

Comparison of indicators in the 2015 and 2017 Index methodology

This table is designed to help stakeholders view the 2015 Index methodology in comparison to the 2017 Index methodology. The left column contains the text of the indicators from the 2015 Index methodology, and the right column includes the revised indicators and elements for the 2017 methodology. The red text in the right column represents substantive additions we have made to an indicator or element.

We encourage stakeholders to review the following documents for additional detail on the changes we have made; they are available for download here:

- A “[Summary of Revisions](#)” made to the 2017 Index methodology
- The [2017 Index methodology](#), with research guidance, and definitions glossary

2015 Index Methodology	2017 Index Methodology
C: Commitment	G: Governance
C1. Policy and leadership A: Does the company make explicit, prominent, and clearly articulated policy commitment to human rights including freedom of expression and privacy? <i>Answer categories (select one):</i> <ol style="list-style-type: none">1. Yes2. No B: Do senior executives of the company make meaningful commitment to advance users’ freedom of expression and privacy? <i>Answer categories (select one):</i> <ol style="list-style-type: none">1. Executive-level comment: a senior executive has made statements in a prominent venue.	G1. Policy commitment The company should publicly commit to respect users’ human rights to freedom of expression and privacy. 1. Does the company make an explicit, clearly articulated policy commitment to human rights, including freedom of expression and privacy?

<ol style="list-style-type: none"> 2. Managerial-level comment: company managers or spokesperson(s) have made statements in a prominent venue. 3. no/insufficient evidence: company representatives have not made related statements in a prominent venue. 	
<p>C2. Governance and management oversight</p> <p>Is there oversight at board, executive, and management levels on how the company's policies and practices affect freedom of expression and privacy?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. Board-level oversight: A board committee has formal oversight over how company practices affect freedom of expression and privacy. 2. Executive-level responsibility: An executive-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy. 3. Management-level responsibility: A management-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy. 	<p>G2. Governance and management oversight</p> <p>The company's senior leadership should exercise oversight over how its policies and practices affect freedom of expression and privacy.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect freedom of expression and privacy? 2. Does the company clearly disclose that an executive-level committee, team, program, or officer oversees how company practices affect freedom of expression and privacy? 3. Does the company clearly disclose that a management-level committee, team, program, or officer oversees how company practices affect freedom of expression and privacy?
<p>C3. Internal implementation</p> <p>Does the company have mechanisms in place to implement its commitment to freedom of expression and privacy?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company provides employee training on freedom of expression and privacy issues. 2. The company maintains an employee whistleblower program. 	<p>G3. Internal implementation</p> <p>The company should have mechanisms in place to implement its commitments to freedom of expression and privacy within the company.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it provides employee training on freedom of expression and privacy issues? 2. Does the company clearly disclose that it maintains a whistleblower program through which employees can report concerns related to how the company treats its users' freedom of expression and privacy rights?

C4. Impact assessment

Does the company conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of their business impact freedom of expression and privacy?

Checklist elements (select all that apply):

1. The company examines laws affecting privacy and freedom of expression in jurisdictions where it operates and uses this analysis to inform company policies and practices.
2. The company regularly assesses free expression and privacy risks associated with existing products and services.
3. The company assesses free expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products or services or entry into new markets.
4. The company assesses free expression and privacy risks associated with the processes and mechanisms used to enforce its Terms of Service.
5. The company conducts in-depth due diligence wherever the company's risk assessments identify concerns.
6. Senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in strategic decision-making for the company.
7. The company conducts assessments on a regular schedule.
8. The company's assessment is assured by an external third party.
9. The external third party that assures the assessment is accredited to a relevant and reputable human rights standard by a credible organization.

G4. Impact assessment

The company should conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of its business impact freedom of expression and privacy.

Elements:

1. As part of its decision-making, does the company consider how laws affect freedom of expression and privacy in jurisdictions where it operates?
2. Does the company regularly assess freedom of expression and privacy risks associated with existing products and services?
3. Does the company assess freedom of expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, **or companies** or entry into new markets?
4. Does the company assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service (ToS)?
5. Does the company conduct **additional evaluation** wherever the company's risk assessments identify concerns?
6. Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
7. Does the company conduct assessments on a regular schedule?
8. Are the company's assessments assured by an external third party?
9. Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?

