Questions and Answers: Turkey's Control of the Internet and the Upcoming Election

1. What International human rights laws and obligations apply to Turkey?
2. What is Turkey's human rights record?
3. What role are social media platforms and messaging apps likely to play in Turkey's elections?
4. How does the government seek to control online discussion?
5. What might the government do to target anonymous online speech and private messages during the election?
6. What power does the government have to block content on the Internet?
7. How can the government sanction social media or messaging platforms for refusing its demands?
8. What other tech-facilitated challenges to human rights might Turkish voters face during this election?
9. What might happen on election day?
10. What human rights responsibilities do social media and messaging platforms have?
11. Have social media and messaging platforms met with their human rights responsibilities in previous elections?
12. What are online platforms doing to protect human rights during the election?
13. What else should social media platforms and messaging apps be doing to respect the right to participate in the election?
14. What human rights responsibilities do internet service providers have?

On May 14, voters in Turkey will vote in a high stakes parliamentary and presidential election that poses a significant challenge to President Recep Tayyip Erdoğan and his Justice and Development Party (AKP), who have been in office since 2002. The election will take place in an environment of intensified centralized control and erosion of fundamental rights and the rule of law, with the Erdoğan government wielding its formidable powers to muzzle media and detain or sideline perceived critics and political opponents.

The online environment plays an important role in Turkish political discourse. The Turkish government has equipped itself with a vast arsenal of digital censorship tools that it has repeatedly used to silence dissenting views online. Over the past nine years, there have been thousands of prosecutions of journalists, political opponents, and others for criticizing the president and the government online or even just sharing or liking critical articles on social media. The government also frequently blocks websites critical of the ruling party or individual ministers. As of December 2021, over half a million domains had been blocked. Social media platforms that reject government demands for user data or content removal could face hefty fines or bandwidth restrictions that would render their platforms effectively unusable in Turkey. The Turkish government has a well-established track record of temporarily throttling access to

popular social media networks at times of political unrest or when it anticipates criticism, as it did in the aftermath of the devastating February 2023 earthquakes.

In addition, networks of fake and compromised accounts can significantly influence Turkish online discussions and are often orchestrated to amplify the reach of political messages. Many of these coordinated networks of social media and messaging accounts are dedicated to advancing pro-AKP views. The government itself has at times pointed to the artificial presence that these networks create as "proof" of grassroots support for its policies and perspectives. These networks are also sometimes used to harass government critics and particularly women politicians and journalists.

In this vote, President Erdoğan and the AKP face one of their most significant electoral challenges since taking office. As election day approaches there is concern the government will exert its considerable control over the digital ecosystem to shape the outcome of the election. Government officials have already begun challenging the integrity of the elections, labelling any future AKP electoral loss a "political coup".

This Q and A examines possible threats to Turkey's online environment in the 2023 parliamentary and presidential elections. Any future Turkish government should reassess its legal framework and ensure it is compliant with its human rights obligations. ARTICLE 19 and Human Rights Watch also urge Turkish authorities to end the crackdown on civil society and ensure the right to freedom of expression and privacy especially in the run up to and during elections.

1. What International human rights laws and obligations apply to Turkey?

Turkey is subject to human rights obligations under regional and international human rights instruments and as a party to these conventions is obliged to conduct elections fairly and freely, including by ensuring that people are able to vote without undue influence or coercion. It is also obligated to secure other rights that are of particular relevance during elections, such as the right to freedom of expression and privacy.

Turkey is party to the Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights) as well as its First additional Protocol, the International Covenant on Civil and Political Rights, the International Convention on the Elimination of All Forms of Discrimination Against Women, the International Convention on the Elimination of All Forms of Racial Discrimination, and the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, among others.

2. What is Turkey's human rights record?

The Turkish government's respect for human rights has sharply declined since the 2013 Gezi Park protests. Successive Erdoğan-led governments have eviscerated most mainstream independent media and created an authoritarian and highly centralized system under an executive presidency that wields control over the courts, has hollowed out public institutions and greatly reduced the role of parliament. Turkey has demonstrated a willingness to flout international law,

rejecting binding judgments of the European Court of Human Rights. It has also withdrawn from the Istanbul Convention, a key mechanism to combat violence against women.

