



Who Has Your Back?

PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS

THE ELECTRONIC FRONTIER FOUNDATION'S FIFTH ANNUAL REPORT ON
Online Service Providers'
Privacy and Transparency Practices Regarding
Government Access to User Data

Nate Cardozo, Kurt Opsahl, Rainey Reitman

June 17, 2015



ELECTRONIC FRONTIER FOUNDATION

EXECUTIVE SUMMARY.....	4
EXPECTING MORE FROM TECH COMPANIES IN 2015.....	4
EVALUATION CRITERIA.....	5
RESULTS SUMMARY.....	7
<i>Industry-Accepted Best Practices.....</i>	8
<i>Notifying Users of Government Requests.....</i>	9
<i>Disclosing Data Retention Policies.....</i>	9
<i>Disclosing Government Content Removal Requests.....</i>	11
<i>Pro-User Public Policy: Opposing Backdoors.....</i>	12
CONCLUSIONS.....	12
2015 RESULTS TABLE.....	13
COMPANY REPORTS.....	14
ADOBE.....	14
AMAZON.....	16
APPLE.....	18
AT&T.....	20
COMCAST.....	21
CREDO MOBILE.....	23
DROPBOX.....	25
FACEBOOK.....	27
GOOGLE.....	29
LINKEDIN.....	31
MICROSOFT.....	33
PINTEREST.....	35
REDDIT.....	37
SLACK.....	39
SNAPCHAT.....	42
SONIC.....	44
TUMBLR.....	46
TWITTER.....	48
VERIZON.....	51
WHATSAPP.....	53
WICKR.....	55
WIKIMEDIA.....	57
WORDPRESS.....	60
YAHOO.....	62
APPENDIX.....	64
2014 RESULTS TABLE.....	64
2013 RESULTS TABLE.....	65
2012 RESULTS TABLE.....	66
2011 RESULTS TABLE.....	67
REMOVING COMPANIES FROM OUR REPORT.....	68
REFERENCES AND HELPFUL LINKS.....	69

Authors: Nate Cardozo, Kurt Opsahl, Rainey Reitman
Editors: Parker Higgins, Dave Maass
Formatting: Parker Higgins
A publication of the Electronic Frontier Foundation, 2015

Who Has Your Back 2015: Which Companies Help Protect Your Data from the Government? The Electronic Frontier Foundation's Fifth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data is released under a Creative Commons Attribution 3.0 License.



Executive Summary

Expecting More From Tech Companies in 2015

We live digital lives—from the videos shared on social networks, to location-aware apps on mobile phones, to log-in data for connecting to our email, to our stored documents, to our search history. The personal, the profound, and even the absurd are all transcribed into data packets, whizzing through the fiber-optic arteries of the network.

While our daily lives have upgraded to the 21st century, the law hasn't kept pace. To date, the U.S. Congress hasn't managed to update the 1986 Electronic Communications Privacy Act to acknowledge that email stored more than 6 months deserves identical protections to email stored less than 6 months. Congress also dragged its feet on halting the NSA's indiscriminate surveillance of online communications and has yet to enact the strong reforms we deserve. Congress is even on the precipice of making things far worse, considering proposals that would mandate government backdoors into the technology we rely on to digitally communicate.

In this climate, we increasingly look to technology companies themselves to have the strongest possible policies when it comes to protecting user rights. Which companies will stand by users, insisting on transparency and strong legal standards around government access to user data? And which companies make those policies public, letting the world—and their own users—judge their stances on standing up for privacy rights?

For four years, the Electronic Frontier Foundation documented the practices of major Internet companies and service providers, judging their publicly available policies, and highlighting best practices. Over the course of those first four reports, we watched a transformation take place among the practices of major technology companies. Overwhelmingly, tech giants began publishing annual reports about government data requests, promising to provide users notice when the government sought access to their data, and requiring a search warrant before handing over user content. Those best practices we identified in early reports became industry standards in a few short years, and we're proud of the role our annual report played in pushing companies to institute these changes.

But times have changed, and now users expect more.

The criteria we used to judge companies in 2011 were ambitious for the time, but they've been almost universally adopted in the years since then. Now, users should expect companies to far exceed the standards articulated in the original *Who Has Your Back* report. Users should look to companies like Google, Apple, Facebook, and Amazon to be transparent about the types of content that is blocked or censored in response to government requests, as well as what deleted data is kept around in case government agents seek it in the future. We also look to these companies to take a principled stance against government-mandated backdoors.

In this, our fifth annual *Who Has Your Back* report, we took the main principles of the prior reports and rolled them into a single category: Industry-Accepted Best Practices. We've also refined our expectations around providing users notice and added new categories to highlight other important transparency and user rights issues.

We think it's time to expect more from Silicon Valley. We designed this report to take the basic principles of *Who Has Your Back* up a notch and see which companies were still leading the pack. Already, our newest report has had a similar effect on the industry as a whole, encouraging companies large and small to strive for more when it comes to standing by their users. In the months since we first told the companies what this year's criteria would be, we've seen significant improvement in company practices. And we hope—and expect—that over the next year, we'll see even more.

Evaluation Criteria

We used the following five criteria to assess company practices and policies:

1. **Industry-Accepted Best Practices.** This is a *combined category* that measures companies on three criteria (which were each listed separately in prior years' reports):
 1. Does the company require the government to obtain a warrant¹ from a judge before handing over the content of user communications?
 2. Does the company publish a transparency report, i.e. regular, useful data about how many times governments sought user data and how often the company provided user data to governments?

¹ In 2010, the Sixth Circuit Court of Appeals held in *United States v. Warshak* that the Fourth Amendment to the U.S. Constitution protects user communications stored with an Internet provider, and law enforcement generally must get a warrant to access the content of those communications. While we believe this is a critically important decision and correctly recognizes constitutional protection for electronic communications stored with third parties, it isn't Supreme Court precedent and therefore is not binding on the government in all jurisdictions. Changing this legislatively is the key goal of the Digital Due Process coalition, but in the meantime, companies can and do refuse to turn over content without a warrant.

3. Does the company publish law enforcement guides explaining how they respond to data demands from the government?

Companies must fulfill *all three* criteria in order to receive credit.

2. **Tell users about government data requests.** To earn a star in this category, Internet companies must promise to tell users when the U.S. government seeks their data unless prohibited by law, in very narrow and defined emergency situations,² or unless doing so would be futile or ineffective.³ Notice gives users a chance to defend themselves against overreaching government demands for their data. The best practice is to give users *prior* notice of such demands, so that they have an opportunity to challenge them in court. We have thus *adjusted our criterion* from prior years. We now require that the company provide advance notice to users except when prohibited by law or in an emergency and that the company also commit to providing *delayed notice* after the emergency has ended or when the gag has been lifted. As we were drafting last year's report, we let the companies know that we were going to make this adjustment for 2015 to give them a full year to implement procedures to give delayed notice when appropriate.
3. **Publicly disclose the company's data retention policies.** This category awards companies that disclose how long they maintain data about their users that isn't accessible to the user—specifically including logs of users' IP addresses and deleted content—in a form accessible to law enforcement. If the retention period may vary for technical or other reasons, the company must disclose that fact and should publish an approximate average or typical range, along with an upper bound, if any. We awarded this star to any company that discloses its policy to the public—even if that policy is one that EFF strongly disagrees with, for instance, if the company discloses that it retains data about its users forever.
4. **Disclose the number of times governments seek the removal of user content or accounts and how often the company complies.** Transparency reports are now industry standard practices. We believe that companies' responsibility to be transparent includes not only disclosing when governments demand user data, but also how often governments seek the removal of user content or the suspension of user accounts and how often the company complies with such demands. We award a star in this category to

² The exceptions should not be broader than the emergency exceptions provided in the Electronic Communications Privacy Act, 18 USC § 2702 (b)(8).

³ An example of a futile scenario would be if a user's account has been compromised or hijacked (or his mobile device stolen) and informing the "user" would concurrently—or only—inform the attacker.

companies that regularly publish this information, either in their transparency report or in another similarly accessible form. Companies should include formal legal process as well as informal government requests in their reporting, as government censorship takes many forms.

5. **Pro-user public policies: opposing backdoors.** Every year, we dedicate one category to a public policy position of a company. For three years, we acknowledged companies working publicly to update and reform the Electronic Communications Privacy Act. Last year, we noted companies who publicly opposed mass surveillance. This year, given the reinvigorated debate over encryption, we are asking companies to take a public position against the compelled inclusion of deliberate security weaknesses or other compelled back doors. This could be in a blog post, in a transparency report, by publicly signing a coalition letter, or through another public, official, written format. We expect this category to continue to evolve, so that we can track industry players across a range of important privacy issues.

Results Summary: Companies Adopt Industry-Accepted Best Practices Around Privacy and Transparency and Reject Government Backdoors

Major Findings in the 2015 Report:

- ▶ **Nine Companies Receive All Available Stars: Adobe, Apple, CREDO, Dropbox, Sonic, Wickr, Wikimedia, Wordpress.com, and Yahoo**
- ▶ **AT&T, Verizon, and WhatsApp Lag Behind Industry in Standing by Users**
- ▶ **Overwhelming Majority of Tech Companies Oppose Government-Mandated Backdoors**

We are pleased to announce that nine companies earned stars in every category that was available to them: Adobe, Apple, CREDO, Dropbox, Sonic, Wickr, Wikimedia, Wordpress.com, and Yahoo. (Note that some companies host little or no content, and thus the transparency about government data removal requests may not apply to them.) These nine companies show that it is practical for major technology companies to adopt best practices around transparency and stand by their users when the government comes knocking.

