Through the looking glass: Analysing transparency reports

October 31, 2019

By **Torsha Sarkar**, **Suhan S** and **Gurshabad Grover**
Research assistance by **Keying Geng** and **Anjanaa Aravindan**
Edited by **Elonnai Hickok**

The Centre for Internet and Society, India

Table of contents

Introduction

Over the past decade, a few private online intermediaries, by rapid innovation and integration, have turned into regulators of a substantial amount of online speech.[1] Such concentrated power calls for a high level of responsibility on them to ensure that the rights of the users online, including their rights to free speech and privacy, are maintained.[2] Such responsibility may include appealing or refusing to entertain government requests that are technically or legally flawed, or resisting gag orders on requests.[3]

For the purposes of measuring a company's practices regarding refusing flawed requests and standing up for user rights, transparency reporting becomes useful and relevant. Making information regarding the same public also ensures that researchers can build upon such data and recommend ways to improve accountability and enables the user to understand information about when and how governments are restricting their rights.

For some time in the last decade, Google and Twitter were the only major online platforms that published half-yearly transparency reports documenting the number of content takedown and user information requests they received from law enforcement agencies.[4] In 2013 however, that changed, when the Snowden leaks revealed, amongst other things, that these companies were often excessively compliant with requests from US' intelligence operations, and allowed them backdoor surveillance access to user information.[5] Subsequently, all the major Silicon Valley internet companies have been attempting to publish a variance or other of transparency reports, in hopes of re-building their damaged goodwill[6], and displaying a measure of accountability to its users.

The number of government requests for user data and content removal has also seen a steady rise. In 2014, for instance Google noted that in the US alone, they observed a 19% rise for the second half of the year, and an overall 250% jump in numbers since Google

---

[1] Kate Klonic, "The New Governors: The People, Rules, and Processes Governing Online Speech" (2018) 131 Harv. L. Rev. <https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf> accessed 19 September 2019 [*hereinafter* Klonic, 2018]

[2] Article 19, "Side-stepping rights: Regulating speech by contract" (Policy Brief, 2018) <https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf> accessed 19 September 2019; *There are several civil society initiatives that seek to achieve this goal: for instance, see* Andrew Crocker, et. al, "Who Has Your Back? Censorship Edition 2019" (Electronic Freedom Foundation, 2019) <https://www.eff.org/wp/who-has-your-back-2019> accessed 19 Septmber 2019 [*hereinafter* Crocker et. al]; "The Santa Clara Principles On Transparency and Accountability in Content Moderation" (Santa Clara Principles, 2018) <https://santaclaraprinciples.org/> accessed 19 September 2019

[3] Id (Crocker, et al, 2019); Id (Article 19, 2018); Klonic, 2018 (n 1)

[4] Kashmir Hill, "Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government" (*Forbes*, 14 November 2013) <https://www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/#538ea6555365> accessed 19 September 2019

[5] Id.

[6] Id.

began providing this information.[7] As per a study done by Comparitech, India sent the maximum number of government requests for content removal and user data in the period of 2009 - 2018.[8] This highlights the increasing importance of accessible transparency reporting.

Initiatives analysing the transparency reporting practices of online platforms, like The Electronic Frontier Foundation (EFF)'s *Who Has Your Back?* reports, for instance, have developed a considerable body of work tracing these reporting practices, but have largely focused at them in the context of the United States (US).[9]

In our research, we found that the existing methodology and metrics to assess the transparency reports of online platforms developed by organisations like the EFF are not adequate in the Indian context. We identify two reasons for developing a new methodology:

1. Online platforms make available vastly different information for US and India. For instance, Facebook breaks up the legal requests it receives for US into eight different classes (search warrants, subpoenas, etc.). Such a classification is not present for India. These differences are summarised in Annexure 1.
2. The legal regimes and procedural safeguards under which states can compel platforms to share information or take content down also differ. For instance, in India, an order for content takedown can be issued either under section 79 and its allied rules or under section 69A and its rules, each having their own procedures and relevant authorities. A summary of such provisions for Indian agencies is given in Annexure 3.

These differences may merit differences in the methodology for research into understanding the reporting practices of these platforms, depending on each jurisdiction's legal context.

In this report, we would be analyzing the transparency reports of online platforms with a large Indian user-base, specifically focusing on data they publish about user information and takedown requests received from Indian governments' and courts.

First, we detail our methodology for this report, including how we selected platforms whose transparency reports we analyse, and then specific metrics relating to information available in those reports. For the latter, we collate relevant metrics from existing frameworks, and propose a standard that can be applicable for our research.

---

[7] Dominic Rushe, "Google: US government demands for user data have risen 250% since 2009" (*The Guardian*, 2014) <https://www.theguardian.com/technology/2014/sep/15/google-demands-user-data-rise> accessed 19 September 2019

[8] Paul Bischoff, "Which government censors the tech giants the most?" <https://www.comparitech.com/blog/vpn-privacy/tech-giant-censorship/> accessed on 22nd October 2019

[9] *See* Crocker, et al (n 2), *which also notes that it is focused on US policies, and how EFF is partnering with organisations to produce jurisdiction-specific reports.*

In the second part, we present company-specific reports. We identify general trends in the data published by the company, and then compare the available data to the best practices of transparency reporting that we proposed.

Methodology

Selection of online platforms

We base the selection of the companies, whose transparency reports would be scrutinized, on the "Top sites in India" list published Alexa,[10] which uses a combination of average daily visitors and pageviews to rank websites. Out of the top 20 of these websites, we have clubbed websites that constitute parts of the same intermediary. For example, we have chosen to include Google.in and Youtube.com as part of Google. Other than that.

- We have eliminated websites that do not seem to be serving any intermediary function qualifying for safe harbour protections, i.e. they do not seem to be dealing with user-generated content. These websites are:
    - State Bank of India
    - Indiatimes
    - HDFC Bank
    - ICICI Bank
    - Incometaxindiaefiling
- We eliminated companies that may be generating third-party content, but do not have any publicly-available transparency reporting documents. These websites are:
    - Hotstar
    - Stackoverflow
    - Netflix
    - Flipkart

The list of 20 websites, and the reasons for their inclusion or exclusion are summarised in Annexure 3. The intermediaries who have, by way of the above criteria, been within the scope of our report are:

1. Google
2. Facebook
3. Twitter
4. Amazon
5. Yahoo
6. Wikimedia Foundation

Only publicly available documents of these intermediaries are within the scope of our analysis. And, for purposes of uniformity, we would be examining the transparency reports of these intermediaries from 2014 onwards.

[10] "Top Sites in India", *Alexa* <https://www.alexa.com/topsites/countries/IN> accessed on 19 September 2019

For government requests to remove content

Several frameworks have been formulated in the last few years that provide a uniform framework for accountable reporting of numbers by online intermediaries. One of these is the Santa Clara Principles, developed in 2018 at the second *Content Moderation at Scale* conference at Washington, DC.[11] These principles since then, have received the support of as many as seventy human rights groups, including the Electronic Frontier Foundation (EFF) and Article 19, in their campaign to push Facebook to incorporate due process in their censorship procedures.[12] These principles, in a nutshell, require the intermediary to be accountable to its users on three broad fronts[13]:

- **Numbers**: Companies must publish the number of posts removed and accounts permanently or temporarily suspended due to violations of their content guidelines. As part of this obligation, companies must also identify the source of the flagger, which can be either a government request, or a trusted flagger.
- **Notice**: Companies must provide notice to each user whose content is taken down or account is suspended about the reason for the removal or suspension. As part of this obligation, where content has been flagged by the government, the company is mandated to reveal the same, as far as it is legally permissible.
- **Appeal**: Companies must provide a meaningful opportunity for timely appeal of any content removal or account suspension.

Notably, the scope of the Santa Clara Principles is broader than our research as it also includes transparency of platforms' actions when it comes to content moderation and enforcement of their own community guidelines. Nevertheless, we use elements of the framework that recommend actions that companies should take in relation to government requests for content removal.

Additionally, the EFF's 2018 *Who Has Your Back?* report[14] lays down five principles that an intermediary must include in their policy regarding content takedown requests issued by the government. They are:

- Transparency in legal takedown requests
- Transparency in platform policy takedown requests
- Meaningful notice
- Allowance of appeals
- Geographical scope of content blocking

For developing our methodology, we also incorporate elements from the EFF Framework.