Turkey's regression on human rights and the rule of law more generally has impacted the exercise of the right to free and fair elections in the country. International election observers have concluded that President Erdoğan and the ruling AKP have enjoyed an undue advantage in numerous past elections, while Turkey's recent 2019 municipal elections demonstrated a stark disregard for basic democratic principles. Demonstrating its lack of independence, Turkey's election authority, the Supreme Election Council (YSK), cancelled the 2019 Istanbul mayoral elections after Erdoğan and the AKP claimed that opposition candidate Ekrem İmamoğlu's electoral victory was marred by irregularities. The YSK and Ministry of Interior also denied mayoral mandates in a manner that was incompatible with basic principles of democracy and rule of law to additional opposition candidates who won elections. And in the mainly Kurdish southeastern part of Turkey, Erdoğan's government fully suspended local democracy by removing the duly elected People's Democratic Party (HDP) mayors and imposing Ankara-appointed trustees to run the municipalities instead.

3. **What role are social media platforms and messaging apps likely to play in Turkey's elections?**

Social media is one of the last means through which people have access to independent news and can express themselves with relative freedom after the broad crackdown on media in Turkey. This is despite Turkey's increasingly restrictive legal framework, which permits arbitrary blocking and removing of websites and other online content.

Online platforms are playing an especially important role during this election as 90 percent of Turkish nation-wide traditional media is closely aligned with the government and provides disproportionate coverage of President Erdoğan and the ruling party's campaign. As a result, opposition parties rely heavily on the Internet to reach voters. The AKP and President Erdoğan himself also view online platforms as important and have experimented with various techniques to ensure their messages circulate online. In 2013, in the wake of the Gezi Park protests, the government reportedly hired a 6,000-person social media team to counter online critics and in 2020 Twitter removed a large coordinated network of pro-AKP accounts it attributed to the Party's youth wing for violating Twitter's policy against platform manipulation.

Turkey's population is also very active on social media. In past Turkish elections, social media has played an important role in drawing attention to allegations of voting irregularities in an atmosphere where traditional media and national election authorities lack independence.

4. **How does the government seek to control online discussion?**

The Turkish government has exercised extensive control over online discussions as part of a broader campaign of repression against opposing views that has targeted civil society, journalists, human rights defenders and others, including for their online activities. The government significantly expanded its online censorship toolkit with a series of legislative amendments passed in October 2022, in the lead-up to this election.

Thousands of people in Turkey face criminal prosecutions for their social media postings, or even for liking or sharing content. Turkey's use of its vague and widely drawn terrorism laws to stifle political dissent is also well documented.

Turkey consistently ranks among the top countries in the world in terms of the volume of content removal requests sent to Twitter. In 2021, the government convicted opposition MP Ömer Faruk Gergerlioğlu and then expelled him from parliament simply for sharing a news story on Twitter.

The October 2022 legislation further outlaws dissent, by criminalizing the public dissemination of "false information intended to cause anxiety, fear, or panic ... in a way likely to damage the public peace," including on social media. Human rights experts have pointed out that these terms are vague and broad, while courts and regulators in Turkey lack the independence necessary to prevent the government from using these vague provisions to silence opposing voices. Preventing "damage" or "disturbance" to "public peace" without reference to an imminent threat is problematic, and particularly with the Turkish government's track record of using these types of laws to target critics is not a legitimate basis to restrict freedom of expression.

The UN, OSCE, and OAS freedom of expression mandates have also jointly denounced the adoption of general or ambiguous laws on false information, underscoring the increased likelihood such laws will be misused to curtail rights during elections.

5. **What might the government do to target anonymous online speech and private messages during the election?**

The Turkish government has been increasing its surveillance of online activity in recent years. For example, Turkish government requests for user data to Meta have grown significantly since 2018 and Turkey is now consistently among the top 10 sources of user data requests in the world. And last year, it was reported that Turkey's Internet regulator, BTK, reportedly began indiscriminately collecting private data on all Turkish Internet and mobile subscribers in 2019.