Unfortunately, not all companies are embodying such forward-thinking practices. Two major telecoms—Verizon and AT&T—received especially poor results, thus

continuing a trend we identified in prior reports where many large telecom providers fail to keep pace with the rest of the tech sector.

Notably, some companies that act as Internet service providers and general telecommunications providers are leading the way in adopting strong policies in defense of user rights. In particular, CREDO and Sonic again received credit in every category EFF rates. Comcast is close behind, earning an impressive 3 out of 4 possible stars. We hope other telecoms can rise to these standards in the coming years.

We added three new companies to this year's report: reddit, Slack, and WhatsApp. All three were responsive to conversations with EFF, and reddit and Slack have fulfilled several of the criteria to earn stars, though neither received credit in all available categories. Despite being given a full year to prepare for its inclusion in the report, WhatsApp did not fare so well. WhatsApp earned credit for its parent company Facebook's public policy position opposing backdoors and nothing else.

It is also clear that the technology industry stands united against government-mandated backdoors. Twenty-one of the 24 companies we evaluated have public statements opposing backdoors, which weaken security and endanger user privacy. ISPs, cloud storage providers, webmail providers, and social networks are overwhelmingly aligned in rejecting government-mandated security weaknesses.

Industry-Accepted Best Practices

These standards were developed over the course of four years of EFF reports, and they encompass three of the main issues at the heart of *Who Has Your Back*: requiring a warrant before handing over user content, publishing regular transparency reports, and publishing law enforcement guides. The transparency reports and the law enforcement guides help users understand how often and under what circumstances the companies are responding to government data requests, while the warrant for content ensures a strong legal requirement be met before data is handed to law enforcement.

In 2011, no company received credit in all of these categories (or even in two of those categories, since in 2011 we didn't include a category for requiring warrants for content). This year, 23 of the 24 companies in our report have adopted these principles. It's clear that these best practices truly are accepted by the technology industry. WhatsApp is notably lagging behind.

Notifying Users of Government Requests

This year, we asked companies to do more than simply promise to inform users about government data requests. We also asked them to provide advance notice to users before handing the data to the government. In cases when companies are prohibited from doing so, we asked the companies to promise to provide notice after an emergency has ended or a gag was lifted. Because we knew it would take significant engineering and workflow changes for some of the larger companies to implement these practices, we gave them more than a year's notice that this criterion would be included in the 2015 report.

Two companies who had previously earned credit in our report for telling users about government data requests did not receive credit this year because they did not have policies that tell users after a gag has been lifted or an emergency ended: Google and Twitter.

Fifteen out of the 24 companies we evaluated did meet this stronger criterion, and we're pleased that the industry is evolving in this way.

We were particularly impressed by the strong policy adopted by Dropbox⁴, which states:

Dropbox's policy is to provide notice to users about law enforcement requests for their information prior to complying with the request, unless prohibited by law. We might delay notice in cases involving the threat of death or bodily injury, or the exploitation of children. It is our policy to provide notice to users about grand jury subpoenas seeking user information. If you object to the user receiving notice in a particular case, please provide legal justification when serving the subpoena or obtain a sealing order prior to service. Once the basis for the non-disclosure has expired, we will give notice to the user.

Disclosing Data Retention Policies

For the first time this year, we evaluated companies on whether they were transparent about what deleted data they stored. Often, users may not realize that data they delete from an email service provider or off a social network is still stored and available to law enforcement agencies upon request. Transparency is the first step to educating users about what happens to their deleted data, so we are evaluating companies on their transparency practices in this category. Note that we aren't making specific requirements about a company deleting data after a certain time. Indeed, some companies publicly state that they maintain deleted data and server logs indefinitely—a practice we think is terrible for users. However, for this report, we're just asking companies to be clear about retention periods for data

⁴ Available at https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html#Notice

collected that may not be easily viewable to the user (including IP addresses and DHCP data) as well as content that users deleted.

Fifteen of the 24 companies we evaluated received credit in this category. We were particularly impressed by the clarity and detail of Comcast's disclosures:

Comcast maintains personally identifiable information about you in our regular business records while you are a subscriber to our cable service or other services. We also maintain this information for a period of time after you are no longer a subscriber if the information is necessary for the purposes for which it was collected or to satisfy legal requirements. These purposes typically include business, legal, or tax purposes. If these purposes no longer apply, we will destroy, de-identify, or anonymize the information according to our internal policies and procedures.

as well as:

Comcast can provide historic Internet Protocol assignment and session information for a period of 180 days for Xfinity Internet users.

and

Customer deleted emails remain in the customer's Trash Folder for 30 days if the folder is not emptied. Once emptied, the customer can retrieve those emails for 15 days via the "Recover Deleted items" folder under the Trash header. Xfinity Internet customers can set their own preferences for certain web mail deletion or retention. Thus, depending on a customer's deletion settings, Comcast may, or may not, have responsive information to a request for email information.

and

Comcast maintains historical call detail records for our Xfinity Voice telephone service for two years. This includes local, local toll, and long distance records. In limited instances, older records may be available, but will require additional time and resources to retrieve.

Comcast has other details available in its Law Enforcement Handbook.⁵

⁵ Available at [https://cdn.comcast.com/~Media/Files/Legal/Law Enforcement Handbook/Comcast Xfinity 2012 Law Enforcement Handbook v022112.pdf](https://cdn.comcast.com/~Media/Files/Legal/Law%20Enforcement%20Handbook/Comcast%20Xfinity%202012%20Law%20Enforcement%20Handbook%20v022112.pdf).

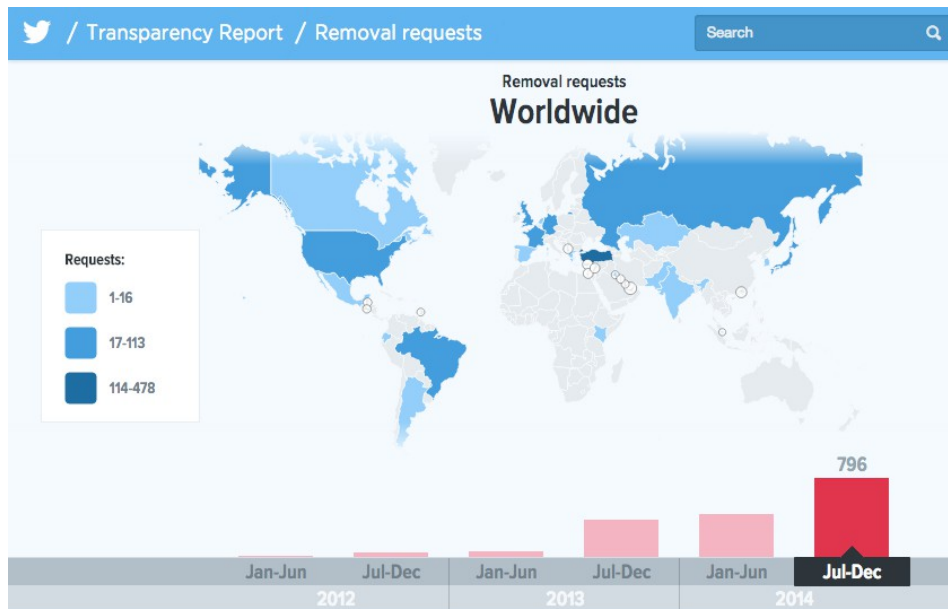
Disclosing Government Content Removal Requests

For more than a year, EFF's lead investigative researcher Dave Maass has been reporting on how Facebook cooperates with prison systems across the United States to block prisoner access to the social network. Facebook had even set up a dedicated "Inmate Account Takedown Request" form to help prison officials quickly and easily flag prisoner-run accounts for suspension, even when the accounts did not violate any of Facebook's terms of service.

This practice was the inspiration for EFF's newest category: tracking how often companies are removing content or shutting down accounts at the behest of the government. To earn credit in this category, companies need not refuse all or even any government content removal requests. Rather, they must simply be transparent about how often they are blocking or removing content or accounts.

Though this is simple enough, many companies are falling short in this area including Facebook, the company whose practices inspired the creation of the category. Fifteen out of the 24 companies we evaluated received credit in this category, though several do not host content and so this category did not apply to them.

A particularly strong example of this practice is the data published by Twitter, which includes an interactive map that allows users to mouse over countries and get details about content removal requests over a six-month time period.⁶



⁶ Available at <https://transparency.twitter.com/removal-requests/2014/jul-dec>.

Pro-User Public Policy: Opposing Backdoors

One of the big trends we're seeing across the tech industry is a rejection of government-mandated security weaknesses. In fact, 21 of the 24 companies we evaluated took a public position opposing backdoors. This is a powerful statement from the technology community that Congress and the White House should heed.

Many of the companies signed onto a letter organized by the Open Technology Institute⁷ that opposed mandates to intentionally weaken security, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them "front doors" or "back doors," introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government's own experts.




















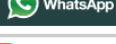




Conclusions

We are pleased to see major tech companies competing on privacy and user rights. Practices that encourage transparency with users about government data requests are becoming the default for companies across the web. While we're only able to judge a small selection of the tech industry, we believe this is emblematic of a broader shift. Perhaps invigorated by the ongoing debates around government surveillance and in response to growing public attention around these issues, more and more companies are voluntarily speaking out about government data requests and giving users tools to fight back.

