Organizational Rating

as of 2019-09-14

Source: https://rankingdigitalrights.org/wp-content/uploads/2018/09/2019RDRIndicators.pdf

1. **Access & changes to privacy policies**
    - 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 disclose that it requires apps made available through its app store to provide users with a privacy policy?
    - 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?
    - Does the company clearly disclose the time frame within which it provides notification prior to changes coming into effect?
    - Does the company maintain a public archive or change log?
    - (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?

2. **Sharing of information**
    - For each type of information the company collects, does the company clearly disclose whether it shares that information?
    - For each type of information the company shares, does the company clearly disclose the types of third parties with which it shares that information?
    - Does the company clearly disclose that it may share information with government(s) or legal authorities?
    - For each type of information the company shares, does the company clearly disclose the names of all third parties with which it shares information?
    - (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 information the apps share?
    - (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 information?

3. **Users' access to their own information**
    - Does the company clearly disclose that users can obtain a copy of their user information?
    - Does the company clearly disclose what user information users can obtain?
    - Does the company clearly disclose that users can obtain their user information in a structured data format?
    - Does the company clearly disclose that users can obtain all public-facing and private information a company holds about them?
    - (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?

4. **Collection of information from third parties**
    - Does the company clearly disclose what information it collects from third-party websites through technical means?
    - Does the company clearly explain how it collects information from third parties through technical means?
    - Does the company clearly disclose its purpose for collecting information from third parties through technical means?
    - Does the company clearly disclose how long it retains the information it collects from third parties through technical means?
    - Does the company clearly disclose that it respects user-generated signals to opt-out of data collection?

5. **Process for responding to third-party requests for information**
    - Does the company clearly disclose its process for responding to court orders, non-judicial government requests, government requests from foreign jurisdictions, or requests made by private parties?
    - Do the company's explanations clearly disclose the legal basis under which it may comply with government requests?
    - Do the company's explanations clearly disclose the basis under which it may comply with requests from private parties?
    - Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond?
    - Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?
    - Does the company commit to push back on inappropriate or overbroad government requests?
    - Does the company commit to push back on inappropriate or overbroad private requests?
    - Does the company provide clear guidance or examples of implementation of its process for government requests?
    - Does the company provide clear guidance or examples of implementation of its process for private requests?

6. **Data and user notification about third-party requests for information**
    - Does the company list the number of requests it receives by country?
    - Does the company list the number of requests it receives for stored user information and for real-time communications access?
    - Does the company list the number of accounts affected?
    - Does the company list whether a demand sought communications content or non-content or both?
    - Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?
    - Does the company include requests that come from court orders?
    - Does the company list the number of requests it receives from private parties?
    - Does the company list the number of requests it complied with, broken down by category of demand?
    - Does the company list what types of government requests it is prohibited by law from disclosing?
    - Does the company report this data at least once per year?
    - Can the data reported by the company be exported as a structured data file?
    - Does the company clearly disclose that it notifies users when government entities(including courts or other judicial bodies) request their user information?
    - Does the company clearly disclose that it notifies users when private parties request their user information?
    - 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?

7. **Security oversight and addressing security vulnerabilities**
    - Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information?
    - Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services?
    - Does the company clearly disclose that it commissions third-party security audits on its products and services?
    - Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?
    - Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities?
    - Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?
    - (For mobile ecosystems) Does the company clearly disclose that software updates, security patches, add-ons, or extensions are downloaded over an encrypted channel?
    - (For mobile ecosystems and telecommunications companies) Does the company clearly disclose what, if any, modifications it has made to a mobile operating system?

- (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?
- (For mobile ecosystems) Does the company clearly disclose the date through which itwill continue to provide security updates for the device/OS?
- (For mobile ecosystems) Does the company commit to provide security updates for theoperating system and other critical software for a minimum of five years after release?
- (Formobile 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?

8. Data breaches

- Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?
- Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?
- Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?