Under the Government's October 2022 law, social media platforms are obligated to identify users accused of certain crimes (including the new "false information" offence) and share user data with courts and prosecutors at request, putting even individuals or organizations behind anonymously run accounts at risk for voicing criticism of the government during the election.

The law also obligates social media companies to proactively report any content that "endangers security of life or property" and provide information on users who posted this content. As this term is also left vague and undefined, it is not clear what categories of content posting platforms will be pressured to proactively monitor and disclose to Turkish officials and lends itself to an overly broad interpretation. Forcing companies to proactively monitor what users post on their platforms and report allegedly problematic content raises serious human rights concerns, both for freedom of expression and for privacy. It is also not clear in which situations companies will be considered to have become aware of such content but failed to disclose it. Criminalizing speech for "endangering the security of property" can be easily misused to target even generalized threats of minor property damage and to stifle peaceful protests.

The October 2022 amendments package also raises concerns about the future security of some private messaging services. Under these amendments, messaging services are now required to establish companies in Turkey and operate under a license that must be obtained from BTK. BTK will introduce secondary regulations that spell out the liabilities of messaging apps under which various communication companies might be required to intercept, access, or disclose private communications. Some private messaging services, such as WhatsApp, Signal, and Telegram Secret Chat, use end-to-end encryption so that only senders and recipients can read exchanged messages. It is not possible for anyone, including messaging companies, to access users' end-to-end encrypted content in intelligible form without severely undermining the security of all private messages. If BTK regulations require access to private messages on these services, it will undermine a key cybersecurity tool while exposing users to Turkey's broader campaign against opposing voices.

These measures collectively pose a serious threat to anonymity and secure communications, which are integrally linked to the ability to voice dissent online. BTK should ensure its lawful intercept regulations preserve end-to-end encryption and the Turkish government's surveillance capabilities should protect online anonymity.

6. What power does the government have to block content on the Internet?

The Turkish government also has a number of powers it can use to order the removal of online statements and the blocking of websites and even entire platforms. The government frequently uses these powers in politically sensitive times such as during protests or around elections.

Turkey can order Internet Service Providers to block or severely slow down access to social media and other websites. The UN Office of the High Commissioner of Human Rights has noted that intentional disruptions of Internet services are "powerful markers of deteriorating human rights situations" and the UN Human Rights Committee has noted in its General Comment No 34 on the ICCPR that generic bans on the operations of certain Internet sites and systems are incompatible with human rights.

Turkey has made extensive use of this power to render critical websites inaccessible. On a number of occasions, entire platforms have been blocked on the basis of a small number of items that allegedly violated Turkish law. For example, it blocked access to Wikipedia for a period of three years, citing threats to national security. As of December 2021, Turkey had blocked more than 570,000 domains.

Under Turkish law, platforms that do not remove user content in response to court orders or demands from BTK could become liable for any damages caused by the content. The October 2022 amendments further equip BTK with new powers to implement censorship on platforms through a series of heavy-handed compliance measures.

Online news sites also face arbitrary rules under Turkey's regulatory regimes, and can be ordered to remove news reporting and publish corrections on their home pages. Online news broadcasters and digital streaming platforms are obliged to apply for licenses from Turkey's government-aligned broadcasting watchdog, the Radio and Television Supreme Council (RTÜK), notorious

for imposing arbitrary fines and even ordering the temporary suspension of broadcasts of the few television channels critical of the government. Both Deutsche Welle and Voice of America have had their online news sites blocked by court order in Turkey because they chose not to apply for licenses from the broadcasting watchdog on the grounds that they did not want to submit to its censorship regime.

How can the government sanction social media or messaging platforms for refusing its demands?

The Turkish government has introduced a swath of compliance measures it can take against online platforms that refuse its content removal and data disclosure demands. With these powers in place, the government can apply significant pressure on social media platforms to ensure its demands are met, including where these demands are inconsistent with human rights.

Under Turkish law, social media platforms can face advertising bans, fines reaching up to 3 percent of global revenues, and bandwidth reductions ("throttling") that greatly slow down access to their services or render them effectively non-functional on Turkish networks if they fail to comply with content removal requests. Non-compliance with requests to hand over user data also opens social media platforms to possible throttling.