We think that this type of transparency can help prompt broader discussion and systematic change about how and when governments access user data and perhaps eventually prompt Congress to clarify and improve the privacy laws for digital data. We also recognize that technology companies are in a position to know about and resist overbroad government requests, so we need to do everything within our power to encourage them to speak out and fight back. In handing our data to these companies, we've handed them a huge responsibility to do what they can to stand up for privacy. We're pleased that many of the companies we evaluated are stepping up to the task.

⁷ A copy of the letter is available at https://static.newamerica.org/attachments/3138-113/Encryption_Letter_to_Obama_final_051915.pdf

2015 Results Table

	Follows industry-accepted best practices	Tells users about government data demands	Discloses policies on data retention	Discloses government content removal requests	Pro-user public policy; opposes backdoors
 Adobe	★	★	★	★	★
 amazon.com	★	★	★	★	★
 Apple	★	★	★	★	★
 at&t	★	★	★	N/A	★
 COMCAST	★	★	★	N/A	★
 CREDO mobile	★	★	★	★	★
 Dropbox	★	★	★	★	★
 facebook	★	★	★	★	★
 Google	★	★	★	★	★
 LinkedIn	★	★	★	★	★
 Microsoft	★	★	★	★	★
 Pinterest	★	★	★	★	★
 reddit	★	★	★	★	★
 slack	★	★	★	★	★
 snapchat	★	★	★	N/A	★
 Sonic.net	★	★	★	★	★
 tumblr	★	★	★	★	★
 Twitter	★	★	★	★	★
 verizon	★	★	★	★	★
 WhatsApp	★	★	★	N/A	★
 WICKR	★	★	★	N/A	★
 WIKIMEDIA	★	★	★	★	★
 WordPress.com	★	★	★	★	★
 YAHOO!	★	★	★	★	★

Company Reports



Adobe

Adobe earns five stars in this year's *Who Has Your Back* report. This is Adobe's second year in the report, and it has adopted every best practice we've identified as part of this report. We commend Adobe for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. Adobe requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

[W]e require a search warrant issued upon a showing of probable cause under relevant state or federal law before we will turn over user content stored on our servers, such as photos, videos, documents, form responses, or email messages.

In addition to a law enforcement guide, Adobe publishes a transparency report.

Inform users about government data demands. Adobe promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

It is Adobe policy to give notice to our customers whenever someone seeks access to their information unless we are legally prohibited from doing so. For example, if we receive a Delayed Notice Order under 18 USC Section 2705(b), we will delay notice for the time period specified in the order and then notify the customer once the order expires.

Disclose data retention policies. Adobe publishes information about its data retention policies, including retention of IP addresses and deleted content:

The length of time Adobe keeps different types of customer data varies depending upon the nature of the service and type of data at issue. For example, Adobe keeps internet protocol (IP) address logs related to Adobe ID

sign-ins for 90 days, but content a customer has deleted from their Creative Cloud account generally is not recoverable after 72 hours. If you are a law enforcement agent with questions about the types of data that may be available for a particular Adobe service, please contact us using the information below. When we receive a preservation request from an agency investigating a crime, Adobe will preserve then-existing customer data for 90 days in anticipation of receiving valid legal process.

Disclose content removal requests. Adobe discloses the number of times governments seek the removal of user content or accounts, and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Adobe opposes the compelled inclusion of deliberate security weaknesses. In its transparency report, Adobe states:

Adobe has not built ‘backdoors’ for any government—foreign or domestic—into our products or services. All government requests for user data need to come through the front door (i.e., by serving valid legal process upon the appropriate Adobe legal department). Adobe vigorously opposes legislation in the US and overseas that would in any way weaken the security of our products or our users’ privacy protections.



Amazon

Amazon earns three stars in this year's *Who Has Your Back* report. This is Amazon's fifth year in the report, and this year marked a turning point for the company. Amazon published its transparency report, law enforcement guidelines, and a statement opposing government mandated backdoors. We have credited Amazon's commitment for requiring a warrant for user content in prior years. However, there is room for improvement. Amazon should strengthen its policy of providing users notice of law enforcement requests and create more transparency around data retention policies.

Industry-Accepted Best Practices. To earn credit in this category, Amazon must meet all three criteria. Amazon requires a warrant before giving content to law enforcement. Amazon Vice President for Global Public Policy Paul Misener testified before the House Judiciary Committee in 2010, stating⁸:

With respect to the content of electronic communications, we believe that ECPA requires law enforcement authorities to obtain a search warrant to compel disclosure. We do not release information without valid process and have not disclosed content without a search warrant.

In addition, Amazon publishes a transparency report and law enforcement guidelines.

Inform users about government data demands. Amazon does not promise to provide advance notice to users about government data demands.

Disclose data retention policies. Amazon does not publish information about its data retention policies, including retention of IP addresses and deleted content.

Disclose content removal requests. In its transparency report, Amazon does disclose the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

⁸ Amazon provided the full transcript of the testimony to EFF.

Pro-user public policy: oppose backdoors. In a public, official written format, Amazon has opposed the compelled inclusion of deliberate security weaknesses. In a blog post, AWS Chief Information Security Officer Steve Schmidt stated:

While we recognize the legitimate needs of law enforcement agencies to investigate criminal and terrorist activity, and cooperate with them when they observe legal safeguards for conducting such investigations, we oppose legislation mandating or prohibiting security or encryption technologies that would have the effect of weakening the security of products, systems, or services our customers use, whether they be individual consumers or business customers.



Apple

Apple earns five stars in this year's *Who Has Your Back* report. This is Apple's fifth year in the report, and it has adopted every best practice we've identified as part of this report. We commend Apple for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. Apple requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Law enforcement is required to obtain a search warrant that is issued upon a probable cause showing for search warrants requesting user content.

In addition to a law enforcement guide, Apple publishes a transparency report.

Inform users about government data demands. Apple promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Apple will notify its customers when their personal information is being sought in response to legal process except where providing notice is prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), or by applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.

Disclose data retention policies. Apple publishes information about its data retention policies, including retention of IP addresses and deleted content. It includes a range of details in its legal process guidelines, for example:

Connection logs are retained up to 30 days.

See Apple's legal process guidelines for more detailed information.

Disclose content removal requests. Apple discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Apple opposes the compelled inclusion of deliberate security weaknesses. In its statement on government information requests, Apple states:

In addition, Apple has never worked with any government agency from any country to create a "back door" in any of our products or services. We have also never allowed any government access to our servers. And we never will.



AT&T

AT&T earns one star in this year's *Who Has Your Back* report. This is AT&T's fifth year in the report, and it has adopted all of the best practice we recognized in prior years' reports. We applaud those commitments and urge the company to integrate the new 2015 standards.

Industry-Accepted Best Practices. AT&T requires a warrant before giving content to law enforcement, stating in its explanation of Total U.S. Criminal and Civil Demands:

Except in emergency circumstances, a search warrant or probable cause court order for all real-time location information (i.e., wiretaps and GPS) and stored content (i.e., text and voice messages) is required for all jurisdictions, courts, and agencies.

In addition, AT&T publishes a transparency report and law enforcement guide.

Inform users about government data demands. AT&T does not promise to provide advance notice to users about government data demands.

Disclose data retention policies. AT&T does not publish information about its data retention policies, including retention of IP addresses and deleted content.

Disclose content removal requests. AT&T does not host significant content nor do we have reason to believe it receives account closure requests domestically, and thus this category is not applicable.

Pro-user public policy: oppose backdoors. In a public, official written format, AT&T has not opposed the compelled inclusion of deliberate security weaknesses.



Comcast

Comcast earns three stars in this year's *Who Has Your Back* report. This is Comcast's fifth year in the report, and it has adopted all of the best practice we recognized in prior years' reports. Comcast's policies also meet several of the 2015 category requirements, including taking a policy position opposing backdoors and disclosing its data retention policies. We're pleased with Comcast's policies in these areas. However, there is still some room for improvement: Comcast can adopt a stronger policy around providing users with notice about government data requests.

Industry-Accepted Best Practices. Comcast requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Comcast requires a warrant for the release of all content data regardless of the amount of time the content has been in electronic storage.

In addition to a law enforcement guide, Comcast publishes a transparency report.

Inform users about government data demands. Comcast does not promise to provide advance notice to users about government data demands, stating in its privacy notice:

Comcast may also be required to disclose personally identifiable information and individually identifiable CPNI about subscribers to high-speed Internet, phone, and home security services to a government entity in response to a subpoena, court order, or search warrant, for example. We are usually prohibited from notifying the subscriber of any disclosure of personally identifiable information to a government entity by the terms of the subpoena, court order, or search warrant.

Disclose data retention policies. Comcast publishes robust and comprehensive information about its data retention policies, including retention of IP addresses and deleted content. For example, Comcast states:

Comcast maintains personally identifiable information about you in our regular business records while you are a subscriber to our cable service or other services. We also maintain this information for a period of time after you are no longer a subscriber if the information is necessary for the purposes for which it was collected or to satisfy legal requirements. These purposes typically include business, legal, or tax purposes. If these purposes no longer apply, we will destroy, de-identify, or anonymize the information according to our internal policies and procedures.

as well as:

Comcast can provide historic Internet Protocol assignment and session information for a period of 180 days for Xfinity Internet users.

and

Customer deleted emails remain in the customer's Trash Folder for 30 days if the folder is not emptied. Once emptied, the customer can retrieve those emails for 15 days via the "Recover Deleted items" folder under the Trash header. Xfinity Internet customers can set their own preferences for certain web mail deletion or retention. Thus, depending on a customer's deletion settings, Comcast may, or may not, have responsive information to a request for email information.

and

Comcast maintains historical call detail records for our Xfinity Voice telephone service for two years. This includes local, local toll, and long distance records. In limited instances, older records may be available, but will require additional time and resources to retrieve.