<p>C5. Stakeholder engagement</p> <p>Does the company engage with a range of stakeholders on freedom of expression and privacy issues?</p> <p>A. The company is a member of a multi-stakeholder initiative whose focus includes a commitment to upholding of freedom of expression and privacy based on international human rights principles.</p> <p>B. If not, does the company satisfy any of the following elements?</p> <ol style="list-style-type: none"> 1. The company is a member of an industry organization that engages with non-industry and non-governmental stakeholders on freedom of expression and privacy. 2. The company initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people directly and adversely impacted by the company's business. 	<p>G5. Stakeholder engagement</p> <p>The company should engage with a range of stakeholders on freedom of expression and privacy issues.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Is the company a member of a multi-stakeholder initiative whose focus includes a commitment to upholding of freedom of expression and privacy based on international human rights principles? 2. If the company is not a member of a multi-stakeholder initiative, is the company a member of an organization that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy? 3. If a company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly and adversely impacted by the company's business?
<p>C6. Remedy</p> <p>Does the company have grievance and remedy mechanisms?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company discloses its processes for receiving complaints or grievances. 2. The company lists the kinds of complaints it is prepared to respond to. 3. The company articulates its process for responding to complaints. 4. The company reports on the number of complaints received. 5. The company provides evidence that it is responding to complaints, including examples of outcomes. 	<p>G6. Remedy</p> <p>The company should have grievance and remedy mechanisms to address users' freedom of expression and privacy concerns.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose its processes for receiving complaints? 2. Does the company clearly disclose that its process includes complaints related to freedom of expression and privacy? 3. Does the company clearly disclose its process for responding to complaints? 4. Does the company report on the number of complaints received related to freedom of expression and privacy?

	5. Does the company provide clear evidence that it is responding to complaints?
F: Freedom of Expression	F: Freedom of Expression
F1. Availability of Terms of Service Are the company's Terms of Service freely available and easy to understand? <i>Checklist elements (select all that apply):</i> <ol style="list-style-type: none"> 1. Free: The company's terms of service (ToS) are easy to find and freely available without needing to sign up or subscribe. 2. Language: The ToS is available in the language(s) most commonly spoken by the company's users. 3. Easy to understand: The ToS are presented in an understandable manner. 	F1. Access to terms of service The company should offer terms of service that are easy to find and easy to understand. <i>Elements:</i> <ol style="list-style-type: none"> 1. Are the company's terms of service (ToS) easy to find? 2. Are the ToS available in the language(s) most commonly spoken by the company's users? 3. Are the ToS presented in an understandable manner?
F2. Terms of Service, notice and record of changes Does the company commit to provide meaningful notice and documentation to users when it changes its Terms of Service? <i>Checklist elements (select all that apply):</i> <ol style="list-style-type: none"> 1. The company discloses the method of direct notification to users (e.g., email, SMS, etc.). 2. The company discloses the timeframe within which it provides notification (e.g., two weeks prior to changes occurring). 3. The company maintains a public archive or change log. 	F2. Changes to terms of service The company should clearly disclose that it provides notice and documentation to users when it changes its terms of service. <i>Elements:</i> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it notifies users about changes to its terms of service? 2. Does the company clearly disclose how it will directly notify users of changes? 3. Does the company clearly disclose the timeframe within which it provides notification prior to changes coming into effect? 4. Does the company maintain a public archive or change log?
F3. Reasons for content restriction Does the company disclose whether it prohibits certain types of content or activities?	F3. Process for terms of service enforcement The company should clearly disclose the circumstances under which it may restrict content or user accounts .