Social media platforms with large followings are also obligated to establish a national subsidiary or appoint a natural Turkish citizen who resides in Turkey as local representative. The Turkish government can apply direct pressure to national entities, including with threats of severe administrative fines and even criminal liability.

This expanded toolkit is particularly concerning in light of the government's demonstrated willingness to threaten platforms. In 2014, in the lead-up to local elections, President Erdoğan threatened to "eradicate" Twitter and ordered the platform to be blocked within Turkey for failing to abide by court orders to remove content on its platform. And in 2020, the head of Erdoğan's communications ministry, Fahrettin Altun threatened Twitter for removing a large network of government-aligned fake and compromised accounts.

Most platforms have policies in place to review and assess legally binding demands – including for their human rights implications - before complying. But with the above-described measures, social media companies can face serious informal pressure to moderate content in a manner that favors the ruling AKP and risk having access to their platforms blocked at critical points in the voting cycle if they resist this pressure.

7. **What other tech-facilitated challenges to human rights might Turkish voters face during this election?**

Social media users in Turkey face additional threats when participating in online political discourse. Incitement of violence and online harassment of government critics are common, and in particular gender-based attacks against [women and LGBT+] journalists and politicians. Turkish journalists, and particular women and LGBT+ journalists, are also frequently targeted with harassment campaigns by online accounts and particularly those critical of the government. This politically motivated targeting sometimes relies on government-aligned online influencers

or coordination techniques and networks to amplify the volume and reach of harassing comments.

The use of large networks of fake or compromised accounts to amplify political views or spread false information on social media is an increasingly common feature of digital political discourse in Turkey and has become particularly prevalent during politically sensitive periods, including elections.

Researchers have documented vast networks of bots and trolls that coordinate their messaging in an attempt to inundate online discussions with pro-AKP perspectives.

In 2020, Twitter removed over 7,000 accounts attributed to the youth wing of the AKP and responsible for over 37 million tweets creating the false impression of grassroots support for government policies, promoting AKP perspectives, and criticizing its opponents. Many of these accounts were fake while others were accounts of real individuals that had been compromised and were controlled by AKP supporters and the network. These tactics violated Twitter's policy on platform manipulation. The Turkish government has often pointed to the output of such accounts as proof of grassroots support for its policies and perspectives, and it decried Twitter's removal of the network of pro-AKP bot and troll accounts as an attack on a "popular political movement."

According to a study by the Stanford Internet Observatory, this coordinated network was prolific during Turkey's 2017 constitutional referendum, where it supported Erdoğan's attempt to centralize and consolidate power in the office of the president, and the network also previously had rallied against opposition parties during the 2015 parliamentary elections.

More recently, a study published in *ACM Web Conference 2023* identified Turkey as one of the most active countries for bot networks on Twitter. It remains difficult to attribute these accounts to specific parties or to the government itself, but the study found that many of these networks were pushing political slogans representative of a manipulation campaign in the lead-up to the 2023 election. In addition to these re-activated bots, the main opposition presidential candidate Kemal Kılıçdaroğlu warned about a threat regarding the circulation of algorithmically fabricated audio or video clips aimed at discrediting him.

The OAS, OSCE and UN mandates on free expression have jointly issued voiced their alarm regarding attempts to subvert the election process through the use of coordinated inauthentic behavior to circulate manipulative propaganda while independent election monitoring bodies have repeatedly warned that AKP is prone to misusing government resources to gain an outsized advantage during elections.

8. What might happen on election day?

The online environment may take on heightened importance on election day and in the immediate aftermath. The Turkish government has a well-established track record of exercising its array of website blocking and throttling capabilities when it anticipates criticism or at times of political sensitivity including during elections.

Given the Turkish government's control over traditional media and over the YSK, civil society groups such as Oy ve Ötesi (Vote and Beyond) work with political parties and tens of thousands of volunteers to provide critical vote monitoring functions. These include documenting voting irregularities as well as confirming election results by conducting an independent ballot count.

Access to timely and accurate results from independent sources such as Oy ve Ötesi (Vote and Beyond) can be critical. In the past, official sources such as Turkey's state-run Anadolu Agency have been accused of manipulation by, for example, publishing government-aligned results and claiming early victory before counting was complete.