Comcast has other details available in its Law Enforcement Handbook.

Disclose content removal requests. Comcast does not host significant content, and thus this category is not applicable.

Pro-user public policy: oppose backdoors. In a public, official written format, Comcast opposes the compelled inclusion of deliberate security weaknesses. In its blog post on Upgrading the Security and Privacy of Your Email, Comcast states:

However, Comcast does not support the creation of extra-legal "backdoors," or the inclusion of deliberate security weaknesses in open source or other software to facilitate surveillance without proper legal process.



CREDO Mobile

CREDO earns five stars in this year's *Who Has Your Back* report. This is CREDO's second year in the report, and it has adopted every best practice we've identified as part of this report. We commend CREDO for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. CREDO requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

CREDO requires third parties to obtain a U.S. subpoena, court order, or warrant (for example, in the case of a request for content) in order to obtain CREDO customer information.

In addition to a law enforcement guide, CREDO publishes a transparency report.

Inform users about government data demands. CREDO promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

For criminal legal process:

CREDO will notify customers upon receipt of criminal legal process seeking information about their accounts unless such notification is prohibited by law. There is a 21-day waiting period before disclosure of account information, unless CREDO is compelled by law to respond earlier. When CREDO is prohibited from notifying a customer before complying with criminal legal process, CREDO will provide notification once the legal prohibition expires.

For Emergency Requests:

CREDO will notify customers when information about their accounts has been provided in response to an emergency request.

Disclose data retention policies. CREDO publishes information about its data retention policies, including retention of IP addresses and deleted content:

CREDO retains customer name, address, phone number, email address, and product type information for historical purposes. CREDO stores individually-identifiable customer billing data for three years unless longer storage is needed for tax, business, accounting, or legal purposes. CREDO does not receive or store precise handset location information or IP addresses. CREDO does not receive or store the content of customer communications sent using our services except customer communications directed to us for customer service purposes.

Disclose content removal requests. CREDO discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests. (Note that CREDO is not a content provider, and thus would likely have received an N/A if had not published this information in its transparency report.)

Pro-user public policy: oppose backdoors. In a public, official written format, CREDO opposes the compelled inclusion of deliberate security weaknesses. CREDO signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.



Dropbox

Dropbox earns five stars in this year's *Who Has Your Back* report. This is Dropbox's fourth year in the report, and it has adopted every best practice we've identified as part of this report. We commend Dropbox for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. Dropbox requires a warrant before giving content to law enforcement, stating in its transparency report:

All requests for content information were accompanied by a search warrant, which is the legal standard that Dropbox requires.

In addition, Dropbox publishes a transparency report and law enforcement guide.

Inform users about government data demands. Dropbox promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Dropbox's policy is to provide notice to users about law enforcement requests for their information prior to complying with the request, unless prohibited by law. We might delay notice in cases involving the threat of death or bodily injury, or the exploitation of children. It is our policy to provide notice to users about grand jury subpoenas seeking user information. If you object to the user receiving notice in a particular case, please provide legal justification when serving the subpoena or obtain a sealing order prior to service. Once the basis for the non-disclosure has expired, we will give notice to the user.

Disclose data retention policies. Dropbox publishes information about its data retention policies, including retention of IP addresses (in this case, subscriber information) and deleted content:

Subscriber information is available while an account is active. Deleted files in an active account will still be available for 30 days after deletion, or if the account has been preserved, until the preservation expires. Once an account

is deleted, subscriber information and the content in the account will be unrecoverable after 30 days, unless the account is preserved.

Disclose content removal requests. Dropbox discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Dropbox opposes the compelled inclusion of deliberate security weaknesses. In its Government Data Request Principles, Dropbox states:

Governments should never install backdoors into online services or compromise infrastructure to obtain user data. We'll continue to work to protect our systems and to change laws to make it clear that this type of activity is illegal.



Facebook

Facebook earns four stars in this year's *Who Has Your Back* report. This is Facebook's fifth year in the report, and it has adopted most of the practices we've identified as part of this report. While we commend the steps it has taken to stand by its users, there is more to be done. Facebook should disclose when it blocks content or closes accounts in response to government requests.

Industry-Accepted Best Practices. Facebook requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.

In addition to a law enforcement guide, Facebook publishes a transparency report.

Inform users about government data demands. Facebook promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when notice would be counterproductive. We will provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing violation of our terms of use, we will take action to

prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Disclose data retention policies. Facebook publishes information about its data retention policies, including retention of IP addresses and deleted content:

We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.

Disclose content removal requests. While Facebook does report on some content restriction internationally, it does not provide transparency into ways it cooperates with the U.S. government to block content and remove accounts. For example, EFF learned through a public-records request that Facebook processed 74 requests from California prison officials in 2014 to suspend inmate profiles. These takedowns requests are not disclosed in Facebook's transparency report.

Pro-user public policy: oppose backdoors. In a public, official written format, Facebook opposes the compelled inclusion of deliberate security weaknesses. Facebook signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government's own experts.



Google

Google earns three stars in this year's *Who Has Your Back* report. This is Google's fifth year in the report, and it has adopted some of the policies we are highlighting, including the best practices from prior reports. Nonetheless, there is room for improvement. Google should take a stronger position in providing notice to users about government data requests after an emergency has ended or a gag has been lifted. Furthermore, Google should provide transparency into its data retention policies.

Industry-Accepted Best Practices. Google requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

But Google requires an ECPA search warrant for contents of Gmail and other services based on the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure.

In addition to a law enforcement guide, Google publishes a transparency report.

Inform users about government data demands. Google promises to provide notice to users about government data requests and, in most cases, promises to make sure the notification happens before the data is turned over. However, Google does not commit to providing notice after an emergency has ended or a gag has been lifted:

If Google receives ECPA legal process for a user's account, it's our policy to notify the user via email before any information is disclosed. (If the account is an Enterprise Apps hosted end user account, notice may go to the domain administrator, or the end user, or both.) This gives the user an opportunity to file an objection with a court or the requesting party. If the request appears to be legally valid, we will endeavor to make a copy of the requested information before we notify the user.

There are a few exceptions to this policy:

A statute, court order or other legal limitation may prohibit Google from telling the user about the request;

We might not give notice in exceptional circumstances involving danger of death or serious physical injury to any person;

We might not give notice when we have reason to believe that the notice wouldn't go to the actual account holder, for instance, if an account has been hijacked.

We review each request we receive before responding to make sure it satisfies applicable legal requirements and Google's policies. In certain cases we'll push back regardless of whether the user decides to challenge it legally.

Disclose data retention policies. Google publishes some information about log data and deleted data, but it is not complete and representative of all its services and thus does not qualify for a star.

Disclose content removal requests. Google does an exemplary job disclosing the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Google opposes the compelled inclusion of deliberate security weaknesses. Google signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.



LinkedIn

LinkedIn earns four stars in this year's *Who Has Your Back* report. This is LinkedIn's fourth year in the report, and it has adopted many of the best practice we've identified as part of this report. We commend LinkedIn for the steps it has taken toward transparency and standing with users, but there's still room for improvement. Specifically, LinkedIn should begin reporting government requests to block content and accounts.

Industry-Accepted Best Practices. LinkedIn requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Please note that certain types of member data, including messages, invitations and connections, have a high bar for disclosure and can only be disclosed pursuant to a valid search warrant from an entity with proper jurisdiction.

In addition to a law enforcement guide, LinkedIn publishes a transparency report.

Inform users about government data demands. LinkedIn promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

LinkedIn's policy is to notify Members of Requests for their data unless we are prohibited from doing so by statute or court order. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other valid legal process that specifically precludes Member notification, such as an order issued pursuant to 18 U.S.C. §2705(b). When a Request is accompanied by a nondisclosure order, LinkedIn will notify the affected Member(s) as soon as the order is overturned or expires on its own terms.

Disclose data retention policies. LinkedIn publishes information about its data retention policies, including retention of IP addresses and deleted content:

LinkedIn generally does not retain a copy of information from a Member's profile page once the information has been revised or removed by the

Member. Other categories of data relating to Member accounts, such as account log-in history for active accounts, are only accessible for a defined time period. Please note that, except in unusual circumstances, 24 months represents the upper limit on IP log data that can be provided in response to any Data Request. Additionally, in the normal course, if a Member closes his or her account, we promptly delete or de-personalize information from that account, generally within 20 to 30 days of account closure. LinkedIn cannot recover Invitations or Messages once they are permanently deleted by a Member, and cannot recreate evidence of Connections that have been severed.

Disclose content removal requests. LinkedIn does not disclose the number of times governments seek the removal of user content or accounts.

Pro-user public policy: oppose backdoors. In a public, official written format, LinkedIn opposes the compelled inclusion of deliberate security weaknesses. LinkedIn signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.



Microsoft

Microsoft earns three stars in this year's *Who Has Your Back* report. This is Microsoft's fifth year in the report, and it has adopted several of the best practices we are highlighting. We appreciate what Microsoft has done to stand up for user transparency and privacy, but it still has more work to do. In particular, Microsoft should make clear its data retention policies and disclose what government content removal requests it receives.

