

## Checklist of Questions

- ❖ Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- ❖ A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.

### **A. OBSTACLES TO ACCESS (0-25 POINTS)**

#### **1. To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)**

- Does poor infrastructure (electricity, telecommunications, etc.) limit citizens' ability to receive internet in their homes and businesses?
- To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?
- To what extent is there internet and mobile phone access, including data connections or satellite?
- Is there a significant difference between internet and mobile phone penetration and access in rural versus urban areas or across other geographical divisions?
- To what extent are broadband services widely available in addition to dial-up?

#### **2. Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)**

- In countries where the state sets the price of internet access, is it prohibitively high?
- Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?
- Do low literacy rates (linguistic and "digital literacy") limit citizens' ability to use the internet?
- Is there a significant difference between internet penetration and access based on gender, or across ethnic or socio-economic societal divisions?
- To what extent are software, news, and other information available online in the main local languages spoken in the country?

#### **3. Does the government impose restrictions on ICT connectivity and access to particular social media and communication apps permanently or during specific events? (0-6 points)**

- Does the government place limits on the amount of bandwidth that access providers can supply?
- Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?
- Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?

- Does the government block protocols and tools that allow for instant, person-to-person communication (VoIP, instant messaging, text messaging, etc.), particularly those based outside the country (e.g. Skype, WhatsApp, etc.)?
- Does the government block protocols, social media, and/or communication apps that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?
- Is there blocking of certain tools that enable circumvention of online filters and censors?

**4. Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)**

Note: Each of the following access providers are scored separately:

**1a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)**

**1b. Cybercafes and other businesses entities that allow public internet access (0-2 points)**

**1c. Mobile phone companies (0-2 points)**

- Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?
- Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?
- Are registration requirements (i.e. bureaucratic “red tape”) for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?
- Does the state place prohibitively high fees on the establishment and operation of access providers?

**5. To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)**

- Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (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’ interests?
- Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?
- Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?
- Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?

**B. LIMITS ON CONTENT (0-35 POINTS)**

**1. To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)**

- Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?
- Is there significant filtering of text messages or other content transmitted via mobile phones?
- Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of email or text messages, etc?
- Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?

**2. To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)**

- To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?
- To what degree do government officials or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
- Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?
- Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?

**3. To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by 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 state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?
- Do state authorities block more types of content than they publicly declare?
- 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)**

- Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?
- Are there unspoken “rules” that prevent an online journalist or user from expressing certain opinions in ICT communication?
- Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?

**5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)**

- To what degree do government officials or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?
- Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize 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 online content they produce or host?
- Does the government employ, or encourage content providers to employ, individuals to post progovernment remarks in online bulletin boards and chat rooms?
- Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?

**6. Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)**

- Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, email applications, blog hosting platforms, etc.) to be economically viable?
- Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?
- Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?
- To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?
- To what extent do users have access to free or low-cost blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?

**7. To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)**

- Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?
- Does the public have ready access to media outlets or websites that express independent, balanced views?
- Does the public have ready access to sources of information that represent a range of political and social viewpoints?

- To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?
- To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?

**8. To what extent have individuals successfully used the internet and other ICTs as sources of information and tools for mobilization, particularly regarding political and social issues? To what extent are such mobilization tools available without government restriction? (0-6 points)**

- To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?
- To what extent are online communication tools or social networking sites (e.g. Twitter, Facebook) used as a means to organize politically, including for “real-life” activities?
- Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?

## **C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)**

**1. To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)**

- Does the constitution contain language that provides for freedom of speech and of the press generally?
- Are there laws or legal decisions that specifically protect online modes of expression?
- Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?
- Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?
- Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?

**2. Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)**

- Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an email, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)
- Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?
- Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?

- Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?
- Are there penalties for libeling officials or the state in online content?
- Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. “libel tourism”)?

**3. Are individuals detained, prosecuted, or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)**

- Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?
- Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via email or text messages?
- Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?
- Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?
- Are penalties for “irresponsible journalism” or “rumor mongering” applied widely?
- Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of “libel tourism”)?

**4. Does the government place restrictions on anonymous communication or require user registration? (0-4 points)**

- Are website owners, bloggers, or users in general required to register with the government?
- Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?
- Are users prohibited from using encryption software to protect their communications?
- Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?

**5. To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)**

- Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of email and mobile text messages?
- To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?
- Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?

- Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?
- Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?

**6. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)**

Note: Each of the following access providers are scored separately:

**6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)**

**6b. Cybercafes and other business entities that allow public internet access (0-2 points)**

**6c. Mobile phone companies (0-2 points)**

- Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?
- Are access providers prosecuted for not doing so?
- Does the state attempt to control access providers through less formal methods, such as codes of conduct?
- Can the government obtain information about users without a legal process?

**7. Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)**

- Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?
- Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?
- Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?
- Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?

**8. Are websites, governmental and private entities, ICT users, or service providers subject to widespread “technical violence,” including cyberattacks, hacking, and other malicious threats? (0-3 points)**

- Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyberespionage, data gathering, DDoS attacks), including those originating from outside of the country?
- Have websites belonging to opposition or civil society groups within the country’s boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?

# FREEDOM ON THE NET 2018



- Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?
- Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by nonstate actors from within the country's borders) and are they enforced?