Civil society organizations, opposition parties, and volunteers rely heavily on social media to disseminate voting results based on their monitoring activities and on digital tools to identify and investigate voting irregularities.

The Turkish government has equipped itself with multiple powers that it can use as a pretext to throttle any social media platform and render it unusable. Such steps could be taken during elections with the ulterior motive of limiting the right to information and independent news online. If election results are contested during election day or in its aftermath, the government may use its full array of censorship powers—and particularly its "spreading false information offence"—to prevent independent groups from challenging results that favor the ruling party. Social media companies may face intense pressure to remove content the government views unfavorably including assessments from independent monitors.

9. What human rights responsibilities do social media and messaging platforms have?

Under the UN Guiding Principles on Business and Human Rights, companies have a responsibility to respect human rights. This requires them to avoid infringing on human rights and to take steps to address adverse human rights impacts that stem from their practices or operations and to provide for remediation of adverse human rights impacts directly linked to their operations, products or services. In the context of elections, social media and messaging platforms have the responsibility to address any aspects of their practices that contribute to the undermining of the right to participate in democratic elections, such as the spread of electoral disinformation, or that could incite violence. Actions that companies take should be in line with international human rights standards and conducted in a consistent, transparent and accountable manner.

10. Have social media and messaging platforms met with their human rights responsibilities in previous elections?

Social media and messaging platforms have come under scrutiny in recent years for failing to address the use of their platforms to undermine participation in democratic elections, such as the circulation of calls seeking to delegitimize the outcome of an election and incitement to violence during election periods. In addition to underinvesting in the resources needed to properly understand and address these challenges, some social media platforms have also provided tools that can contribute to the undermining of democratic elections. These include platform features such as engagement-driven recommendation algorithms that can prioritize and amplify

misinformation, divisive content, and incitement to violence. They also include political ads whose targeting techniques are inherently opaque, making it impossible to independently conclude whether or not their targeting was discriminatory or whether it excluded potential voters by relying directly or indirectly on sensitive data.

11. What are online platforms doing to protect human rights during the election?

In response to public pressure, in recent years some platforms and messaging apps have announced a number of steps they are taking to prepare for elections.

Meta and TikTok are the only companies that have announced specific measures they will be taking ahead of Turkey's elections. Meta, the parent company of Facebook, Instagram, and WhatsApp, says it will establish a Türkiye Elections Operations Center to bring together experts from the company's engineering, legal, research, and analysis teams to identify and respond to potential threats across its apps in real-time. Meta says its efforts will center around combating misinformation and false news, addressing viral messaging on WhatsApp, making political advertising more transparent, combating election interference, and focusing on so-called coordinated inauthentic behavior. Meta works with fact-checking partners in Turkey. In specific cases, Meta says it removes misinformation from Facebook and Instagram entirely when it could contribute to imminent violence, cause physical harm, or may be content intended to suppress voting, such as incorrect information about voting dates, locations, times, and methods. For all other types of misinformation, it focuses on slowing the spread so fewer people see it and directing people to information from authoritative sources.

TikTok says it prohibits misinformation about civic and electoral processes. Included under this policy is misinformation about how to vote, registering to vote, eligibility requirements of candidates, the processes to count ballots and certify elections, and the final outcome of an election. TikTok stated that it works with a fact-checking partner and launched its Türkiye Election Tracking Center for users who want to access election-related information. TikTok says it reduces the discoverability of unverified claims, including by redirecting search results or making such content ineligible for recommendation into anyone's For You feed. On election day, TikTok says it will cooperate with its fact checking partners to reduce the visibility of content that claims early victory without confirming the results by the relevant institutions and organizations. TikTok informed Human Rights Watch and ARTICLE 19 that it will add a banner pointing viewers to its election guide on content with unverifiable claims about voting or premature declarations of victory. It blocks use of the platform, or some of its features, for repeat offenders.

Twitter and YouTube have general policies around elections but have not released specific information on their efforts around Turkey's election.