Industry-Accepted Best Practices. Microsoft requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Microsoft requires an official, signed document, issued pursuant to local law and rules. Specifically, we require a subpoena or equivalent before disclosing non-content, and only disclose content in response to a warrant or court order. Microsoft's compliance team reviews government demands for user data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order.

In addition to a law enforcement guide, Microsoft publishes a transparency report.

Inform users about government data demands. Microsoft promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Microsoft will give prior notice to users whose data is sought by a law enforcement agency or other governmental entity, except where prohibited by law. We may also withhold notice in exceptional circumstances, such as emergencies, where notice could result in danger (e.g., child exploitation investigations), or where notice would be counterproductive (e.g., where the user's account has been hacked). Microsoft will also provide delayed notice to users upon expiration of a valid and applicable nondisclosure order unless Microsoft, in its sole discretion, believes that providing notice could result in danger to identifiable individuals or groups or be counterproductive.

Disclose data retention policies. Microsoft does not publish information about its data retention policies that includes information about retention of IP addresses and deleted content.

Disclose content removal requests. Microsoft does not disclose the number of times governments seek the removal of user content or accounts. Microsoft informs us that they will be publishing this in September.

Pro-user public policy: oppose backdoors. In a public, official written format, Microsoft opposes the compelled inclusion of deliberate security weaknesses. John Frank, Microsoft's Deputy General Counsel and Vice President of Legal and Corporate Affairs, stated:

We're also seeing officials around the world try to limit security measures such as encryption without making progress on the stronger legal protections that people deserve. The bottom line is that while governments only request data on a very small fraction of our customers, governments are seeking to alter the balance between privacy and public safety in a way that impacts everyone.

As we have said before, there are times when law enforcement authorities need to access data to protect the public. However, that access should be governed by the rule of law, and not by mandating backdoors or weakening the security of our products and services used by millions of law-abiding customers. This should concern all of us.



Pinterest

Pinterest earns four stars in this year's *Who Has Your Back* report. This is Pinterest's second year in the report, and it has adopted many of the best practices we're highlighting in this report. We commend Pinterest's efforts to stand up for their users, but there is still room for improvement. Pinterest should disclose its data retention policies.

Industry-Accepted Best Practices. Pinterest requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

To compel Pinterest to provide any user's content, you must obtain a valid search warrant.

In addition to a law enforcement guide, Pinterest publishes a transparency report.

Inform users about government data demands. Pinterest's policies include a strong promise to provide advance notice to users about government data demands, and the company will delay notice only in limited circumstances:

Yes, our policy is to notify users of Law Enforcement Requests by providing them with a complete copy of the request before producing their information to law enforcement. We may make exceptions to this policy where:

1. we are legally prohibited from providing notice (e.g. by an order under 18 U.S.C. § 2705(b));
2. an emergency situation exists involving a danger of death or serious physical injury to a person;
3. we have reason to believe notice wouldn't go to the actual account holder (e.g. an account has been hijacked)

In cases where notice isn't provided because of a court order or emergency situation, our policy is to provide notice to the user once the court order or emergency situation has expired.

Note: Officer authored affidavits, descriptions, cover letters or similar statements are not sufficient to preclude notice to our users. You must provide a court order issued in accordance with 18 U.S.C. § 2705(b) or cite an applicable

statute if you wish to prohibit user notice of your Law Enforcement Request. Please contact us if you have any questions regarding this.

Disclose data retention policies. Pinterest publishes information about its data retention policies, but it is not detailed enough to meet the standards of this category. Specifically, Pinterests says in its terms of service:

Following termination or deactivation of your account, or if you remove any User Content from Pinterest, we may retain your User Content for a commercially reasonable period of time for backup, archival, or audit purposes. Furthermore, Pinterest and its users may retain and continue to use, store, display, reproduce, re-pin, modify, create derivative works, perform, and distribute any of your User Content that other users have stored or shared through Pinterest.

Disclose content removal requests. Pinterest does disclose the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Pinterest opposes the compelled inclusion of deliberate security weaknesses. In its law enforcement guidelines, Pinterest says:

Pinterest opposes compelled back doors and supports reforms to limit bulk surveillance requests.



reddit

reddit earns four stars in this year's *Who Has Your Back* report. This is reddit's first year in the report, and it has adopted many of the best practice we've identified as part of this report. We commend reddit for its strong stance regarding user rights, but there's still room to improve. We urge reddit to take an official stance opposing government mandated backdoors.

Industry-Accepted Best Practices. reddit requires a warrant before giving content to law enforcement, stating in its transparency report:

reddit requires a search warrant based on probable cause to disclose user content information, which includes private messages and posts/comments that have been deleted or otherwise hidden from public view.

In addition to a transparency report, reddit publishes a law enforcement guide (which is also on its transparency report page).

Inform users about government data demands. reddit promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Many government requests we receive contain demands to withhold notice from users that carry no legal weight. We actively disregard these non-binding demands. Our goal is to give users the information they need to seek legal advice before their records are disclosed. As stated in our privacy policy, we provide advance notice to affected users unless prohibited by a court order or where we decide delayed notice is appropriate based on clear criteria.

Disclose data retention policies. reddit publishes information about its data retention policies, including retention of IP addresses and deleted content:

registration information

When you create an account, you are required to provide a username and password, and may opt to provide an email address. We also log, and retain indefinitely, the IP address from which the account is initially created.

post, comment and messaging data

The posts and comments you make on reddit are not private, even if made to a subreddit not readily accessible to the public. This means that, by default, they are not deleted from our servers – ever – and will still be accessible after your account is deleted. However, we only save the most recent version of comments and posts, so your previous edits, once overwritten, are no longer available.

Your messages are generally only viewable by the parties involved, but they may be accessed internally as needed for community support. Moreover, we keep a complete log of all messages sent on our service, even when both parties later delete their accounts.

reddit stores the IP addresses associated with specific posts, comments, and private messages for 90 days after they are made or sent.

Disclose content removal requests. reddit does disclose the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. reddit has not published a public, official written statement opposing the compelled inclusion of deliberate security weaknesses.



Slack

Slack earns three stars in this year's *Who Has Your Back* report. This is Slack's first year in the report, and it has adopted several of the best practices we are highlighting in this report. We appreciate the steps Slack has taken to stand by its users, but there's room for improvement. Slack should improve its policies around providing users notice of government requests and clarify its data retention policies with regard to IP addresses.

Industry-Accepted Best Practices. Slack requires a warrant before giving content to law enforcement, stating in its user data request policy:

Slack does not disclose account content absent a search warrant in criminal cases.

In addition, Slack publishes a transparency report and law enforcement guide (which Slack calls a "user data request policy").

Inform users about government data demands. While Slack promises to provide advance notice to users about government data demands, it does not make clear that it will provide delayed notice after an emergency has ended or a gag has been lifted.

Disclose data retention policies. Slack publishes extensive information about its data retention policies, including deleted content, and the retention of IP addresses. From their FAQ:

Our position is simple: if we get a legal request for user data, we will provide notice in advance to affected parties, teams, or individual users, unless we are legally prohibited from doing so or unless some circumstance exists that prevents us from doing so. This includes situations when disclosure could cause harm to specific people or jeopardize the security of our network.

I deleted a message in my Slack team. Is it gone?

On free Slack teams, if you're able to delete a message, that message is marked for deletion and permanently deleted within a matter of days.

If you're a member of a paid Slack team, your team administrator may have selected a message retention option to keep all messages, even if they have been deleted by the user. View your team's settings to learn more.

What is the default message retention setting?

The default Slack message retention setting for all teams is to retain all messages in channels, private groups, and DMs, for all team members, for as long as the team exists.

With the default settings in place, if a message is edited, only the last edited version of the message is retained. If a message is deleted, it is removed from the archive.

What message retention options exist for paid teams?

Once a team has moved to a paid version of Slack, administrators can manage message retention settings in a much more granular way. Messages can be automatically deleted in as little as a day, week, or month.

Administrators can also increase the scope of message retention by retaining all versions of edited and deleted messages for channels, private groups, and direct messages for a set time period.

Administrators also gain the ability to manage retention settings across all channels uniformly, or on a per-channel basis.

Do message retention settings apply to files?

No. Files can be shared in multiple channels and groups or private to an individual, so message retention settings do not apply. The person who uploads the file can view and delete that file at any time. Administrators may also delete files that are shared to their team.

Can I delete my Slack account?

Team members have the ability to deactivate their own Slack account. In addition, administrators can deactivate accounts for any users on their team. Deactivation does not fully delete accounts, so that team members may be reactivated at a later date.

Before deactivating their account, a user can edit any of their profile fields to omit or include any information they like, and can delete all optional fields completely.

And from the Slack privacy policy:

Log data. When you use Slack, our servers automatically record information, including information that your browser sends whenever you visit a website or your mobile app sends when you're using it. This log data may include your Internet Protocol address, the address of the web page you visited before coming to Slack, your browser type and settings, the date and time of your request, information about your browser configuration and plug-ins, language preferences, and cookie data. Log data does not contain message content and is not routinely deleted.

Disclose content removal requests. Slack does disclose the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Slack opposes the compelled inclusion of deliberate security weaknesses. Anne Toth, Slack's Vice President of People, Policy and Compliance, stated:

Transparency is a key value for us and an important feature in Slack itself. It's this commitment to transparency that brings me to my last point — Slack opposes government-mandated “back-doors” of any kind but particularly a government-mandated requirement that would compromise data security.