---

[11] Santa Clara Principles (n 2)

[12] "An Open Letter to Mark Zuckerberg", Santa Clara Principles <https://santaclaraprinciples.org/open-letter/> accessed on 19 Septmber 2019

[13] Santa Clara Principles (n 2)

[14] Nate Cardozo, et al, "Who Has Your Back? Censorship Edition 2018" <https://www.eff.org/who-has-your-back-2018 accessed on 19 September 2019

Finally, the New America Transparency Reporting Toolkit: Content Takedown Reporting ["the Content Takedown Toolkit"], released in 2018, lays down some general best practices that an online intermediary must adhere to[15]. These are:

- Issuing regular reports on clearly demarcated reporting periods
- Issuing reports specific to the type of demand
- Reporting on types of demands using specific numbers
- Breaking down demands by country
- Reporting on categories of objectionable content targeted by demands
- Reporting on products targeted by demands
- Reporting on specific government agencies/parties that submitted demands
- Specifying which laws pertain to specific demands
- Reporting on the number of accounts and items specified in demands
- Reporting on the number of accounts and items impacted by demands
- Reporting on how the company responded to demands

For the purposes of our research, we would be analysing the transparency reports of the chosen intermediaries on the metrics of:

- **Numbers**: As the Santa Clara Principles and the Content Takedown Toolkit both indicate, the transparency report should contain the number of requests granted. We also believe that the report should also contain the number of requests received by them during one reporting period.
  Additionally, the current Indian legal regime provides for two ways in which public access to a particular content can be disabled: through the procedure under Section 69A of the Information Technology Act[16] ("the IT Act") and the corresponding blocking rules[17], or through the intermediary liability guidelines[18] issued under Section 79 of the IT Act[19]. Accordingly, the intermediary should also provide a numerical breakdown of the number of removal requests they receive from under Section 69A and those under Section 79. This is also in tune with the Content Takedown Toolkit's mandate of specifying the law pertaining to the specific request.
- **Sources**: The Santa Clara Principles recommend that the intermediary identify the source of the flagging. Under the intermediary liability regime in India, content takedown requests can be sent by the executive, the courts, or third parties.[20] We

---

[15] New America, "The Transparency Reporting Toolkit: Content Takedown Reporting" <https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/general-best-practices-for-content-takedown-reporting> accessed on 24 October 2019 ["the Content Takedown Toolkit"]

[16] Information Technology Act, 2000, s 69A

[17] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 [*hereinafter* IT Rules (Blocking) 2009]

[18] Information Technology (Intermediaries Guidelines) Rules, 2011

[19] Information Technology Act, 2000, s 79

[20] *Shreya Singhal v Union of India*, AIR 2015 SC 1523 . In that case, the court read down "actual knowledge" to mean a notice from the executive or the judiciary. However, third parties can send notices to intermediaries about copyright infringement. *See MySpace Inc. v Super Cassettes* Industries Ltd., FAO(OS) 540/2011; For

believe that transparency reports must classify the received requests into these three categories. This mandate is in tune with the Content Takedown Toolkit's mandate of reporting the specific government agency/party.

- **Items**: The intermediary should show the number of items taken down, in addition to the number of requests acted upon, since a single request may specify numerous items to be taken down.[21] An 'item' here refers to one particular piece of user content, (eg. a blog post. a video, etc.). This is in line with the recommendations in the Santa Clara Principles and the Content Takedown Toolkit.
- **Platforms**: For further accountability, we believe an intermediary owning or operating multiple platforms, should publish platform-wise breakdown of content taken down and data produced. Alternatively, they should publish separate transparency reports for each platform.
- **Notice**: As both the Santa Clara Principles and the methodology used by EFF in the *Who Has Your Back* reports emphasise, in the event of content being taken down, the owner/publisher of that item must be given a clear notice as to why the content was taken down. While this is not possible for requests received under the blocking rules under Section 69A of the IT Act because of a confidentiality clause,[22] they have the ability to do so for requests received under the intermediary liability rules issued under Section 79 of the IT Act.
- **Geographical Scope**: In tune with recommendations of EFF *Who Has Your Back* report , intermediaries should aim to remove the content only from the jurisdiction where it is deemed to violate the law. In the current study, content removed in India should be made available elsewhere.

For government data requests

The EFF's *Who has your back?* reports[23], have developed a detailed methodology over the years. According to their 2017 report, an intermediary's transparency reporting about government data requests should:

- **Follow industry-wide best practices**: In the context of the US, this means that the company must:
    - Have a public policy requiring the government to obtain a warrant from a judge before the company discloses the content of user communications.

---

analysis of the judgment, see Gautam Bhatia, "Online Speech and Intermediary Liability: The Delhi High Court's MySpace Judgment" (*Indian Constitutional Law and Philosophy*, 16 January 2017) <https://indconlawphil.wordpress.com/2017/01/16/online-speech-and-intermediary-liability-the-delhi-high-courts-myspace-judgment/> accessed on 19 September 2019; Anubha Sinha, "Super Cassettes v. MySpace (Redux)", (*Centre for Internet and Society*, 16 January 2017) <https://cis-india.org/a2k/blogs/super-cassettes-v-myspace> accessed on 19 September 2019

[21] Google, "Government requests to remove content" <https://transparencyreport.google.com/government-removals/overview?hl=en> accessed on 19 September 2019

[22] IT Rules (Blocking) 2009, r 16

[23] Electronic Freedom Foundation (EFF), "Who Has Your Back? EFF Surveys Major Tech Companies' Privacy and Transparency Policies" <https://www.eff.org/homepage-feature/who-has-your-back> accessed on 19 September 2019

    - Have published a transparency report in the last year, and the report includes useful data about how many times governments sought user data and how often the company provided user data to governments.
    - Have public, published law enforcement guides explaining how it responds to data demands from the government.
- **Tell users about government data requests**: The company must give prior notice to the user whose account data has been requested by the government, before acceding to the request.
- **Promise to not sell out users**: The company must have a public policy that ensures data is not flowing to the government outside of its law enforcement guidelines — for example, through voluntary contracts or via a third party vendor who sells data to the government.
- **Stand up to NSL gag orders**: National Security Letters (NSL) are administrative subpoenas to gather information, that usually come with a non-disclosure clause that forbids the company from disclosing the receipt of such a request.[24] By way of an amendment through the US FREEDOM Act, the receiver of NSL now have the prerogative of calling for a judicial review of such a request.[25] Accordingly, the EFF mandates that to earn a point in this category, the company must publicly undertake such an endeavour.
- **Pro-user public policy reform**: To earn credit in this category, the company must publicly support reforms to section 702 of Electronic Communications Privacy Act, thereby limiting the government's power to collect data.

Accordingly, for our framework, we would also be adopting some of their metrics, wherever it is appropriate. Details of our framework of analysis are given below:

- **Numbers**: The transparency report should contain both the numbers of requests received and the number of requests granted. Additionally, we believe the reporting must include the total number of user accounts against which such requests were made.
- **Sources**: There are several legal provisions that can allow the Government to request or access information held by intermediaries[26]:

---

[24] EFF, "National Security Letters" <https://www.eff.org/issues/national-security-letters> accessed on 19 September 2019

[25] Nate Cardozo, "Requiring Judicial Review for Every Gag Order Is a Simple Way to Have Our Backs: Apple Does but Google and Facebook Fall Short", (*EFF*, 10 July 2017) <https://www.eff.org/deeplinks/2017/07/requiring-judicial-review-every-gag-order-simple-way-have-our-backs-apple-does> accessed on 19 Septermber 2019

[26] Vipul Kharbanda, "Policy Paper on Surveillance in India" (*Centre for Internet and Society*, 3 August 2015) <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india> accessed on 19 September 2019; Rishab Bailey, et al, "Use of personal data by intelligence and law enforcement agencies" (*National Institute of Public Finance and Policy*, 1 August 2018) <https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed on 19 September 2019; "India's surveillance state: Other provisions of law that enable collection of user information" (*Software Freedom Law Centre*, 2 December 2015) <https://sflc.in/indias-surveillance-state-other-provisions-of-law-that-enable-collection-of-user-information> accessed on 19 September 2019

- Section 91 in the Code of Criminal Procedure (CrPC), 1973 empowers courts and police officers to call for any document if they deem it useful for a trial or investigation.[27]
- Section 69 of the IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["the interception rules"] permit the Government to compel any intermediary or person to assist with the interception and decryption of user information in any "computer resource."[28] Under these rules, emergency situations are also envisaged, were the legal requirements for seeking of information are different.[29] We believe as part of the transparency reporting, intermediaries must also represent the number of emergency requests it receives, separately from the normal legal requests under the interception rules.
- Section 69B of the IT Act allows governmental agencies to collect traffic and metadata for the purposes of cybersecurity.[30]
- Section 79 of the IT Act and the intermediary guidelines issued under it allow the Government to request information and/or assistance from an intermediary.[31]

We believe that the intermediary must represent the number of requests received by them under these laws separately.