<p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company explains what types of content or activities it does not permit. 2. The company explains its process for enforcing its rules. 3. The company provides examples to help the user understand what the rules are and how they are enforced. 	<p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose what types of content or activities it does not permit? 2. Does the company clearly disclose the reasons why it may restrict a user's account? 3. Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules? 4. Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules? 5. Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules? 6. Does the company clearly disclose its process for enforcing its rules? 7. Does the company provide clear examples to help the user understand what the rules are and how they are enforced?
<p>F4. Reasons for account or service restriction</p> <p>Does the company explain the circumstances under which it may restrict or deny users from accessing the service?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company explains the reason(s) why it may restrict a user's account. 2. The company explains why it may shut down or restrict service to a particular area or group of users (where applicable). 3. The company provides specific examples of situations that may trigger restriction or denial of service by the company. 	

F9. Data about Terms of Service enforcement

Does the company regularly publish information about the volume and nature of actions taken to enforce the company's own terms of service?

Checklist elements (select all that apply):

1. The company lists the number of accounts affected.
2. The company lists the number of pieces of content or URLs restricted.
3. The company lists the types of content restricted during the reporting period (e.g., hate speech, harassment, incitement to violence, sexually explicit content, etc.).
4. The company provides examples of why it took action in different types of cases.
5. The company reports this data at least once a year.
6. The data reported by the company can be exported as a structured data file.

F4. Data about terms of service enforcement

The company should **clearly disclose** and regularly publish data about the volume and nature of actions taken to restrict content or accounts that violate the company's rules.

Elements:

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

F6. Process for responding to third-party requests

Does the company publish information about its process for evaluating and responding to requests from governments and other third parties to restrict content or service?

Checklist elements (select all that apply):

1. The company explains its process for receiving and responding to non-judicial government requests.
2. The company explains its process for responding to court orders.
3. The company explains its process for responding to requests made by private parties.
4. The company explains its process for responding to requests from foreign jurisdictions.
5. The company's explanations include the legal basis under which it may comply.

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

The company should clearly disclose its process for responding to government requests (including judicial orders) and private requests to remove, filter, or restrict content or accounts.

Elements:

1. Does the company **clearly disclose** its process for responding to non-judicial government requests?
2. Does the company **clearly disclose** its process for responding to court orders?
3. Does the company **clearly disclose** its process for responding to **government** requests from foreign jurisdictions?
4. Does the company **clearly disclose** its process for responding to private requests?

<ol style="list-style-type: none"> 6. The company commits to carry out due diligence on requests before deciding how to respond. 7. The company's process commits to push back on unlawful requests. 8. The company provides guidance or examples of policy implementation. 	<ol style="list-style-type: none"> 5. Do the company's explanations clearly disclose the legal basis under which it may comply with government requests? 6. Do the company's explanations clearly disclose the basis under which it may comply with private requests? 7. Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond? 8. Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond? 9. Does the company commit to push back on inappropriate or overbroad requests made by governments? 10. Does the company commit to push back on inappropriate or overbroad private requests? 11. Does the company provide clear guidance or examples of implementation of its process of responding to government requests? 12. Does the company provide clear guidance or examples of implementation of its process of responding to private requests?
<p>F7. Data about government requests</p> <p>Does the company regularly publish data about government requests (including judicial orders) to remove, filter, or restrict content or access to service, plus data about the extent to which the company complies with such requests?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company breaks out the number of requests it receives by country. 2. The company lists the number of accounts affected. 3. The company lists the number of pieces of content or URLs affected. 	<p>F6. Data about government requests for content or account restriction</p> <p>The company should regularly publish data about government requests (including judicial orders) to remove, filter, or restrict content or accounts.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company break out the number of requests it receives by country? 2. Does the company list the number of accounts affected? 3. Does the company list the number of pieces of content or URLs affected?