Snapchat

Snapchat earns three stars in this year's *Who Has Your Back* report. This is Snapchat's second year in the report, and it has adopted many of the best practices we are highlighting in this report. We appreciate the steps Snapchat has made to stand by its users, but there is more to be done. Specifically, Snapchat should have a stronger policy of notifying users about government requests.

Industry-Accepted Best Practices. Snapchat requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Process required for message content: A federal or state search warrant is required for requests that include message content.

In addition to a law enforcement guide, Snapchat publishes a transparency report.

Inform users about government data demands. Snapchat does not promise to provide advance notice to users about government data demands.

Disclose data retention policies. Snapchat publishes information about its data retention policies, including retention of IP addresses and deleted content:

The reason Snapchat often will not be able to retrieve message content is that Snapchat deletes each Snap from its servers once all recipients have viewed it. And even when a Snap remains unopened, it will be deleted 30 days after it was first sent.

...

Snapchat retains different types of user information for different periods of time. Snapchat honors valid law enforcement preservation requests made during the period the requested user information is available.

Basic Subscriber information: The basic subscriber information entered by a user in creating an account is maintained as long as the user has not edited the information or removed the information from the account. Once the user makes a change, the previously existing information is overwritten. Upon receipt of a preservation request, however, Snapchat can capture the user

information available at that time; and future actions by the user will not affect the preserved user information. Snapchat also retains logs containing IP addresses associated with account login and logout for a limited period of time after the user has deleted his or her Snapchat account.

Disclose content removal requests. Snapchat does not retain content for long periods of time, and thus this category does not apply.

Pro-user public policy: oppose backdoors. In a public, official written format, Snapchat opposes the compelled inclusion of deliberate security weaknesses. In its transparency report, Snapchat states:

Privacy and security are core values here at Snapchat and we strongly oppose any initiative that would deliberately weaken the security of our systems. We're committed to keeping your data secure and we will update this report bi-annually.



Sonic

Sonic earns five stars in this year's *Who Has Your Back* report. This is Sonic's fourth year in the report, and it has consistently adopted every best practice we've identified as part of this report. We commend Sonic for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. Sonic requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Sonic.net, Inc. / Sonic Telecom will not provide user content without a U.S. search warrant

In addition to a law enforcement guide, Sonic publishes a transparency report.

Inform users about government data demands. Sonic promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

For criminal legal process - Sonic.net will notify customers upon receipt of criminal legal process seeking information about their accounts unless prohibited by law. Please note: If due to emergency threat to life, or legal process prohibits notification, Sonic will notify customer after emergency has ended, or once suppression order expires.

Disclose data retention policies. Sonic publishes information about its data retention policies, including retention of IP addresses and deleted content:

Record Retention Timeline

The following retention policies generally apply to frequently sought records:

Dynamic IP Assignment Logs: 0-14 Days

VPN IP Assignment Logs: 14 Days

Static IP Assignment Logs: Indefinite Toll Call Records: 18 Months

Preservation Requests: 90 Days

Disclose content removal requests. Sonic discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Sonic opposes the compelled inclusion of deliberate security weaknesses. In its 2014 transparency report, Sonic states:

Finally, we are stating for the record our position regarding compelled inclusion of back doors, deliberate security weaknesses or disclosure of encryption keys. Sonic does not support these practices.



Tumblr

Tumblr earns three stars in this year's *Who Has Your Back* report. This is Tumblr's third year in the report, and it has adopted several of the best practices we are highlighting in this report. We appreciate the steps Tumblr has taken to stand by its users, but there is room for improvement. Tumblr should disclose its data retention policies and the number of government content removal requests it receives.

Industry-Accepted Best Practices. Tumblr requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures, based on a showing of probable cause, is required to compel disclosure of the stored contents of any account, such as blog posts or messages.

In addition to a law enforcement guide, Tumblr publishes a transparency report.

Inform users about government data demands. Tumblr promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Tumblr respects its users' rights and privacy. Tumblr's policy is to notify its users about requests for their information, and to provide them with copies of the legal process underlying those requests. This sort of notice is necessary so that affected users have the chance, if they wish, to challenge those requests. In some cases, Tumblr may be prohibited by law from providing notice, such as when we receive a non-disclosure order pursuant to 18 U.S.C. § 2705(b). In these situations, Tumblr's policy is to notify the affected users after the non-disclosure period has elapsed.

In exceptional circumstances, such as cases involving the sexual exploitation of a child, Tumblr may elect not to provide user notice before complying with the request. If an investigation involves such an exceptional circumstance, law enforcement should provide a description of the situation for us to

evaluate. In these exceptional circumstances, Tumblr's policy is to notify the affected users 90 days after the time we respond to the request.

Disclose data retention policies. Tumblr does not publish information about its data retention policies, including retention of IP addresses and deleted content.

Disclose content removal requests. Tumblr does not disclose the number of times governments seek the removal of user content or accounts, and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Tumblr opposes the compelled inclusion of deliberate security weaknesses. In its transparency report, Tumblr states:

Security: we believe that no government should install backdoors into web security protocols, or otherwise compromise the infrastructure of the internet. We'll fight the laws that allow them to do so, and we'll work to secure our users' data against such intrusions



Twitter

Twitter earns four stars in this year's *Who Has Your Back* report. This is Twitter's fifth year in the report, and it has adopted many of the best practices we've identified as part of this report. We appreciate the steps Twitter has taken to stand up for its users, but more can be done. Twitter should strengthen its policy for notifying users of government requests.

Industry-Accepted Best Practices. Twitter requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Requests for the contents of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter.

In addition to a law enforcement guide, Twitter publishes a transparency report.

Inform users about government data demands. Twitter promises to provide advance notice to users about government data demands, but does not promise to provide notice after an emergency has ended or a gag has been lifted. Instead, Twitter says that it *may* provide post-notice:

Yes. Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies; account compromises). We may also provide post-notice to affected users when prior notice is prohibited.

While we appreciate Twitter's forward progress on this issue, we urge it to go further and promise to give all users notice of government attempts to access their data.

Disclose data retention policies. Twitter publishes information about its data retention policies, including retention of IP addresses and deleted content:

Log Data: When you use our Services, we may receive information (“Log Data”) such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device information (including device and application IDs), search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your account to authenticate to a third-party website or application, or visit a third-party website that includes a Twitter button or widget. We may also receive Log Data when you click on, view or interact with links on our Services, including links to third-party applications, such as when you choose to install another application through Twitter. Twitter uses Log Data to provide, understand, and improve our Services, to make inferences, like what topics you may be interested in, and to customize the content we show you, including ads. If not already done earlier, for example, as provided below for Widget Data, we will either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after a maximum of 18 months.

and also

You can also permanently delete your Twitter account. If you follow the instructions here, your account will be deactivated and then deleted. When your account is deactivated, it is not viewable on Twitter.com. For up to 30 days after deactivation it is still possible to restore your account if it was accidentally or wrongfully deactivated. Absent a separate arrangement between you and Twitter to extend your deactivation period, after 30 days, we begin the process of deleting your account from our systems, which can take up to a week.

Disclose content removal requests. Twitter discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Twitter opposes the compelled inclusion of deliberate security weaknesses. Twitter signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.



Verizon

Verizon earns two stars in this year's *Who Has Your Back* report. This is Verizon's fifth year in the report, and it has adopted some of the best practices we've identified as part of this report. We appreciate the steps Verizon has taken to stand by its users, but there is room for improvement. Verizon should have a stronger policy of informing users of government requests, disclose its data retention policies, and take a public position opposing back doors.

Industry-Accepted Best Practices. Verizon requires a warrant before giving content to law enforcement, stating in its transparency report:

“Stored content” refers to communications or other data that our users create and store through our services, such as text messages, email or photographs. We require a warrant before disclosing stored content to law enforcement, absent an emergency involving the danger of death or serious physical injury. Non-content refers to records we create such as subscriber information that a customer provides at the time she signs-up for our services, and transactional information regarding the customer's use of our services, such as phone numbers that a customer called.

Verizon publishes a combined transparency report and law enforcement guide.

Inform users about government data demands. Verizon does not promise to provide advance notice to users about government data demands.

Disclose data retention policies. Verizon does not publish information about its data retention policies, including retention of IP addresses and deleted content.

Disclose content removal requests. Verizon discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Verizon does not oppose the compelled inclusion of deliberate security weaknesses.



WhatsApp

WhatsApp earns one star in this year's *Who Has Your Back* report. This is WhatsApp's first year in the report, and although EFF gave the company a full year to prepare for its inclusion in the report, it has adopted none of the best practices we've identified as part of this report. We appreciate the steps that WhatsApp's parent company Facebook has taken to stand by its users, but there is room for WhatsApp to improve. WhatsApp should publicly require a warrant before turning over user content, publish a law enforcement guide and transparency report, have a stronger policy of informing users of government requests, and disclose its data retention policies. WhatsApp does get credit for Facebook's public position opposing back doors, and we commend Facebook for that.

Industry-Accepted Best Practices. WhatsApp does not publicly require a warrant before giving content to law enforcement. WhatsApp does not publish a transparency report or a law enforcement guide.

Inform users about government data demands. WhatsApp does not promise to provide advance notice to users about government data demands.

Disclose data retention policies. WhatsApp does not publish information about its data retention policies, including retention of IP addresses and deleted content.

Disclose content removal requests. WhatsApp does not host content nor do we have reason to believe it receives account closure requests domestically, and thus this category is not applicable.