- **Best practices**: In tune with the EFF's framework, the intermediary must have:
  - A publicly available document where they explain their review mechanism for each data request they receive. This relates to the substantive part of the request. For earning credit in this category, the intermediary must state, in clear terms, what the relevant law obligates the government to do. For instance, the interception rules mandate that the direction of interception must contain the reasons for such a direction and the name and designation of the officer to whom the information will be disclosed.[32] For earning credit in this category, the wording of the policy must be exact, with proper explanation on the identifiers the intermediary utilizes to determine the correctness of the request.
  - A publicly available policy that explicitly prohibits third-party applications from using information from the platform for enabling government surveillance. This is inline with the metric 'Promises Not to Sell Out Users' used by the *Who Has Your Back 2017* report.
- **Notification**: The intermediary must also undertake to notify the user of a request for their account data prior to granting such a request, unless the intermediary is expressly prohibited by law from doing so.

---

[27] Code of Criminal Procedure, 1973, s 91
[28] Information Technology Act, 2000, s 69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
[29] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r 3
[30] Information Technology Act, 2000, s 69B
[31] Information Technology Act, 2000, s 79; Information Technology (Intermediaries Guidelines) Rules, 2011, r 3(7)
[32] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 [*hereinafter* IT Rules (Interception) Rules 2009] r 7 & r 10

- **Platforms**: In the instance the company owns and operates more than one platform, there must be a numerical breakdown of the data requests platform-wise.

Analysis

In this section, we would be analyzing the existing transparency reports of the intermediaries identified in the methodology. We use the following markers to indicate compliance with each metric highlighted in the methodology:

✔: Complies ✖: Does not comply ✔: Partially complies

Facebook[33]

Facebook has been publishing transparency reports documenting content removal requests since the second half of 2013.

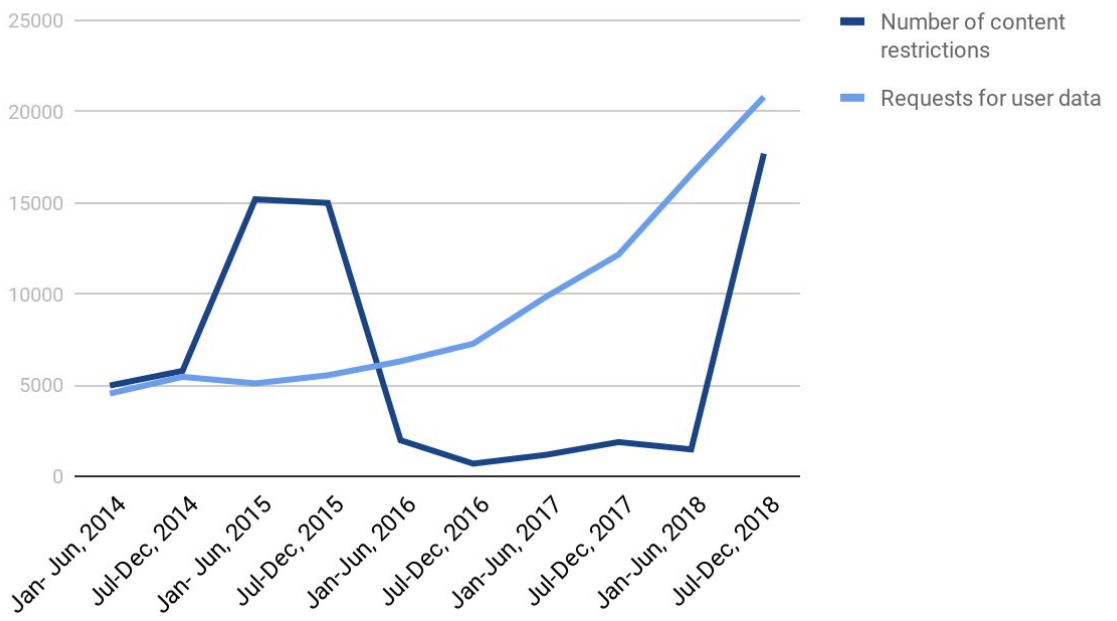
Facebook only publishes the number of items it removes pursuant to requests, and not the actual number of requests. Their data shows a steady incline in items taken down till 2015, and steep decline thereafter, the latter of which Facebook attributed to the judgment in *Shreya Singhal*.[34] There was a monumental increase in the second half of 2018 that was attributable to an order by the Delhi High Court to remove 16,600 items making claims about Pepsico products.[35]

On the other hand, Facebook documents the number of data requests it receives from the government. Since 2014, this number has been seeing a steep incline.

[33] Facebook Transparency Report <https://transparency.facebook.com> accessed on 19 September 2019

[34] Facebook, "Legal Requests for Content Restrictions - India" <https://transparency.facebook.com/content-restrictions/country/IN> accessed on 19 September 2019; "*Note: In 2016, informed by the decision of the Supreme Court of India last year amending the proper interpretation of the Information Technology Act of 2000, we ceased acting upon legal requests to remove access to content unless received by way of a binding court order and/or a notification by an authorized agency which conforms to the constitutional safeguards as directed by the Supreme Court.*"

[35] Facebook, "Legal Requests for Content Restrictions - India" <https://transparency.facebook.com/content-restrictions/country/IN> accessed on 19 September 2019



Graph 1: Number of content restrictions and government requests for user data to Facebook from 2014-2018.

Government requests for content removal

Criteria	Compliance	Notes
Numbers	✖	In its transparency reports, Facebook only publishes the number of items removed, and not the number of requests received for removal. No accurate statistics are available regarding the commonly cited grounds on which content removal requests were made. For IP Infringement, Facebook publishes a global statistic which does not differentiate requests from specific countries. No further demarcation of the removal requests based on those received under section 69A and those under section 79, exist.
Sources	✖	Facebook publishes the number of content removal requests it receives, where it also acknowledges that it receives reports from governments courts, as well from

		non-government entities).[36] These numbers, however, do not indicate how many of the content removal requests are received from each actor (government/judiciary/third-party). Facebook also does not categorize the numbers on the basis of which branch of the government made the request.
Items	✔	From the second half of 2018, Facebook has been categorizing the numbers based on the nature of items taken down (posts, accounts, etc.). However, no such demarcations exist for their earlier reports.[37]
Platforms	✔	In addition to the eponymous social media platform, Facebook owns Instagram (since 2012) and WhatsApp (since 2014). Since July 2018, their transparency reports began to show a platform-wise breakup of the data; whether or not data from Instagram had been included in their older reports is not completely clear. Due to the nature of WhatsApp's service, it is out of the scope of this particular metric of analysis.
Notice	✖	Facebook gives notices to users when their content is taken down under copyright law[38] or Community Standards [39]. However, there is no public undertaking by Facebook to notify users if their content was taken down following a government request.
Geographical scope	✔	For content restrictions on the basis of domestic law, Facebook restricts them only in that jurisdiction.[40]

[36] Facebook, "Content Restrictions Based on Local Law" <https://transparency.facebook.com/content-restrictions> accessed on 19 September 2019 [*hereinafter* Facebook Content Restrictions];
In the FAQ section Facebook says the following: "*[...] we may receive orders to restrict content from national courts, or reports alleging illegality from non-government entities like members of the Facebook community and NGOs.*"
[37] While we recognize that Facebook has updated its transparency reporting practices, for this year's report, we are looking at aggregated data from 2014-2018, and the compliance is also accordingly recorded.
[38] Facebook, "Content I posted was removed because it was reported for intellectual property (copyright or trademark) infringement. What are my next steps?" <https://www.facebook.com/help/365111110185763?helpref=popular_topics> accessed on 19 September 2019
[39] Facebook Terms of Service <https://www.facebook.com/legal/terms#account-termination> accessed on 19 September 2019
[40] Facebook Content Restrictions (n 28)

Government requests for user data

Facebook has been publishing information about government requests of user data since the first half of 2013.