<ol style="list-style-type: none"> 4. The company lists the types of subject matter associated with the requests it receives. 5. The company identifies the specific legal authority making the requests. 6. The company lists the number of requests it complied with. 7. The company either publishes the original requests or provides copies to a third-party archive such as Chilling Effects or a similar organization. 8. The company reports this data at least once a year. 9. The data reported by the company can be exported as a structured data file. 	<ol style="list-style-type: none"> 4. Does the company list the types of subject matter associated with the requests it receives? 5. Does the company list the number of requests that come from different legal authorities? 6. Does the company list the number of requests it receives from government officials to restrict content or accounts through unofficial processes? 7. Does the company list the number of requests with which it complied? 8. Does the company publish the original requests or disclose that it provides copies to a public third-party archive? 9. Does the company report this data at least once a year? 10. Can the data data be exported as a structured data file?
<p>F8. Data about private requests</p> <p>Does the company regularly publish data about requests from non-governmental (and non-judicial) parties to remove, filter, or restrict access to content, plus data about the extent to which the company complies with such requests?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company breaks out the number of requests it receives by country. 2. The company lists the number of accounts affected. 3. The company lists the number of pieces of content or URLs affected. 4. The company lists the reasons for removal associated with the requests it receives (e.g., copyright violation, hate speech, incitement to violence, child abuse images, etc.). 5. The company describes the types of parties from which it receives requests (e.g. requests made under a notice-and-takedown system, requests from a non-governmental organization, requests from a voluntary industry self-regulatory body, etc.). 6. The company lists the number of requests it complied with. 	<p>F7. Data about private requests for content or account restriction</p> <p>The company should regularly publish data about private requests to remove, filter, or restrict access to content or accounts.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company break out the number of requests it receives by country? 2. Does the company list the number of accounts affected? 3. Does the company list the number of pieces of content or URLs affected? 4. Does the company list the reasons for removal associated with the requests it receives? 5. Does the company describe the types of parties from which it receives requests? 6. Does the company list the number of requests it complied with? 7. Does the company publish the original requests or provide copies to a public third-party archive? 8. Does the company report this data at least once a year? 9. Can the data reported be exported as a structured data file?

<p>7. The company either publishes the original requests or provides copies to a third-party archive such as Chilling Effects or a similar organization.</p> <p>8. The company reports this data at least once a year.</p> <p>9. The data reported by the company can be exported as a structured data file.</p>	<p>10. Does the company clearly disclose that its reporting covers all types of private requests that it receives?</p>
<p>F5. Notify users of restriction</p> <p>If the company restricts content or access, does it disclose how it notifies users?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. If the company hosts user-generated content, the company commits to notify users who generated the content when it is restricted. 2. The company commits to notify users who attempt to access content that has been restricted. 3. In its notification, the company includes an explanation of the basis for the content restriction (legal or otherwise). 4. The company commits to notify users when it restricts access to the service. 	<p>F8. User notification about content and account restriction</p> <p>The company should clearly disclose that it notifies users when it restricts content or accounts.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. If the company hosts user-generated content, does the company clearly disclose that it notifies users who generated the content when it is restricted? 2. Does the company clearly disclose that it notifies users who attempt to access content that has been restricted? 3. In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)? 4. Does the company clearly disclose that it notifies users when it restricts their account?
<p>F10. Network management (telecommunications companies)</p> <p>Does the company disclose whether it prioritizes or degrades transmission or delivery of different types of content (e.g., traffic shaping or throttling) and if so, for what purpose?</p> <p><i>Answer categories (select one)</i></p> <ol style="list-style-type: none"> 1. The company discloses that it does not prioritize or degrade the delivery of content. 2. The company discloses that it prioritizes or degrades content delivery and the purpose of doing so. 	<p>F9. Network management (telecommunications companies)</p> <p>The company should clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?

<ol style="list-style-type: none"> 3. The company discloses that it prioritizes or degrades content delivery but doesn't explain the purpose. 4. The company does not disclose information about prioritizing or degrading the delivery of content. 	<ol style="list-style-type: none"> 2. If the company does engage in these practices, does it clearly disclose its purpose for doing so?
	<p>F10. Network shutdown (telecommunications companies)</p> <p>The company should clearly explain the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly explain why it may shut down service to a particular area or group of users? 2. Does the company clearly explain why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users? 3. Does the company clearly explain its process for responding to requests to shut down a network or restrict access to a service? 4. Does the company commit to push back on requests to shut down a network or restrict access to a service? 5. Does the company clearly disclose that it notifies users directly when it shuts down the network or restricts access to a service? 6. Does the company list the number of network shutdown requests it receives? 7. Does the company provide specific examples of situations that may trigger shutdowns or restriction of service by the company?
<p>F11. Identity policy (Internet companies)</p>	<p>F11. Identity policy</p> <p>The company should not require users to verify their identity with their government-issued identification, or other forms of identification that could be connected to their offline identity.</p>