Pro-user public policy: oppose backdoors. In a public, official written format, WhatsApp' parent company Facebook opposes the compelled inclusion of deliberate security weaknesses. On behalf of itself as well as WhatsApp, Facebook signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.



WICKR



Wickr

Wickr earns four stars in this year's *Who Has Your Back* report. This is Wickr's second year in the report, and it has adopted all of the best practices we've identified as part of this report. We commend Wickr for its strong stance regarding user rights, transparency, and privacy

Industry-Accepted Best Practices. Wickr requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Wickr requires a warrant supported by probable cause prior to handing over the content of user communications. Therefore, while we receive informal requests or inquiries from law enforcement around the world, we have yet to receive a single formal law enforcement/government request for information regarding our users or their accounts.

In addition to a law enforcement guide, Wickr publishes a transparency report.

Inform users about government data demands. Wickr, in its privacy policy, promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

We will always notify you of any third party requests for your information unless legally unable to do so. As soon as legally permitted to do so, we will notify our users of requests for their information.

Disclose data retention policies. In its privacy policy, Wickr publishes information about its data retention policies, including retention of IP addresses and deleted content:

Data Retention on Wickr's Servers: Our servers store the encrypted messages that you send and receive only long enough to ensure their reliable delivery to each device associated to your account. Undelivered messages are deleted

after 7 days. We retain non- message data (i.e. Types of messages) for as long as you use the Wickr Services and for an indefinite time thereafter.

Data Retention on Your Device: All messages are stored in encrypted form on end users' devices. You choose your own retention policy for your messages by choosing how long a message is viewable before it is deleted (via the self-destruct time for sent messages and manual deletion for your device).

Deleted messages cannot be recovered.

Disclose content removal requests. Wickr does not have access to user content, and thus this category does not apply.

Pro-user public policy: oppose backdoors. In a public, official written format, Wickr opposes the compelled inclusion of deliberate security weaknesses. In its 2014 transparency report, Wickr states:

At the beginning of this year, Wickr's CEO Nico Sell spoke publicly about saying no to an FBI backdoor which is why we are happy to see other companies fighting back against the government's overreaching behavior. Our belief is that while all governments must protect their citizens, we as citizens and as companies, must stand up for one of the pillars of freedom—privacy.



Wikimedia

Wikimedia earns five stars in this year's *Who Has Your Back* report. This is Wikimedia's second year in the report, and it has adopted all of the best practices we've identified as part of this report. We commend Wikimedia for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. Wikimedia requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

Your request must be legally valid and enforceable under US law and be in one of the following forms: ... A warrant issued under the procedures of the Federal Rules of Criminal Procedure or equivalent state warrant procedures, based upon a showing of probable cause -- if you are a government or law enforcement agency and are requesting disclosure of the contents of any user communication, nonpublic user content information, or any other information where a warrant is required by law;

In addition to a law enforcement guide, Wikimedia publishes a transparency report.

Inform users about government data demands. Wikimedia promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

We believe in transparency about when requests are made for our users' nonpublic information. This means that we will notify the user(s) affected by your request of your request and that we will report the receipt and resolution of your request in our transparency report.

When we receive your request, we will notify and provide a copy of your request to the affected user(s) at least 10 calendar days before we disclose

the requested information, provided that (1) we have contact information for the affected user(s); (2) disclosing your request will not create or increase a credible threat to life or limb; and (3) we are not otherwise prohibited by law or an order from a US court of competent jurisdiction, such as an order issued pursuant to 18 U.S.C. § 2705(b), from doing so. If we are unable to provide information about your request to affected users because disclosing it would create a credible threat to life or limb; or we are prohibited by law, we will provide information about your request to affected users that we have contact information for within a reasonable period after the threat or legal restriction has terminated.

If you are requesting disclosure of nonpublic user information that you believe requires confidentiality, please provide a legally valid and enforceable protective, sealing, or "gag" order from a US court of competent jurisdiction. Please note that we must receive notice of such protective, sealing, or gag order prior to the date the Wikimedia Foundation notifies the user for confidentiality to be considered.

Upon notification to the affected user(s), the user(s) will generally be provided at least 10 calendar days before we will disclose the requested information (assuming we find your request to be otherwise valid), during which time the affected user(s) may attempt to quash or otherwise legally challenge the request. If, prior to the disclosure, we receive notice from the affected user(s) that he or she intends to challenge your request, no information will be delivered until that legal challenge is resolved.

Disclose data retention policies. Wikimedia publishes highly detailed information about its data retention policies, including retention of IP addresses and deleted content, for example:

How long do we retain non-public data?

Unless otherwise indicated, we retain the following types of data for no more than the following periods of time:

Data type	Origin	Examples	Maximum Retention Period
Personal information	Collected automatically from a user	<ul style="list-style-type: none"> IP addresses of site visitors (operational data) IP addresses of A/B test subjects (analytical data) Identifying user-agent information of site visitors 	After at most 90 days, it will be deleted, aggregated, or anonymized
	Account settings	<ul style="list-style-type: none"> Email address 	Until user deletes/changes the account setting.
Non-personal information associated with a user account*	Collected automatically from a user	<ul style="list-style-type: none"> Data collected by MediaWiki about a user account's activity (e.g., first time a user goes to an edit page, date and time that a user verifies their email address) Data collected by EventLogging and associated with their user ID (e.g., whether an account was created on mobile, A/B test data for Getting Started) 	Indefinitely
	Provided by a user	<ul style="list-style-type: none"> Logs of terms entered into the site's search box, or terms within prefilled links to the search engine that have been followed by user navigation 	After at most 90 days, it will be deleted, aggregated, or anonymized
Non-personal information not associated with a user account*	Collected automatically from various users	<ul style="list-style-type: none"> Counts of how many times certain events have occurred (e.g. successful HTTPS requests) 	Indefinitely
Articles browsed by readers	Collected automatically from a reader	<ul style="list-style-type: none"> A list of articles visited by readers 	After at most 90 days, if retained at all, then only in aggregate form

(*) For the purposes of this table, "user account" means username, user ID, or IP address; "reader" means visitor to a Wikimedia project.

Disclose content removal requests. Wikimedia discloses the number of times governments seek the removal of user content or accounts, and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Wikimedia opposes the compelled inclusion of deliberate security weaknesses. Twitter signed a coalition letter organized by the Open Technology Institute, which stated:

We urge you to reject any proposal that U.S. companies deliberately weaken the security of our products... Whether you call them “front doors” or “back doors,” introducing intentional vulnerabilities into secure products for the government’s use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government’s own experts.



WordPress.com

WordPress.com earns five stars in this year's *Who Has Your Back* report. This is WordPress.com's third year in the report, and it has adopted all of the best practices we've identified as part of this report. We commend WordPress.com for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. WordPress.com requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

We require a warrant before disclosing content of user communications to government agencies/law enforcement. We also require a warrant before providing any non-public content information (such as private or draft post content, or pending comments).

In addition to a law enforcement guide, WordPress.com publishes a transparency report.

Inform users about government data demands. WordPress.com promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

As permitted by US law, we may disclose user information to the government or law enforcement, without a subpoena or warrant if we have a good faith belief that an emergency (danger of death or serious physical injury) requires disclosure of information related to the emergency without delay. We require emergency requests to be made in writing and include all the information available so that we may evaluate the urgency of the request. Additionally, we may ask for a subpoena, search warrant, or court order after the disclosure. In these circumstances our policy is still to notify users and provide them with a copy of any legal process regarding their account or site unless we are prohibited by law or court order from doing so. However, in some circumstances, notification may come after the information has been disclosed.

Disclose data retention policies. Wordpress.com publishes information about its data retention policies, including retention of IP addresses and deleted content:

We will generally retain the above information until changed or removed by the user (if it's possible to do so). We also collect log data, which may include a user's IP address, browser type, operating system. We keep this information for up to 30 days as a matter of course. You can read more about how we handle preservation requests under "Preservation Requests for WordPress.com Sites" below. ... We retain commenter information until the site owner of the site on which the comment appears deletes the comment.

Disclose content removal requests. Wordpress.com discloses the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Wordpress opposes the compelled inclusion of deliberate security weaknesses. In its legal guidelines, Wordpress states:

Some governments have recently sought to weaken encryption, in the name of law enforcement. We disagree with these suggestions and do not believe that it's feasible to include any deliberate security weaknesses or other back doors in encryption technologies, even if "only" for the benefit of law enforcement. As a wise man said, "there is no such thing as a vulnerability in technology that can only be used by nice people doing the right thing in accord with the rule of law." We agree wholeheartedly.



Yahoo

Yahoo earns five stars in this year's *Who Has Your Back* report. This is Yahoo's fifth year in the report, and just as it did last year, it has adopted every best practice we've identified as part of this report. We commend Yahoo for its strong stance regarding user rights, transparency, and privacy.

Industry-Accepted Best Practices. Yahoo requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

We will only disclose content (e.g. email messages, Flickr photos) with a search warrant or the user's consent.

In addition to a law enforcement guide, Yahoo publishes a transparency report.

Inform users about government data demands. Yahoo promises to provide advance notice to users about government data demands and will delay notice only in limited circumstances:

Provide Notice to Our Users. Our policy is to explicitly notify our users about third-party requests for their information prior to disclosure, and thereby provide them with an opportunity to challenge requests for their data. In some cases, we may be prohibited by law from doing so, such as when we receive a non-disclosure order pursuant to 18 U.S.C. § 2705(b). Additionally, in exceptional circumstances, such as imminent threats of physical harm to a person, we may elect to provide delayed notice. When the circumstance that prevented us from providing notice prior to disclosure is removed, e.g., the non-disclosure order expired or the threat has passed, we take steps to inform the affected user(s) that data was disclosed.