Criteria	Compliance	Notes
Numbers	✔	Facebook publishes the number of user data requests it receives, as well as the number of requests where some user data was produced. Additionally, Facebook also publishes the number of user accounts against which such requests were made.
Sources	✔	Facebook publishes a numerical breakdown of the data requests it receives under the normal procedure of the interception rules, as well as those received under the emergency instances, though it is not clear if these requests are specifically made under the emergency provisions of the interception rules. Additionally, Facebook also provides a percentage of requests of each case, where some user data was produced. Facebook does not demarcate the requests on the basis of which law it receives them under.
Best practices	✔	In its report for data requests, while Facebook states that it responds to data requests in compliance with the relevant law their terms of service, it does not clarify the exact metrics of their review mechanism.[41] Facebook provides information regarding how the form of the request should look like. Among other things, this involves the name of the

[41] Facebook, "Legal Requests for User Data - India" <https://transparency.facebook.com/government-data-requests/country/IN> accessed on 19 September 2019; "*Facebook responds to government requests for data in accordance with applicable law and our terms of service. Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague.*"

		issuing authority, the e-mail address, phone number or username of the Facebook profile.[42] Facebook prohibits its developers from building tools that can be used for unauthorised surveillance on its users. [43]
Notification	✔	Facebook undertakes to notify users about requests for their information prior to such disclosure, unless they are prohibited by law, or in emergency cases.[44]
Platforms	✖	Facebook does not provide any numerical breakdown of the data requests it receives by the separate platforms it operates, i.e., Facebook, Instagram, and Whatsapp.

Google[45]

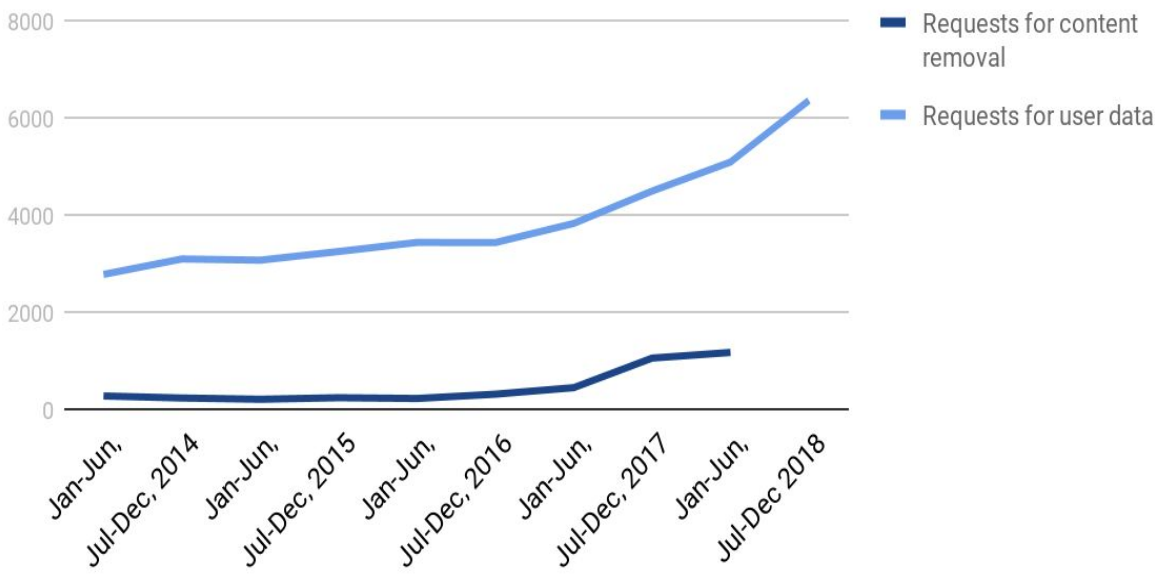
Google has been publishing transparency reports detailing content removals since the first half of 2010. Their data shows a steady rise of these numbers over the years.

Unlike Facebook, Google publishes information regarding both the number of content removal requests and the number of data requests. The number of government requests for both the sections have also seen a steady increase.

[42] Facebook, "Information for law enforcement authorities" <https://www.facebook.com/safety/groups/law/guidelines/> accessed on 19 September 2019 [*hereinafter* Facebook law enforcement];
"All requests must identify requested records with particularity including the specific data categories requested and date limitations for the request, as well as including:

- *The name of the issuing authority and agent, email address from a law-enforcement domain, and direct contact phone number.*
- *The email address, phone number (+XXXXXXXXXX), user ID number (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) or username (http://www.facebook.com/username) of the Facebook profile."*

[43] Facebook Platform Policy <https://developers.facebook.com/policy/> accessed on 19 September 2019;
"Protect the information you receive from us against unauthorized access, use, or disclosure. For example, don't use data obtained from us to provide tools that are used for surveillance."
[44] Facebook law enforcement (n 33)
[45] Google Transparency Report <https://transparencyreport.google.com/?hl=en> accessed on 19 September 2019



Graph 2: Number of government requests for content removal and user data to Google from 2014-2018.

Government requests for content removal

Criteria	Compliance	Notes
Numbers	✔	Google publishes comprehensive figures for user data and content takedown requests received and the number of requests granted. Additionally, Google also breaks up these numbers on the basis of the commonly cited reasons of requests - like defamation, fraud, religious offences and so on. No further demarcation of the removal requests based on those received under section 69A and those under section 79, exist.
Sources	✔	In its transparency report, Google has a separate section for government requests for content removal. They also demarcate between how many requests it received from the executive and the judiciary. Additionally, it also publishes figures for content removal notices filed by individuals under copyright law.
Items	✔	Google publishes the number of items it has taken down and additionally splits them up into items taken down on executive or judicial requests.

Platforms	✔	In its transparency report, Google lists out separately, the number of content removal requests it receives from Youtube, Gmail, Google Play Apps. For the rest of the platforms, it lists the numbers an 'All Others' category. It also provides figures of items specifically requested to be removed from Google Search, YouTube, Blogger and 'All Others'. However, Google fails to provide the number of items removed from each platform.
Notice	✖	Google provides the creators, publishers or owners of content, reasons for content takedown in its platforms like YouTube[46] and Play Store[47]. However, Google does not explicitly provide for issuance of such a notice for all its users across all its platforms.
Geographical scope	✔	Google restricts access to content that violates the law of a particular country but is not illegal in others[48].

Government requests for user data

Google's practice of reporting requests of user data and information began in the second half of 2009.

Criteria	Compliance	Notes
Numbers	✔	Google provides both the number of data requests from government it receives, as well as the percentage of instances where such requests produce data. Google also provides the number of user accounts against which such requests were being made.
Sources	✔	Google breaks down the number of requests it receives on the basis of 'All requests', 'Other legal requests' and 'Emergency disclosure requests'. Till the first half of 2014, 'All requests' predominated the number of requests, which has been subsequently replaced by 'Other legal requests'. Though the report does not define what 'all requests' constitute, it can be assumed that prior to the second half

[46] Youtube Help, "Copyright strike basics" <https://support.google.com/youtube/answer/2814000?hl=en> accessed on 19 September 2019

[47] Google Play, "Developer Policy Centre - Enforcement Process" <https://play.google.com/about/enforcement/enforcement-process/> accessed on 19 September 2019

[48] Google Transparency Report Help Center, "Government requests to remove content FAQs" <https://support.google.com/transparencyreport/answer/7347744?hl=en> accessed on 20 September 2019

		of 2014, Google treated both legal requests and emergency requests similarly, and only started providing this demarcation subsequently. Google does not demarcate the requests on the basis of which law it receives them under.
Best practices	✔	Google lays down the metrics of their review mechanism, as well as the specific format in which such a request must be presented. [49] Notably, while there is a reference to the review mechanism, the exact legal requirements that Google would review are not mentioned. In the second half of the information mentioned, Google lays down in general terms the format of government request, thereby partially fulfilling our criteria. In the FAQs discussed in the previous section, Google also states that it requires the government requests to be sent directly, and not through any 'backdoor' access.[50] Additionally, in the Google API Services: User Data Policy, Google also prohibits third-party APIs from accessing, aggregating and analyzing user data with the intention of building tools that can be used for surveillance.[51]
Notification	✖	While Google undertakes to inform users inside United States before sharing their information with law enforcement authorities, such a commitment is absent for users outside the United States.
Platforms	✖	Google does not provide any numerical demarcations for data requests received for the different platforms it operates.

[49] Google Transparency Report Help Center, "Legal process for user data requests FAQs" <https://support.google.com/transparencyreport/answer/7381738?hl=en&ref_topic=7380433> accessed 20 September 2019; "[...] *When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and Google's policies. Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law.*[...]"