<p>Does the company require users to verify their identity with government-issued identification, or with other forms of identification connected to their offline identity?</p> <p><i>Answer categories (select one):</i></p> <ol style="list-style-type: none"> No Yes 	<ol style="list-style-type: none"> Does the company require users to verify their identity with government-issued identification, or with other forms of identification connected to their government-issued identity?
P: Privacy	P: Privacy
<p>P1. Availability of Privacy Policies</p> <p>Are the company's privacy policies freely available and easy to understand?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> Free: The company's privacy policies are easy to find and freely available without needing to sign up or subscribe. Language: The privacy policies are available in the language(s) most commonly spoken by the company's users. Easy-to-understand: The policies are presented in an understandable manner. 	<p>P1. Access to privacy policies</p> <p>The company should offer privacy policies that are easy to find and easy to understand.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> Are the company's privacy policies easy to find? Are the privacy policies available in the language(s) most commonly spoken by the company's users? Are the policies presented in an understandable manner? (For mobile ecosystems): Does the company require apps made available through its app store to provide users with a privacy policy?
<p>P2. Privacy Policies, notice and record of changes</p> <p>Does the company commit to provide meaningful notice and documentation to users when it changes its privacy policies?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> The company discloses the method of direct notification to users (e.g., email, SMS, etc.). The company discloses the time frame within which it provides notification (e.g., two weeks prior to changes occurring). The company maintains a public archive or change log. 	<p>P2. Changes to privacy policies</p> <p>The company should clearly disclose that it provides notice and documentation to users when it changes its privacy policies.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> Does the company clearly disclose that it notifies users about changes to its privacy policies? Does the company clearly disclose how it will directly notify users of changes?

	<ol style="list-style-type: none"> 3. Does the company clearly disclose the time frame within which it provides notification prior to changes coming into effect? 4. Does the company maintain a public archive or change log? 5. (For mobile ecosystems): Does the company clearly disclose that it requires apps sold through its app store to notify users when the app changes its privacy policy?
<p>P3. Collection of user information</p> <p>Does the company disclose what user information it collects, how it collects this information, and why?</p> <p>A. The company discloses that it collects no user information.</p> <p>B. If not, does the company satisfy any of the following elements?</p> <ol style="list-style-type: none"> 1. Data minimization: The company commits to limit collection of user information to what is directly relevant and necessary to accomplish the purpose of its service. 2. The company clearly discloses what user information it collects. 3. The company clearly discloses how it collects user information. 4. The company clearly discloses why it collects user information. 	<p>P3. Collection of user information</p> <p>The company should clearly disclose what user information it collects and how.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose what types of user information it collects? 2. For each type of user information the company collects, does the company clearly disclose how it collects that information? 3. Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service? 4. (For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose what user information the apps collect? 5. (For mobile ecosystems): Does the company clearly disclose that it evaluates whether third-party apps made available through its app store limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the app?

P4. Sharing of user information

Does the company disclose if and why it shares user information with third parties?

- A. The company discloses that it does not share user information.
- B. If not, does the company satisfy any of the following elements?
 - 1. The company clearly discloses what user information it shares.
 - 2. The company clearly discloses why it shares user information.
 - 3. The company provides a detailed description of the types of third parties with which it shares user information.
 - 4. The company discloses the names of all third parties with which it shares user information and explains what information it shares with each third party.
 - 5. If the company offers multiple services, it clearly discloses whether and how it will share user information between different services.

P4. Sharing of user information

The company should **clearly** disclose what user information it shares and with whom.

Elements:

- 1. **For each type of user information the company collects**, does the company clearly disclose whether it shares that user information?
- 2. **For each type of user information the company shares**, does the company **clearly disclose** the types of third parties with which it shares that user information?
- 3. **Does the company clearly disclose that it may share user information with government(s) or legal authorities?**
- 4. **For each type of user information the company shares**, does the company **clearly** disclose the names of all third parties with which it shares that user information?
- 5. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose what user information the apps share?**
- 6. **(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose the types of third parties with whom they share user information?**

P5. Purpose for collecting and sharing user information

The company should clearly disclose why it collects and shares user information.