Twitter's approach to elections focuses on elevating credible information, promoting safety on the platform, promoting transparency, and collaborating with partners. Twitter policies state that it prohibits the use of its services for the purpose of manipulating or interfering in elections or other civic processes. This includes posting or sharing content that may suppress participation or mislead people about when, where, or how to participate in a civic process. Twitter may label and reduce

the visibility of Tweets containing false or misleading information about civic processes in order to provide additional context. Severe or repeated violations of this policy by specific accounts may lead to permanent suspension.

YouTube says it removes policy-violative content, raises authoritative news sources, reduces the spread of election-related misinformation, and provide a range of resources for government officials, candidates, and civic organizations. YouTube's policy prohibits content that misleads people about the voting process (like when to vote), false claims around candidate eligibility, incitement to interfere with democratic processes, distribution of hacked material, and content that has been manipulated or doctored in a way that misleads users and may pose a serious risk of egregious harm. YouTube also prohibits content advancing false claims that widespread fraud, errors, or glitches in certain past elections, or claims that the certified results of those elections were false. This policy only applies to *past* elections in specified countries, of which Turkey is not one. Content violating this policy gets removed, and channels that have violated the policy three times will be terminated.

Telegram has no publicly available policy on its efforts to address and mitigate potential rights abuses around Turkey's elections or even general policies on disinformation or attacks on democracy. It has repeatedly failed to respond to requests from civil society organizations, including ARTICLE 19 and Human Rights Watch, to address human rights concerns about its services in other countries. Human Rights Watch and ARTICLE 19 wrote to Meta, Telegram, TikTok, Twitter, and YouTube on May 1 to inquire about the resources they have invested to protect human rights in the context of Turkey's elections. Meta provided a link to its newsroom post and only TikTok expanded on publicly available information. At the time of publication, Human Rights Watch and ARTICLE 19 have not received responses to our detailed questions from any of the other companies.

12. What else should social media platforms and messaging apps be doing to respect the right to participate in the election?

Turkey undoubtedly presents a challenging environment for social media platforms and messaging apps so companies need to adopt all necessary steps to respect human rights in Turkey. They should prioritize human rights even if it comes at the expense of profit losses – for example due to advertising bans

Despite the October 2022 amendments, companies should continue to resist pressure from authorities when responding to content removals and data access requests. This is particularly important for content shared by civil society which is crucial for election monitoring and the removal or blocking of which might have an adverse impact on election results. Companies should also be transparent regarding government takedown and data access requests and how they responded, whether it consists of proactive reporting of content and user data to law enforcement, and any other steps taken in compliance with Turkish law, particularly the October 2022 amendments.

A recent analysis by Rest of the World based on data disclosed to the independent transparency clearinghouse Lumen indicates that Twitter has complied with a higher volume of government

requests since Elon Musk took over in October 2022 and until April 2023. Twitter complied with a larger number of requests from Turkey than any other government in the world over that period. Additionally, Twitter is late in publishing its biannual transparency report and Lumen reported that as of April 15 Twitter has suspended its disclosure of government requests to the Lumen database and is reassessing its government request data sharing policies.

Twitter has also failed to label Turkey's state-run news agency, Anadolu Ajansi, as "state-affiliated" despite its longstanding policy of so labelling news sources that lack editorial independence due to government financial resources and direct or indirect political pressure. On election day, this account is expected to be a primary source of skewed voting results, including early claims of AKP victory as seen in previous elections and that may be heavily contested by independent monitoring bodies such as Oy ve Ötesi (Vote and Beyond), making the absence of a "state-affiliated" label one week away from voting day a concern.

Given the credible threat of having their applications and websites blocked, social media companies should establish a contingency plan to ensure the public has access to their platforms throughout the election period. They should also have clear plans in place for how to deal with competing claims of victory and electoral fraud in order to ensure that their platforms and services are not contributing to the spread of misinformation about the outcome and integrity of the process. Platforms should work with civil society organizations to guide their efforts.

Ahead of elections, and in between election cycles, companies should carry out rigorous human rights impact assessments for product and policy development and engage in ongoing assessment and reassessment and consult with civil society in a meaningful way.