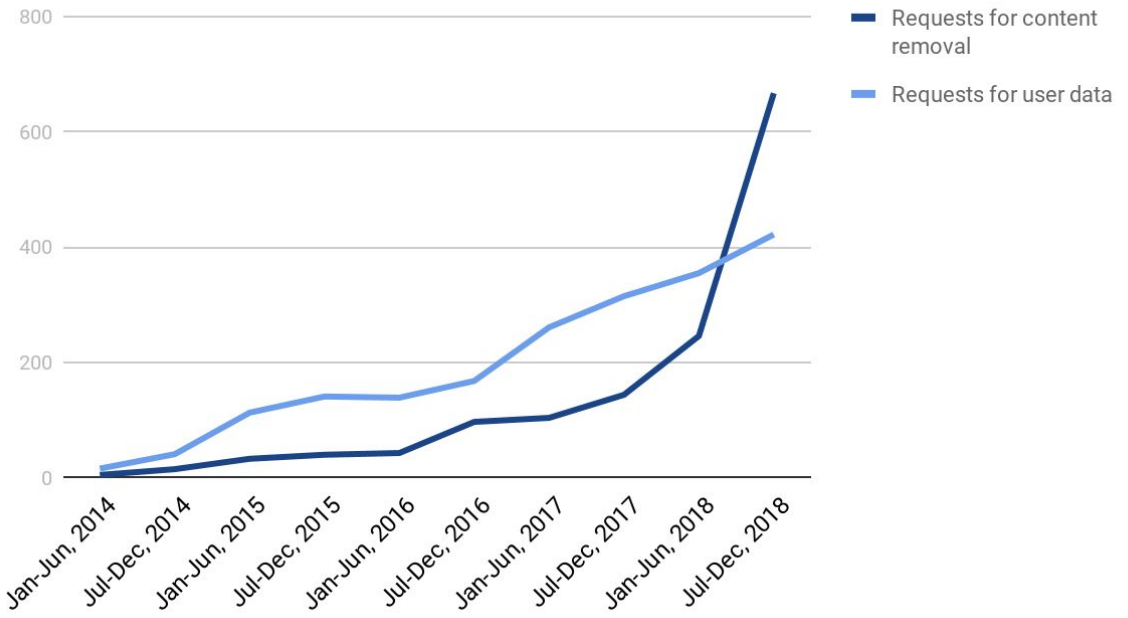
[50] Id

[51] Google Developers, "Google API Services: User Data Policy" <https://developers.google.com/terms/api-services-user-data-policy> accessed on 20 September 2019

Twitter[52]

Twitter began its transparency reporting practices from the first half of 2012.

Twitter reports both the number of requests for content removal and user data. While the general trend shows that there has been a steady increase in the number of information requests as well as content takedown requests from both the executive and judiciary, the social media platform has only complied in a small percentage of those cases.[53] A brief look at the numbers from the first half of 2018 shows that Twitter received nearly twice the number of content takedown requests in comparison to the six months that preceded that.



Graph 3: Number of government requests for content removal and user data to Twitter from 2014-2018.

Government requests for content removal

Criteria	Compliance	Notes
Numbers	✔	Twitter produces the total number of content removal requests for a certain reporting period, as well as the percentage where some content was withheld.

[52] Twitter Transparency Report <https://transparency.twitter.com/en.html> accessed on 20 September 2019
[53] Twitter Transpareny Report - India <https://transparency.twitter.com/en/countries/in.html> accessed on 20 September 2019

		Additionally, Twitter also provides the number of user accounts reported. No further demarcation of the removal requests based on those received under section 69A and those under section 79, exist.
Sources	✔	Twitter breaks down the number of government content removal requests on the basis of those received from the courts, and those received from government agencies, police and other executive bodies.
Items	✔	In its transparency reports, Twitter provides the number of both Tweets withheld, as well as accounts withheld.
Platforms	✔	Twitter reports the number of requests it receives for content removal for Periscope and Vine, but they are aggregated. These numbers additionally are not separated by country.
Notice	✖	Twitter states that it "*may*" notify users of legal requests unless they are prohibited to do so or in exceptional cases (eg. when the request relates to "emergencies regarding imminent threat to life", or "child sexual exploitation", etc.).[54] This does not fulfill our criteria since '*may*' does not translate to a compulsory undertaking.
Geographical scope	✔	Twitter withholds content that is found to be illegal or is requested to be removed from only those jurisdictions where it is illegal.[55]

Government requests for user data

Criteria	Compliance	Notes
Numbers	✔	Twitter publishes the number of account information requests it receives and the number of accounts specified.

[54] Twitter Help Center, "Legal request FAQs" <https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs> accessed on 20 September 2019; Their policy reads: "*Twitter may notify you of the existence of a legal request pertaining to your account unless we are prohibited or the request falls into one of the exceptions to our user notice policy (e.g., emergencies regarding imminent threat to life, child sexual exploitation, terrorism). [...]*"

[55] Twitter Help Center, "About country withheld content" <https://help.twitter.com/en/rules-and-policies/tweet-withheld-by-country> accessed on 20 September 2019

		It also publishes the percentage of instances where such requests produced some information.
Sources	✖	Twitter does not indicate any classification of the requests as those made under the 'emergency' requirement under the blocking rules, and those otherwise. Twitter does not demarcate the requests on the basis of which law it receives them under.
Best practices	✔	Twitter has a comprehensive mechanism delineated for the review of information requests it receives. This includes the requirement of a valid legal process such as a court order to disclose non-public information, and the requirement of a search warrant or its equivalent for disclosure of private communication.[56] Additionally, Twitter has a specific form through which law enforcement authorities have to submit their data information requests. As part of this submission, the submitting party also needs to prove their authority and thereby the eligibility of such submission. No other use of the form is permitted.[57] This satisfies the requirement of mandating government requests to be submitted in a specific format only. In a blogpost about developer policies, Twitter explained that they prohibit public APIs and Gnip data products from allowing law enforcement authorities to use Twitter data for surveillance purposes.[58]
Notification	✔	As part of their policy, Twitter also provides notifications to users whose accounts have been identified for disclosure requests. As part of their notification, they include a copy of the request, unless they are prohibited to do so. In case of non-disclosure provisions accompanying the request, Twitter ask for such non-disclosure to be restricted to a specific period. They include exceptions when such

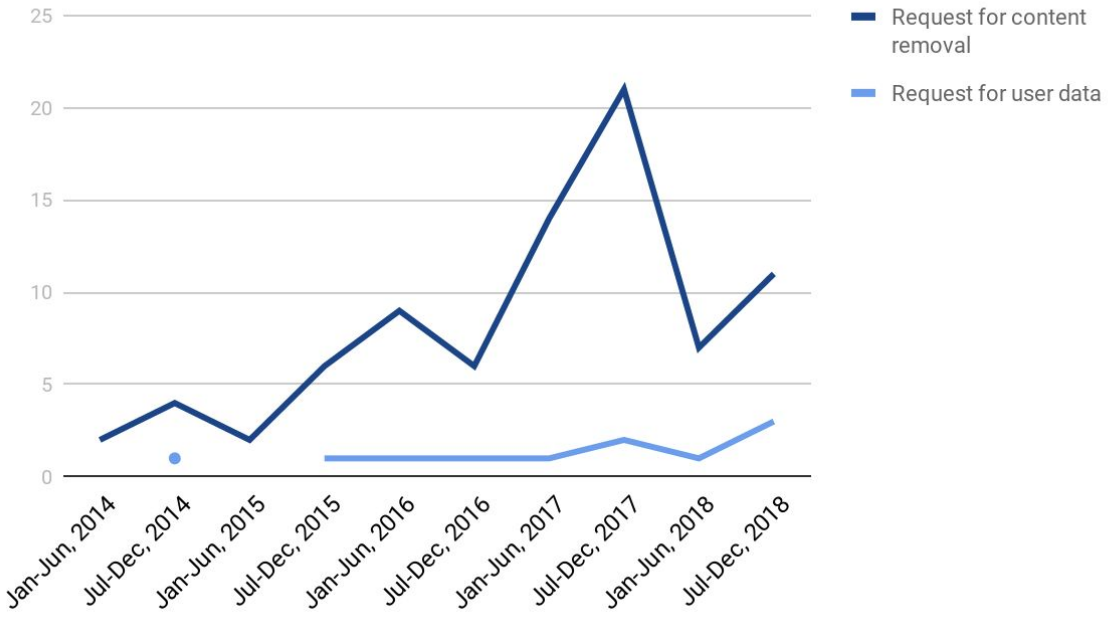
[56] Twitter Help Center, "Guidelines for law enforcement" <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#8> accessed on 20 September 2019 [*hereinafter* Twitter Guidelines]
[57] Twitter, "Legal requests Submissions" <https://legalrequests.twitter.com/forms/landing_disclaimer> accessed on 20 September 2019
[58] Chris Moody, "Developer Policies to Protect People's Voices on Twitter" <https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html> accessed on 20 September 2019

		notification system may be suspended, including in cases of terrorism, child sexual exploitation and so on.[59]
Platforms	✖	Twitter does not provide any numerical demarcations for the information requests received for the different platforms it operates.