Elements:

- 1. **For each type of user information the company collects**, does the company clearly disclose its purpose for collection?

	<ol style="list-style-type: none"> 2. Does the company clearly disclose its purpose for combining user information between other company services or services? 3. For each type of user information the company shares, does the company clearly disclose its purpose for sharing? 4. Does the company commit to limit its use of user information to the purpose for which it was collected?
<p>P7. Retention of user information</p> <p>Does the company disclose how long it retains user information?</p> <p>A. The company discloses that it does not retain user information.</p> <p>B. If not, does the company satisfy any of the following elements?</p> <ol style="list-style-type: none"> 1. The company discloses that it retains user information (not actively submitted by the user for the purpose of storage or publication) in an anonymized form. 2. The company discloses the types of user information it retains. 3. The company discloses how long it retains user information. 4. The company discloses that it deletes all user information after users terminate their account. 	<p>P6. Retention of user information</p> <p>The company should clearly disclose how long it retains user information.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. For each type of user information the company collects, does the company clearly disclose how long it retains that user information? 2. Does the company disclose what de-identified user information it retains? 3. Does the company clearly disclose the process for de-identifying user information? 4. Does the company clearly disclose that it deletes all user information after users terminate their account? 5. Does the company clearly disclose the time frame in which it will delete user information after users terminate their account? 6. (For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose how long they retain user information? 7. (For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose that all user information is deleted when users terminate their accounts or delete the app?

P5. User control over information collection and sharing

Does the company provide users with options to control the company's collection and sharing of their information?

Checklist elements (select all that apply):

1. The company provides users with options to control the company's collection of their information.
2. The company provides users with options to control the company's sharing of their information.

P7. Users' control over their own user information

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

Elements:

1. For each type of user information the company collects, does the company clearly disclose whether users can control the collection of their information?
2. For each type of user information the company collects, does the company clearly disclose whether users can delete this information?
3. Does the company clearly disclose that it provides users with options to control how their information is used to target advertising?
4. Does the company clearly disclose that targeted advertising is off by default?
5. (For mobile ecosystems): Does the company clearly disclose that it provide users with options to control the device's geolocation functions?

P6. Users' access to their own information

Are users able to view, download or otherwise obtain, in structured data formats, all of the information about them that the company holds?

Checklist elements (select all that apply):

1. The company allows users to view their data.
2. The company allows users to receive a copy of their data.
3. The data can be downloaded in a structured data format.
4. This data includes all public-facing and private information a company holds about a user.

P8. Users' access to their own user information

Companies should allow users to obtain all of their user information the company holds.

Elements:

1. Does the company clearly disclose that users can obtain a copy of their information?
2. Does the company clearly disclose what user information users can obtain?
3. Does the company clearly disclose that users can obtain their user information in a structured data format?

	<p>4. Does the company clearly disclose that users can obtain all public-facing and private information a company holds about them?</p> <p>5. (For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose that users can obtain all of the information about them the app holds?</p>
<p>P8. Collection of user information from third parties (Internet companies)</p> <p>Does the company publish clear information about whether it collects user information from third parties?</p> <p>A. The company discloses that it does not collect user information from third parties.</p> <p>B. If not, does the company satisfy any of the following elements?</p> <ol style="list-style-type: none"> 1. The company clearly explains how it may collect user information from third parties (e.g. use of a widget or advertising service). 2. The company clearly states how it uses the information it collects. 3. The company clearly states how long it retains information it collects. 4. The company respects user-generated signals (e.g. “Do Not Track” headers) to opt-out of data collection. 	<p>P9. Collection of user information from third parties (Internet companies)</p> <p>The company should clearly disclose its practices with regard to user information it collects from third-party websites or apps through technical means.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose what user information it collects from third-party websites through technical means? 2. Does the company clearly explain how it collects user information from third parties through technical means? 3. Does the company clearly disclose its purpose for collecting user information from third parties through technical means? 4. Does the company clearly disclose how long it retains user information it collects from third parties through technical means? 5. Does the company clearly disclose that it respects user-generated signals to opt-out of data collection?
<p>P9. Process for responding to third-party requests for user information</p>	<p>P10. Process for responding to third-party requests for user information</p> <p>The company should clearly disclose its process for responding to requests from governments and other third parties for user information.</p>