Due to past use of coordinated pro-AKP bot and troll networks to shape public opinion in Turkey during political sensitive periods, such as around elections, platforms should also enforce their existing policies around "inauthentic behavior" and coordinate with one another, in a transparent manner, to address cross-platform manipulation.

Some companies' longstanding flawed policy choices can have particularly harmful effects during election periods. For example, many platforms, as a matter of policy or practice, make exceptions to their content policies for politicians and exempt them from their rules on disinformation and incitement to violence or hatred. Depending on the platform, violative content may stay online, or the powerful accounts that post them may not face the same penalties that ordinary users face. Platforms should address incitement to violence and efforts to undermine the legitimacy of Turkey's election, for example the spreading claims voter "fraud' without any credible information, and do not contain a label or link to authoritative information, especially from accounts of politicians and others with large followings.

Political and other leaders' speech can be more likely to incite violence or make the public believe disinformation than that of an ordinary user. Yet, platforms often do not consistently take steps to remove or limit the reach of inciting posts or label posts containing disinformation for violating content guidelines because they treat posts from political figures as inherently newsworthy or in the public interest. The public has a right to know what their elected officials and candidates are saying on matters of public interest, especially in the context of elections. But

an overall deference to politicians combined with a narrow interpretation of election integrity policies can allow politicians to get away with misrepresenting electoral information and undermining public trust in the election. In addition, under international freedom of expression standards on incitement, the position and influence of the speaker is one of the key factors courts have to consider if and when certain speech reaches the level of incitement to hatred. Social media companies therefore need to conduct a case-by-case human-rights based analysis when they moderate such content.

More generally, companies need to address their chronic underinvestment in user safety outside of North America and Western Europe. This includes publishing their election policies, terms of service, and community guidelines in Turkish; investing in rights-respecting moderation practices, both human and automated; and being transparent about where they are allocating resources and why, among other steps. Company staff should be accessible to ordinary as well as high-risk users, to help them address threats concerning the election on platforms and services. Shortcomings in investment can impede companies' ability to consistently apply their policies across all regions. The concerns about the impact of their data harvesting practices, their engagement-based recommender systems and the targeting and amplification techniques when it comes to political ads also remain unaddressed.

No company responded to Human Rights Watch and ARTICLE 19's request for information about how many content moderators, human rights, and policy experts they have working on Turkey and how they ensure the political independence of their staff and contractors. Only TikTok responded to way that it works with native Turkish, Kurdish and Arabic speakers to moderate content and detect local narratives that violate its policies.

13. What human rights responsibilities do internet service providers have?

Just like social media and messaging platforms, Internet service providers should respect human rights in line with the UN Guiding Principles on Business and Human Rights and take measures to avoid complicity in human rights abuses.

Intentionally shutting down or restricting access to the internet violates multiple human rights. When faced with shutdown, throttling, or blocking requests, internet service providers should take all feasible efforts to avoid or mitigate any unjustified measures, including by interpreting requests narrowly and imposing the least intrusive restrictions possible, and employing all lawful measures to challenge unwarranted disruptions of service. Providers should give customers advance notice of shutdowns and disclose the government's role, the scope of the shutdown, and legal basis for restricting networks and services.

For more reporting on technology and rights, please visit:
https://www.hrw.org/topic/technology-and-rights https://www.article19.org/issue/digital-rights/

For more reporting on Turkey, please visit:
https://www.hrw.org/europe/central-asia/turkey https://article19.org/region/turkey

For more information, please contact:

In Istanbul, Emma Sinclair-Webb (English, Turkish): +90-538-972-4486 (WhatsApp/Signal); or sinclae@hrw.org. Twitter: @esinclairwebb

In New York, Deborah Brown (English): +1-347-920-8978 (mobile); or brownd@hrw.org. Twitter: @deblebrown

In Berlin, Frederike Kaltheuner (English, German): +1-917-902-5851 (mobile); or kalthef@hrw.org. Twitter: @F_Kaltheuner

In Amsterdam, Katia Mierzejewska (English, Turkish): katiamierzejewska@article19.org

In London: Aga Maciejewska (English, Turkish): +44 7776 968113 (mobile); or agamaciejewska@article19.org. Twitter: @article19europe