Wikimedia Foundation[60]

Wikimedia Foundation ("WMF"), which hosts Wikipedia, has been providing information on content removal requests and data requests since 2012. Till the end of 2014, they provide one annual report, which has been now replaced by the practice of bi-annual reporting.

WMF reports both the number of requests for content removal and user data. The number of requests for content removal and user data is considerably lower than the other intermediaries. In reference to content removals, majority of their disputes are resolved by users themselves[61]. And in reference to data requests, the number is low,[62] which as WMF claims, is attributable to WMF collecting very little nonpublic information about its users.[63]



[59] Twitter Guidelines (n 47)
[60] Wikimedia Foundation: Transparency Report <https://transparency.wikimedia.org> accessed on 20 September 2019
[61] Wikimedia Foundation Transparency Report, "Requests for Content Alteration & Takedown" <https://transparency.wikimedia.org/content.html> accessed on 20 September 2019
[62] Wikimedia Foundation Transparency Report, "Requests for User Data" <https://transparency.wikimedia.org/privacy.html> accessed on 20 September 2019
[63] Wikimedia Foundation Transparency Report, "Requests for User Data" <https://transparency.wikimedia.org/privacy.html> accessed on 20 September 2019

Graph 4: Number of government requests for content removal and user data to Wikimedia Foundation from 2014-2018.

Government requests for content removal

Criteria	Compliance	Notes
Numbers	✔	WMF provides both the number of requests received, as well as the number of requests granted. These numbers are broken down country-wise. It is interesting to note that in its six years of reporting, WMF has granted only one of these requests. No further demarcation of the removal requests based on those received under section 69A and those under section 79, exist.
Sources	✔	For the reporting period of July-December 2018, WMF indicated that one out of the seven requests received by them was from a political party. Aside this, there is no other indication of where the other requests originated from.
Items	✖	WMF does not indicate how many items (for instance, articles) were requested for takedown, nor do they indicate how many items were taken down following such requests.
Platforms	✔	WMF provides a breakdown of the Wikimedia projects which were target of the content removal requests. The representation is not further broken down into country-wise categories, and the numbers are aggregated for a global view.
Notice	✖	In its publicly available documents, WMF does not undertake to provide a notice to the users in case their content is taken down.
Geographical scope	✖	In its publicly available documents, we could not find any commitment regarding restricting content only in jurisdictions where it is illegal.

Government requests for user data

Criteria	Compliance	Notes
Numbers	✔	WMF provides the number of user data requests it receives, as well as the percentage of instances where they provided data.
Sources	✔	WMF classifies the information requests it receives into various categories, such as informal government requests, informal non-government requests, search warrants and court orders. The breakdown of these categories are represented country-wise. Additionally, WMF also has is place a system where they proactively report user data when they detect emergency situations in one of their projects. These numbers are also represented as part of their transparency reports. These do not fall within the ambit of the emergency provisions of the blocking rules. WMF does not demarcate the requests on the basis of which law it receives them under.
Best practices	✖	While WMF provides clear guidelines regarding both the legal requirements for the validity of a request as well as the specific format in which the request is to be provided, such guidelines are only specific to the US. For the Indian context, such guidelines are missing. In the past few years for India, a predominant number of requests received by WMF are informal government requests, which means that the request does not involve a legal process.[64] WMF does not make any public undertaking regarding not accepting such requests. Due to the nature of the service provided by WMF, the criteria of prohibiting is not applicable to their transparency reports.
Notification	✖	WMF undertakes to provide notice to an affected user at least 10 calendar days before disclosing the information to the authorities. This commitment, however, is also specific to users in the US, and it is not clear whether it extends to India.

[64] Wikimedia Foundation Transparency Report, "Frequently Asked Questions" <https://transparency.wikimedia.org/faq.html> accessed on 20 September 2019

Platforms	✖	WMF does not provide any demarcations of data requests based on the different platforms.

Amazon[65]

Amazon has been one of the last intermediaries to begin the practice of transparency reporting.[66] Since the beginning of 2015, they have initiated the practice of reporting of content removal requests and information requests received from the government, twice a year.

Two important notes must be made. First, the scope of this information is limited to only the US; no separate information is available for India. And second, while Amazon previously provided information about content removal till the first half of 2018, this information is visibly absent in the subsequent reports.

Government requests for content removal

Criteria	Compliance	Notes
Numbers	✖	Till the first half of 2018, Amazon provided the number of removal requests it received, as well as the number of requests upon which it acted, either fully or partially. This information, however, is absent from the subsequent reports.
Sources	✖	Amazon provides no indication of the source of these requests.
Items	✖	There is no indication of how many items were marked for removal by way of these requests, nor is there any indication of how many items were actually removed pursuant to Amazon acting upon these requests.
Platforms	✖	Amazon owns and operates several platforms, like Twitch, Audible and Zaapos. Whether these platforms have ever received a content removal request is not clear, as Amazon does not provide any information on this in its reports.

[65] Amazon, "Law Enforcement Information Requests" <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF> accessed on 20 September 2019 [*hereinafter* Amazon Law Enforcement Requests]

[66] Cory Doctorow, "Amazon's useless "transparency reports" won't disclose whether they're handing data from always-on Alexa mics to governments" (*Boingboing*, 18 January 2018) <https://boingboing.net/2018/01/18/nunya-bizness.html> accessed on 20 September 2019

Notice	✖	Amazon provides no undertaking to provide notice to users whose content would be subject to successful content takedown.
Geographical scope	✖	Amazon undertakes no commitment to restrict the content geographically to jurisdictions where such content is illegal.

Government requests for user data

Criteria	Compliance	Notes
Numbers	✖	Amazon provides the number of information requests it receives, as well the number of instances where it acted upon such requests. It further classifies such responses as 'full', 'partial' and 'none'. This information is however, aggregated for all countries except the US, as 'non-US requests'. This does not clarify if the requests were for users residing in the US, or whether it also includes non-US users. Additionally, Amazon does not mark the number of user accounts specified in such requests.
Sources	✖	In the context of US, Amazon provides a demarcation of the requests based on the source of its receipt, say subpoenas, or search warrants. This classification however is absent for India. Amazon does not demarcate the requests on the basis of which law it receives them under.
Best practices	✖	In its page titled 'Law Enforcement Information Requests', Amazon says the following: "Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. [...]" [67] This does not throw light on the exact review mechanism Amazon undertakes to assess whether the order is 'legally

[67] Amazon Law Enforcement Requests (n 55)

		valid and binding', nor does it lay down what are the valid constituents of such an order. Amazon makes no commitment against allowing law enforcement agencies or other third-parties from utilizing its tools for surveillance.
Notification	✔	Amazon undertakes to notify its users before disclosing content information about them.[68]
Platforms	✖	As with the section on content removals, Amazon provides no numerical breakdown of information requests based on the platforms it operates. Additionally, it provides no indication whether the data collected by some of their tools, like Echo or Alexa, have ever been subject to a data request.