<p>Does the company publish information about its process for evaluating and responding to requests from government and other third parties for stored user data and/or real-time communications, including the legal basis for complying with such requests?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company explains its process for receiving and responding to non-judicial government requests. 2. The company explains its process for responding to court orders. 3. The company explains its process for responding to requests made by private parties. 4. The company explains its process for responding to requests from foreign jurisdictions. 5. The company's explanations include the legal basis under which it may comply. 6. The company commits to carry out due diligence on requests before deciding how to respond. 7. The company's process commits to push back on unlawful requests. 8. The company provides guidance or examples of policy implementation. 	<p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose its process for responding to non-judicial government requests? 2. Does the company clearly disclose its process for responding to court orders? 3. Does the company clearly disclose its process for responding to requests from foreign jurisdictions? 4. Does the company clearly disclose its process for responding to requests made by private parties? 5. Do the company's explanations clearly disclose the legal basis under which it may comply with government requests? 6. Do the company's explanations clearly disclose the basis under which it may comply with requests from private parties? 7. Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond? 8. Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond? 9. Does the company commit to push back on inappropriate or overbroad government requests? 10. Does the company commit to push back on inappropriate or overbroad private requests? 11. Does the company provide clear guidance or examples of implementation of its process for government requests? 12. Does the company provide clear guidance or examples of implementation of its process for private requests?
<p>P11. Data about third-party requests for user information</p> <p>Does the company regularly publish data about government and other third-party requests for user information, plus data about the extent to which the company complies with such requests?</p>	<p>P11. Data about third-party requests for user information</p> <p>The company should regularly publish data about government and other third-party requests for user information</p> <p><i>Elements:</i></p>

<p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company breaks out the number of user data and real-time communications access demands it receives by country. 2. The company lists the number of accounts affected. 3. The company lists whether a demand sought communications content or non-content (e.g., metadata, basic subscriber information, or non-content transactional data) or both. 4. The company identifies the specific legal authority or type of legal process through which law enforcement and national security demands are made. 5. The company includes requests that come from court orders or subpoenas (including civil cases). 6. The company includes other non-governmental requests. 7. The company lists the number of requests it complied with, broken down by category of demand. 8. The company lists what types of government requests it is prohibited by law from disclosing. 9. The company reports this data at least once per year. 10. The data reported by the company can be exported as a structured data file. 	<ol style="list-style-type: none"> 1. Does the company list the number of requests it receives by country? 2. Does the company list the number of requests it receives for stored user information and for real-time communications access? 3. Does the company list the number of accounts affected? 4. Does the company list whether a demand sought communications content or non-content or both? 5. Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made? 6. Does the company include requests that come from court orders? 7. Does the company list the number of requests it receives from private parties? 8. Does the company list the number of requests it complied with, broken down by category of demand? 9. Does the company list what types of government requests it is prohibited by law from disclosing? 10. Does the company report this data at least once per year? 11. Can the data reported by the company be exported as a structured data file?
<p>P10. User notification about third-party requests for user information</p> <p>Does the company commit to notify users to the extent legally possible when their data has been requested by governments and other third parties?</p> <p><i>Checklist elements (select all that apply):</i></p>	<p>P12. User notification about third-party requests for user information</p> <p>The company should notify users to the extent legally possible when their user information has been requested by governments and other third parties.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) request their user information?

