaries, despite the potential repercussions?

5. **Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest? (0–4 points)**

- Do government officials or other powerful actors pressure or coerce online news outlets, journalists, or bloggers to follow a particular editorial direction in their reporting and commentary?
- Do authorities issue official guidelines or directives on coverage to online media outlets, including instructions to downplay or amplify certain comments or topics for discussion?
- Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the content they produce or host?
- Do government officials or other actors surreptitiously employ individuals or automated systems to artificially amplify political narratives or smear campaigns on social media?
- Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?
- Does misleading and/or false information online, coordinated by foreign or local actors for political purposes, have a significant impact on public debate?

6. **Are there economic or regulatory constraints that negatively affect users' ability to publish content online? (0–3 points)**

- Are favorable informal connections with government officials necessary for online media outlets or service providers (e.g., search engines, email applications, blog-hosting platforms) to be economically viable?
- Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it discourage advertisers from conducting business with disfavored online media or service providers?
- Do onerous taxes, regulations, or licensing fees present an obstacle to participation in, establishment of, or management of online news outlets, blogs, or social media groups/channels?
- Do ISPs manage network traffic and bandwidth availability in a manner that is transparent, is evenly applied, and does not discriminate against users or producers of content based on the nature or source of the content itself (i.e., do they respect "net neutrality" with regard to content)?

7. **Does the online information landscape lack diversity? (0–4 points)**

- Are people able to access a range of local and international news sources that convey independent, balanced views in the main languages spoken in the country?
- Do online media outlets, social media pages, blogs, and websites represent diverse interests within society, for example by providing content produced by different ethnic, religious, gender, LGBT, and other relevant groups?
- If there is extensive censorship, do users employ virtual private networks (VPNs) and other circumvention tools to access a broader array of information sources?

8. Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues? (0–6 points)

- Do online communities organize on political, social, cultural, and economic issues, including during electoral campaigns and nonviolent protests?
- Do state or other actors block online tools and websites (e.g., social media platforms, messaging groups, petition websites) for the purpose of restricting freedoms of assembly and association online?
- Does the state place legal or other restrictions on digital advocacy?

C. VIOLATIONS OF USER RIGHTS (0–40 POINTS)

1. Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence? (0–6 points)

- Does the constitution contain language that provides for press freedom and freedom of expression generally?
- Are there laws or binding legal decisions that specifically protect online modes of expression?
- Are online journalists and bloggers accorded strong rights and protections to perform their work?
- Is the judiciary independent, and do senior judicial bodies and officials support free expression online?
- Is there implicit impunity for private or state actors who commit crimes against online journalists, bloggers, or other people targeted for their online activities?

2. Are there laws that assign criminal penalties or civil liability for online activities? (0–4 points)

- Do specific laws—including those related to the media, defamation, cybercrime, cybersecurity, and terrorism—criminalize online expression and activities that are protected under international human rights standards (e.g., journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression)?
- Are restrictions on internet freedom defined by law, narrowly circumscribed, and both necessary and proportionate to address a legitimate aim?
- Are vaguely worded penal codes or security laws applied to legitimate online activities?

3. Are individuals penalized for online activities? (0–6 points)

- Are writers, commentators, bloggers, or social media users subject in practice to civil liability, imprisonment, arbitrary detention, or other legal sanction for publishing, sharing, or accessing material on the internet?
- Are penalties for defamation; spreading false information or "fake news"; national security, terrorism, and extremism; blasphemy; insulting state institutions and officials; or harming foreign relations applied widely?

4. Does the government place restrictions on anonymous communication or encryption? (0–4 points)

- Are website owners, bloggers, or users in general required to register with the government?
- Does the government require that individuals use their real names or register with the authorities when posting comments or purchasing electronic devices, such as mobile phones?
- Are users prohibited from using encryption services to protect their communications?
- Are there laws requiring that users or providers of encryption services turn over decryption keys to the government?

5. Does state surveillance of internet activities infringe on users' right to privacy? (0–6 points)

- Do state authorities engage in the blanket collection of communications metadata and/or content transmitted within the country?
- Are there legal guidelines and independent oversight on the collection, retention, and inspection of surveillance data by state security agencies, and if so, do those guidelines adhere to international human rights standards regarding transparency, necessity, and proportionality?
- Do state authorities monitor publicly available information posted online (including on websites, blogs, social media, and other digital platforms), particularly for the purpose of deterring independent journalism or political, social, cultural, religious, and artistic expression?
- Do authorities have the technical capacity to regularly monitor or intercept the content of private communications, such as email and other private messages, including through spyware?
- Do local authorities such as police departments surveil residents (including through "stingray" technology), and if so, are such practices subject to rigorous guidelines and judicial oversight?
- Do state actors use artificial intelligence and other advanced technology for the purposes of surveillance without appropriate oversight?
- Do government surveillance measures target or disproportionately affect political dissidents, human rights activists, journalists, or certain ethnic, religious, gender, LGBT, and other relevant groups?

6. Are service providers and other technology companies required to aid the government in monitoring the communications of their users? (0–6 points)

- Can the government obtain user information from companies (e.g., service providers, providers of public access, internet cafés, social media platforms, email providers, device manufacturers) without a legal process?
- Are these companies required to collect and retain data about their users?
- Are these companies required to store users' data on servers located in the country, particularly data related to online activities and expression that are protected under international human rights standards (i.e., are there "data localization" requirements)?
- Are these companies required to monitor users and supply information about their digital activities to the government (either through technical interception, data sharing, or other means)?
- Does the state attempt to impose similar requirements on these companies through less formal methods, such as codes of conduct?

- Are government requests for user data from these companies transparent, and do companies have a realistic avenue for appeal, for example via independent courts?

7. **Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities? (0–5 points)**

- Are individuals subject to physical violence—such as murder, assault, torture, or enforced disappearance—as a result of their online activities, including membership in certain online communities?
- Are individuals subject to other intimidation and harassment—such as verbal threats, travel restrictions, or property destruction or confiscation—as a result of their online activities?
- Are individuals subject to online intimidation and harassment specifically because they belong to a certain ethnic, religious, gender, LGBT, or other relevant group?
- Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such consequences?
- Have the online activities of dissidents, journalists, bloggers, human rights defenders, or other users based outside the country led to repercussions for their family members or associates based in the country?

8. **Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack? (0–3 points)**

- Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks meant to steal data or disable normal operations, including attacks that originate outside the country?
- Have websites belonging to opposition or civil society groups in the country been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
- Are websites or blogs subject to targeted technical attacks as retribution for posting certain content, for example on political and social topics?
- Are laws and policies in place to prevent and protect against cyberattacks (including systematic attacks by domestic nonstate actors), and are they enforced?