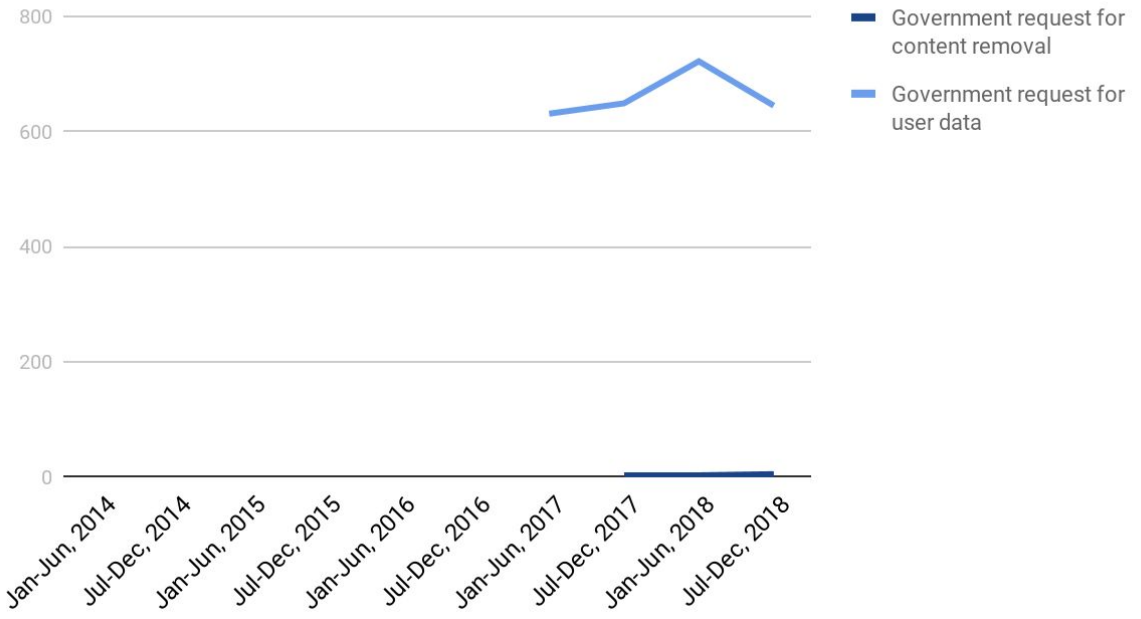
Oath Inc.[69]

Yahoo was acquired by Verizon in 2017. As a result of this acquisition, Yahoo, along with AOL and Huffington Post now operate under the umbrella of a new entity called Oath Inc. In the website of Oath Inc., accordingly, the transparency reporting period begins from the first half of 2017, and the numbers represented are aggregated for all the entities.

Oath Inc. received considerably less content removal requests as compared to other intermediaries. As indicated in the graph, the number of requests over these reporting periods did not cross 10. On the other hand, it received a high number of requests for user data, almost more than those received by Twitter. Due to a relatively short reporting period, at this current juncture, it is difficult to predict trends.

[68] Id.

[69] Oath Transparency Report <https://transparency.oath.com/> accessed on 20 September 2019



Graph 5: Number of government requests for content removal and user data to Oath Inc. from 2014-2018

Government requests for content removal

Criteria	Compliance	Notes
Numbers	✔	Oath Inc. provides the number of content removal requests it receives, as well as the number of instances where such requests have been acted upon. No further demarcation of the removal requests based on those received under section 69A and those under section 79, exists.
Sources	✖	Oath Inc. does not indicate the sources of the content removal requests.
Items	✔	Oath Inc. mentions the number of items specified for removal, as well as the compliance percentage for such requests. It does not however, specifies the exact nature of these items.
Platforms	✖	As we have indicated previously, Oath Inc. operates three platforms - Yahoo, AOL and Huffington Post. The numbers represented in their transparency reports, however, do not make a distinction between these platforms, and instead provide aggregated information.

Notice	✖	In the page for FAQs, Oath Inc. says that if the user has posted content that violated their policies, then the user 'may' receive a notification.[70] As per their policies, apart from other users, government can also submit removal requests on the ground that a certain piece of content violates the community guidelines and policies of Oath Inc[71]. For such instances, the undertaking to provide notice is not mandatory, as the language used is 'may' and not 'shall'. For all other instances where the government's removal request is based on the violation of local law, there is no undertaking to provide a notice as well.
Geographical scope	✖	There is no undertaking on their part to restrict content only to jurisdictions where such content violates the local law.

Government requests for user data

Criteria	Compliance	Notes
Numbers	✔	Oath Inc. provides the number of data requests it receives and the number of requests where it was acted upon. Such responses are further classified as instances where some data was disclosed, where the request was rejected and where no data was found. Additionally, they also provide the number of user accounts specified in these requests.
Sources	✔	Oath Inc. differentiates between normal requests and emergency requests, as well as the number of times when such requests met with a response. The number of accounts specified in such requests is also mentioned. However, in the context of India, it is not clear if such emergency requests were made under the specific provision in the blocking rules. Oath Inc. does not demarcate the requests on the basis of which law it received the requests under.

[70] Oath Transparency Report, "Frequently Asked Questions" <https://transparency.oath.com/about/faq-glossary.html> accessed on 20 September 2019 [*hereinafter* Oath FAQs]
[71] Id.

Best practices	✔	There is no specific reference to the exact review mechanism Oath Inc. undertakes to assess the substantive validity of a request. In the FAQs to the reports, Oath Inc. provides for the exact metrics which it will look for to ensure that the data request is valid. This includes, the legal process to specifically identify the user account by use of a proper identifier, the request to be submitted in writing and the request to be submitted in an official letterhead with enough information to prove that it originated with an entity authorized to make the request.[72] This fulfills the second of our criteria. As part of Yahoo's Developer Network FAQs, Yahoo forbids its developers from selling user data to third parties.[73] No such similar prohibition exists for AOL or Huffington Post, so this category is only partially fulfilled.
Notification	✖	Oath Inc. provides mandatory notices in instances of user data requests from third-party. However, this does not clarify whether or not they provide notices for government requests as well.[74]
Platforms	✖	The information represented in the reports are aggregated, and not classified on the basis of platforms.

Preliminary thoughts on qualitative transparency

As New America's Transparency Reporting Toolkit mentions, a substantial amount of our analysis found above focuses on quantitative transparency - concerning numbers and items.[75] Aside such analysis, in the context of India, two broad issues stood out to us, which forms part of larger, recommended qualitative transparency practices.

[72] Id

[73] Yahoo! Developer Network, "Frequently Asked Questions" <https://developer.yahoo.com/faq/?guccounter=1#cache> accessed on 20 September 2019

[74] Oath FAQs (n 60)

[75] New America, "The Transparency Reporting Toolkit: Content Takedown Reporting" <https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/introduction-and-executive-summary/> accessed on 20 September 2019

Material regarding local laws

One of our preliminary findings regarding the way these intermediaries report data for India, has been that most of the time, the information is incomplete, especially with regards to material regarding the local laws. Compared to the US, for which most of these companies dedicate separate sections, India features relatively fewer times in their reports. As we have already pointed out in our methodology section, India has various governing laws for requests of content removal and user data. More details about these laws can be found in Annexure 3. Under these different laws, different authorities are empowered to issue orders, and the procedural and substantive requirements of a valid request also vary. For the empowerment of users, we believe that the exact metrics and requirements of these laws must be presented by the intermediaries, in a clear and readable format.

Accessibility of policies

On the topic of empowerment of users, we also believe that the basic information and policies regarding these requests should be placed at one place, for maximum accessibility by users. During our research, we discovered that the information mapped in this report was spread over different policies, some of which were not easily accessible. For instance, while the numbers regarding government requests were available at one page for Facebook, information regarding its law enforcement practices and developer policies were not accessible through the same page.

While it is not possible at this juncture to predict a comprehensively objective way of making all these information accessible, we believe it would be a useful step if the basic information regarding the intermediary's transparency reporting policies were presented in the same manner as the company's Terms and Services and Privacy Policy. Additionally, given the diversity of languages in India, we believe that this information should be translated into the major languages for further accessibility.

Summary of our findings

In the course of our research, we noticed a gradual increase in the numbers of government requests for both content removal and information requests in India over the period 2014-2018.

In this section, we summarise our findings for each of the companies against each of the categories highlighted in our methodology.

Government requests for content removal

	Numbers	Sources	Items	Platforms	Notice	Geographical

						Scope
Facebook	✖	✖	✔	✔	✖	✔
Google	✔	✔	✔	✔	✖	✔
Twitter	✔	✔	✔	✔	✖	✔
WMF	✔	✔	✖	✔	✖	✖
Amazon	✖	✖	✖	✖	✖	✖
Oath	✔	✖	✔	✖	✖	✖

Government requests for user data

	Numbers	Sources	Best Practices	Notifications	Platforms
Facebook	✔	✔	✔	✔	✖
Google	✔	✔	✔	✖	✖
Twitter	✔	✖	✔	✔	✖
WMF	✔	✔	✖	✖	✖
Amazon	✖	✖	✖	✔	✖
Oath	✔	✔	✔	✖	✖

Future Work

We incorporated several metrics that we found useful from the methodologies by EFF's *Who Has Your Back* reports, the Santa Clara Principles and the Content Takedown Toolkit. We also came across the New America: Transparency Toolkit for user information, whose metrics we have not included in the current report. In the future editions of this report, we hope to incorporate more nuance into our criteria, by introducing more critical factors of analysis in our methodology inspired from the New America's Transparency Toolkits and future developments in the Indian context.