<ol style="list-style-type: none"> 1. The company commits to notify users when government entities (including courts or other judicial bodies) request their user data. 2. The company commits to notify users when non-government entities request their user data. 3. The company discloses situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users. 	<ol style="list-style-type: none"> 2. Does the company clearly disclose that it notifies users when private parties request their user information? 3. Does the company clearly disclose situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users?
<p>P12. Security standards</p> <p>Does the company deploy industry standards of encryption and security for its products and services?</p> <p><i>Checklist elements (select all that apply):</i></p> <ol style="list-style-type: none"> 1. The company commits to keep up-to-date with the latest encryption and security standards and publishes evidence that it does so. 2. The company commits to address security vulnerabilities when they are discovered and publishes general information about how it does so. 3. The company discloses that it has systems in place to limit and monitor employee access to user information. 4. The company discloses that it regularly conducts security audits on its technologies and practices affecting user information. 5. The company discloses that the transmission of user communications is encrypted by default. 6. The company discloses that it deploys advanced authentication methods to prevent fraudulent access. 	<p>P13. Security oversight</p> <p>The company should clearly disclose information about its institutional processes to ensure the security of its products and services.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information? 2. Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services? 3. Does the company clearly disclose that it commissions third-party security audits on its products and services?
	<p>P14. Addressing security vulnerabilities</p> <p>The company should address security vulnerabilities when they are discovered.</p> <p><i>Elements:</i></p>

	<ol style="list-style-type: none"> 1. Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover? 2. Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities? 3. Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism? 4. (For mobile ecosystems) Does the company clearly disclose that software updates, security patches, add-ons, or extensions are downloaded over an encrypted channel? 5. (For mobile ecosystems and telecommunications companies) Does the company clearly disclose what, if any, modifications it has made to a mobile operating system? 6. (For mobile ecosystems and telecommunications companies) Does the company clearly disclose what, if any, effect such modifications have on the company's ability to send security updates to users? 7. (For mobile ecosystems) Does the company clearly disclose the date through which it will continue to provide security updates for the device/OS? 8. (For mobile ecosystems) Does the company commit to provide security updates for the operating system and other critical software for a minimum of five years after release? 9. (For mobile ecosystems and telecommunications companies) If the company uses an operating system adapted from an existing system, does the company commit to provide security patches within one month of a vulnerability being announced to the public?
	<p>P15. Data breaches</p> <p>The company should publicly disclose information about its processes for responding to data breaches.</p>

	<p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs? 2. Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach? 3. Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?
<p>P13. Encryption of users' private content (Internet companies)</p> <p>Can users encrypt their own content and thereby control who has access to it?</p> <p><i>Answer categories (select one):</i></p> <ol style="list-style-type: none"> 1. Private user content is encrypted by default; the company itself has no access. (100 points) 2. The company offers a built-in option to encrypt private content. (67 points) 3. The company's terms or other policies explain that the user may deploy third party encryption technologies. (33 points) 4. No disclosure. (0 points) 5. The company's terms or other policies prohibit encryption. (0 points) 	<p>P16. Encryption of user communication and private content (Internet, software, and device companies)</p> <p>The company should encrypt user communication and private content so users can control who has access to it.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that the transmission of user communications is encrypted by default? 2. Does the company disclose that transmissions of user communications are encrypted using unique keys? 3. Does the company clearly disclose that users can secure their content using end-to-end encryption? 4. Does the company clearly disclose that end-to-end encryption is enabled by default?
<p>P14. Inform and educate users about potential threats</p> <p>Does the company publish information to help users defend against cyber threats?</p> <p><i>Checklist elements (select all that apply):</i></p>	<p>P17. Account Security (Internet, software, and device companies)</p> <p>The company should help users keep their accounts secure.</p> <p><i>Elements:</i></p> <ol style="list-style-type: none"> 1. Does the company clearly disclose that it deploys advanced authentication methods to prevent fraudulent access? 2. Does the company clearly disclose that users can view their recent account activity?

<ol style="list-style-type: none"> 1. The company commits to inform users about unusual account activity, most recent account activity, and possible unauthorized access. 2. The company publishes practical materials that educate users on how to protect themselves from cyber threats relevant to their services. 	<ol style="list-style-type: none"> 3. Does the company clearly disclose that it notifies users about unusual account activity and possible unauthorized access to their account? <p>P18. Inform and educate users about potential risks</p> <p>The company should publish information to help users defend themselves against cyber risks.</p> <ol style="list-style-type: none"> 1. Does the company publish practical materials that educate users on how to protect themselves from cyber risks relevant to their products or services?
---	---