This would include, but would not be limited to:

Government requests for content takedown

- Asking companies to break down the requests they received by the categories of objectionable contents as per the categories cited by the government in removal

requests.[76] For instance, in one reporting period, a company receives 200 requests for taking down blasphemous content, and 300 requests for removing fraudulent content, then such a demarcation must be reflected in their reports. Such a demarcation is particularly important in India, due to the verdict of *Shreya Singhal* [77], where the Supreme Court had laid down that only the reasonable restrictions under Article 19(2) can form part of a valid government takedown order.

- Asking companies to report the number of accounts and items specified in the government request.[78]
- Asking companies to report the number of accounts and items impacted by the government request.[79]
- Asking companies to publicly express support to the Santa Clara Principles.[80]

Government requests for user data

- Asking companies to be specific and clear in the way they define the terms used in their reports. For instance, several of the companies reviewed dedicate a separate section for 'emergency requests', though the term is not defined anywhere in the report.[81]
- Asking companies to maintain separate records for preservation requests.[82]
- Asking companies to provide further granularity in the information. This may include documenting how the company chooses to respond to requests on a process-by-process basis. For instance, the company may choose to report that out of 200 requests received under the interception rules, 50 were successful, 100 were partially rejected, and the rest were completely rejected.[83]
- Asking companies to have a publicly available policy clearly affirming that they will only accept requests sent directly and officially to it. As part of this obligation we also ask companies that they publicly undertake that they will not accept requests that are extralegal or do not follow legal requirements.

[76] The Content Takedown Toolkit (n 14)
[77] *Shreya Singhal* (n 19)
[78] The Content Takedown Toolkit (n 14)
[79] Id
[80] Electronic Frontier Foundation, "Who Has Your Back? Censorship Edition 2019" <https://www.eff.org/wp/who-has-your-back-2019> accessed on 24 October 2019
[81] New America et. al, "The Transparency Reporting Toolkit" <https://na-production.s3.amazonaws.com/documents/Transparency_Reporting_Guide_and_Template-Final.pdf> accessed on 24 October 2019
[82] Id
[83] Id

Annexure 1: An illustrative list of differences in information made available by the intermediaries

Google

Criteria	India	USA
Types of information requests	Only 3 types: Emergency disclosure, preservation and other legal requests	8 types of requests in total: pen register orders, wiretap orders, preservation requests, other court orders, other legal requests, emergency disclosure, subpoenas and search warrants

Twitter

Criteria	India	USA
Footnotes section	**N/A**	Below each graph illustrating the cases, there is a footnotes section that offers rich details and explanations about the information above.
Types of legal requests	**N/A**	Reports sorted by subpoenas, court orders. Search warrants and others description for each type of legal processes also mentioned
User notice	**N/A**	Mentions the percentage of requests under seal, percentage of requests where user notice provided and percentage not under seal and no notice provided

Facebook

Criteria	India	USA
Cases sorted by Legal Process Request Types & Description of each type	N/A	Search warrants, subpoenas, Title III, Pen Register, Trap & Trace, Court Orders issued under 18 USC 2703(d), and other court orders

Annexure 2: An illustrative list of the trends reflected in the US and the Indian transparency reports

Grounds of differentiation	USA	India
Branches of the government from where the requests came from	Judicial orders for content takedown outweigh those coming from the executive. At the end of 2017, however, the number of requests from either branches have somewhat come to par, with 422 requests from the executive and 577 from the judiciary.	In India, the requests for content removal have come more from the executive branch of the government than the judiciary.
The major reasons for request of takedown	Defamation continues to be one of the major reasons for content-takedown requests, followed by fraud, followed by bullying and harassment.	Since 30th June 2017, fraud has skyrocketed to become one of the major reasons for content takedown, followed by defamation, followed by privacy and security. Prior to that date, defamation was the only prominent, specific reason for content request takedown, preceded by the miscellaneous ground of 'all others'.
Products targeted by the requests	The Google service which was the target of the most takedown requests was 'Web search', followed by 'Google voice', followed by Youtube.	In India, the target of the most takedown requests was Youtube, followed by Google Play apps and Gmail. Interestingly, Google Play Apps feature as the target of the second-most takedown requests only in the second half of 2017, before which its presence in the reports is very less, and it is only Gmail and Youtube which features prominently.

Removal percentages	The highest amount of removals against requests occurred in 2010, which was a staggering 87%, followed by another spurt in 2015, of 81%. Interestingly, the lowest percentage of removal came at the end of 2016 (fresh off the Trump elections), with 32% as the point.	The highest amount of removals against requests occurred at the end of 2009, with 77%. Contrasted to that, the lowest point in the graph came in the first half of 2014, with 8%. The difference between the highest and the lowest point of this graph is more prominent than the one in the US.

Annexure 3: The legal ecosystem surrounding government requests

For government requests for content removal

Relevant law and sections	Issuing authority	Substantive and procedural requirements for a valid request
Section 79, Information Technology Act, read with Rule 3(4) of the Information Technology (Intermediaries guidelines) Rules, 2011	Court or a government agency	The rationale for the request must relate to one of the grounds mentioned in Article 19(2).
Section 69A, Information Technology Act, read with Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009	An officer of the Central Government not below the rank of a Joint Secretary	The rationale for the request must relate to "[...] sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above [...]" The designated officer shall make reasonable efforts to identify the person or intermediary who has hosted the concerned information, and if they are able to identify, they shall issue a notice by way of letters or fax or e-mail signed with electronic signatures [...]

		Intermediary must revert back with replies and/or clarifications within a timeframe not less than 48 hours.

For government data requests

Relevant law and sections	Issuing authority	Substantive and procedural requirements for a valid request
Section 69, Information Technology Act, read with Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009	- Secretary, Ministry of Home Affairs, for Central Government - Secretary, Home Department for State/UT Government	The rationale for the request must relate to "[...] sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above [...]" The request must contain the reasons, and the name of the designated officer to which the intercepted information would be disclosed. The use of such information must also be mentioned. The duration of the request would be a maximum of 60 days. In case of renewal, the total duration of the request cannot be more than 180 days.
Section 79, Information Technology Act, read with Information Technology (Intermediaries guidelines) Rules, 2011	- Government agencies lawfully authorized	The request must be in writing stating clearly the purpose of seeking such information or assistance.
Section 91 and 92, Code of Criminal Procedure, 1973	District Magistrate, Chief Judicial Magistrate, Court of Session or High Court	The request for information must be in written or it must be a summons from the court.

Annexure 4: Top 20 websites in the Alexa list for Top websites India

S. No.	Website	Company/ Organisation	Reason for exclusion
1	google.com	Google	Covered under 'Google'
2	youtube.com	Google	Covered under 'Google'
3	google.co.in	Google	Covered under 'Google'
4	amazon.in	Amazon	Covered under 'Amazon'
5	facebook.com	Facebook	Covered under 'Facebook'
6	wikipedia.org	Wikimedia	Covered under 'Wikimedia Foundation'
7	yahoo.com	Oath	Covered under 'Oath'
8	flipkart.com	Flipkart	Doesn't have one
9	onlinesbi.com	State Bank of India	Does not seem to be dealing with third-party content. We could not find a transparency report.
10	indiatimes.com	Indiatimes	Does not seem to be dealing with third-party content. We could not find a transparency report.
11	blogspot.com	Google	Clubbed under 'Google'
12	hotstar.com	Star India	We could not find a transparency report.
13	stackoverflow.com	Stack Exchange	Deals with third-party content. But, there is no transparency report.[84]

[84] "Please upload DMCA takedowns to the Chilling Effects Clearinghouse / Lumen Database" (*Meta Stack Exchange*, 20 April 2013) <https://meta.stackexchange.com/questions/177269/please-upload-dmca-takedowns-to-the-chilling-effects-clearinghouse-lumen-datab/177303#177303> accessed 19 September 2019; "Does Stack Exchange report on the numbers of requests and orders it receives from law enforcement agencies?" (*Meta Stack Exchange*, 3 October 2013) <https://meta.stackexchange.com/questions/199283/does-stack-exchange-report-on-the-numbers-of-requests-and-orders-it-receives-fro> accessed 19 September 2019

14	amazon.com	Amazon	Covered under ‘Amazon’
15	hdfcbank.com	HDFC Bank	Does not seem to be dealing with third-party content. We could not find a transparency report.
16	netflix.com	Netflix	We could not find a transparency report.
17	primevideo.com	Amazon	Covered under ‘Amazon’
18	icicibank.com	ICICI Bank	Does not seem to be dealing with third-party content. We could not find a transparency report.
19	twitter.com	Twitter	Covered under ‘Twitter’
20	incometaxindiaefiling.gov.in	Government of India	Does not seem to be dealing with third-party content. We could not find a transparency report.