Disclose data retention policies. Yahoo publishes information about its data retention policies, including retention of IP addresses and deleted:

We retain different types of information for varied periods of time depending on a variety of factors, such as user account activity, user requests for deletion, and/or storage capacity. Generally, user login records for the past year are available in response to legal process. In many cases, our users

maintain control over the content they store on our network and may remove, alter, or otherwise modify such content at any time. As such, permanently deleted emails, for example, are not available in response to legal process. For more information on our data collection and storage policies, please see our Privacy Center.


























Disclose content removal requests. Yahoo does disclose the number of times governments seek the removal of user content or accounts and how often the company complies, including formal legal process as well as informal government requests.

Pro-user public policy: oppose backdoors. In a public, official written format, Yahoo opposes the compelled inclusion of deliberate security weaknesses. In its transparency report, Yahoo states:

We've encrypted many of our most important products and services to protect against snooping by governments or other actors. This includes encryption of the traffic moving between Yahoo data centers; making browsing over HTTPS the default on Yahoo Mail and Yahoo Homepage; and implementing the latest in security best-practices, including supporting TLS 1.2, Perfect Forward Secrecy and a 2048-bit RSA key for many of our global properties such as Homepage, Mail and Digital Magazines. We've also rolled out an end-to-end (e2e) encryption extension for Yahoo Mail, now available on GitHub. Our goal is to provide an intuitive e2e encryption solution for all of our users by the end of 2015. We are committed to the security of this solution and oppose mandates to deliberately weaken it or any other cryptographic system.

Appendix



















2014 Results Table

	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
 Adobe	★	★	★	★	★	★
 amazon.com	★	★	★	★	★	★
 Apple	★	★	★	★	★	★
 at&t	★	★	★	★	★	★
 COMCAST	★	★	★	★	★	★
 CREDO mobile	★	★	★	★	★	★
 Dropbox	★	★	★	★	★	★
 facebook	★	★	★	★	★	★
 foursquare	★	★	★	★	★	★
 Google	★	★	★	★	★	★
 Harvard Law School	★	★	★	★	★	★
 LinkedIn	★	★	★	★	★	★
 Lookout	★	★	★	★	★	★
 Microsoft	★	★	★	★	★	★
 myspace	★	★	★	★	★	★
 Pinterest	★	★	★	★	★	★
 Snapchat	★	★	★	★	★	★
 Sonic.net	★	★	★	★	★	★
 StumbleUpon	★	★	★	★	★	★
 tumblr	★	★	★	★	★	★
 Twitter	★	★	★	★	★	★
 Verizon	★	★	★	★	★	★
 Wickr	★	★	★	★	★	★
 WordPress	★	★	★	★	★	★
 YAHOO!	★	★	★	★	★	★

2013 Results Table

	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★
	★	★	★	★	★	★

2012 Results Table

	Tell users about data demands	Be transparent about government requests	Fight for user privacy in the courts	Fight for user privacy in Congress
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★

2011 Results Table

	Tell users about data demands	Be transparent about government requests	Fight for user privacy in the courts	Fight for user privacy in Congress
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★
	★	★	★	★

Removing Companies From Our Report

Who Has Your Back is designed to help users decide which popular technology companies to do business with, highlight the practices of some of the biggest players in the tech space, and draw awareness of some smaller companies that are outpacing large industry competitors. As the years have gone by, we've added more and more companies to the report.

However, we recognize that more doesn't always mean better. In fact, we fear that including too many companies may make the report overly complicated and hide important industry trends among the major players. We also acknowledge that some companies that had a larger user base in 2011 have seen a decline in users in subsequent years, while other companies are still doing important work for many users but don't actively host much sensitive user content.

With that in mind, we've removed several companies from this year's report to streamline and simplify the results. The following companies were removed: Foursquare, Internet Archive, LookOut, MySpace, and SpiderOak. To see how those companies rated previously, please see the 2014 *Who Has Your Back* report.⁹

⁹ Available at <https://www.eff.org/who-has-your-back-government-data-requests-2014>

References and Helpful Links

All current as of June 16, 2015

Open Technology Institute Coalition Letter Against Backdoors

https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf

Adobe

Law enforcement guide:

<https://www.adobe.com/legal/compliance/law-enforcement.html>

Transparency report:

<https://www.adobe.com/legal/compliance/transparency.html>

Amazon

Law enforcement guide:

http://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

Transparency report:

http://d0.awsstatic.com/certifications/Transparency_Report.pdf

Privacy notice:

<http://www.amazon.com/gp/help/customer/display.html?nodeId=468496>

Conditions of use:

https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088

Privacy and data security blog post:

<http://blogs.aws.amazon.com/security/post/Tx35449P4T7DJIA/Privacy-and-Data-Security>

Apple

Law enforcement guide:

<https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf>

Transparency report:

<https://www.apple.com/privacy/transparency-reports/>

Government information requests:

<https://www.apple.com/privacy/government-information-requests>

AT&T

Law enforcement guide:

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html>

and

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/location-demands.html>

and

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/emergency-requests.html>
and

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/international.html>
and

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/partial-or-no-data-provided.html>
Transparency report:

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>
and

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html#sthash.BMutOWAH.dpuf>

Comcast

Law enforcement guide:

<http://www.comcast.com/~ /Media/403EEED5AE6F46118DDBC5F8BC436030.aspx>

Transparency report:

<http://corporate.comcast.com/images/Third-Comcast-Transparency-Report-2H2014-FINAL-02022015.pdf>

Privacy notice:

<http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html?CCT=53BA3D76CB1473BFF49C79FE4AA86DFF1EE2DE626F409A592CC8FD4F97F987FDED44763A4B54572047B30DDBC6AEBC5DCED6A73183C574B8E5697D9E3FD17293EB4FE71DF37B56C34FF77B9D0E092477A8C3958E8CC866906A7E34373B5718A30AEEF8F52C31E24CFFD314BC83C96E756A5AA0BA63C22EBO#When%20is%20Comcast%20required%20to%20disclose%20personally%20identifiable%20information%20and%20CPNI%20by%20law?>

Statement on Upgrading the Security and Privacy of Your Email:

<http://corporate.comcast.com/comcast-voices/upgrading-the-security-and-privacy-of-your-email>

CREDO Mobile

Law enforcement guide:

<http://www.credomobile.com/law-enforcement-guidelines>

Transparency report:

<http://www.credomobile.com/transparency>

Privacy and security policy:

<http://www.credomobile.com/privacy>

Dropbox

Transparency report:

<https://www.dropbox.com/transparency>

Government Data Request Principles:
<https://www.dropbox.com/transparency/principles>

Facebook

Law enforcement guidelines:
<https://www.facebook.com/safety/groups/law/guidelines/>
Transparency report:
<https://govtrequests.facebook.com/>
Data policy:
https://www.facebook.com/full_data_use_policy

Google

Legal process:
<https://www.google.com/transparencyreport/userdatarequests/legalprocess/>
Transparency report:
<https://www.google.com/transparencyreport/>
Dashboard data:
<https://support.google.com/accounts/answer/162743?hl=en>
Government requests to remove content:
<https://www.google.com/transparencyreport/removals/government/>

LinkedIn

Law enforcement guidelines:
https://help.linkedin.com/app/answers/detail/a_id/16880/~ /linkedin-law-enforcement-data-request-guidelines
Transparency report:
<https://www.linkedin.com/legal/transparency>
Data request guidelines:
<https://help.linkedin.com/ci/fattach/get/4773861/1431363803/redirect/1/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf>

Microsoft

Principles, policies, and practices FAQ (law enforcement guidelines and other information):
<https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/>
Transparency report
<https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>
U.S. National Security Order Requests:
<https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/fisa/>
Privacy statement:
<http://www.microsoft.com/privacystatement/en-us/core/default.aspx#EHC>
When transparency alone isn't enough:
<http://blogs.microsoft.com/on-the-issues/2015/03/27/when-transparency-alone-isnt-enough/>

Pinterest

Law enforcement guidelines:

<https://help.pinterest.com/en/articles/law-enforcement-guidelines>

Transparency report:

<https://help.pinterest.com/en/articles/transparency-report-archive>

Terms of service:

<https://about.pinterest.com/en/terms-service>

reddit

Transparency report (including law enforcement guidelines)

<https://www.reddit.com/wiki/transparency/2014>

What information we collect:

https://www.reddit.com/help/privacypolicy#section_what_information_we_collect

Slack

User data request policy:

<https://slack.com/user-data-request-policy>

Transparency report:

<https://slack.com/transparency-report>

Slack and transparency:

<http://slackhq.com/post/117871977170/transparency>

FAQ about privacy policy:

<https://slack.zendesk.com/hc/en-us/articles/203950296-FAQs-about-Slack-s-Privacy-Policy>

Privacy policy:

<https://slack.com/privacy-policy>

Snapchat

Law enforcement guidelines:

https://www.snapchat.com/static_files/lawenforcement.pdf?version=20150604

Transparency report:

<http://blog.snapchat.com/post/115310648870/our-transparency-report>

Sonic

Law enforcement guidelines:

https://wiki.sonic.net/images/0/05/Sonic.net_Legal_Process_Policy.pdf

Transparency report:

<https://corp.sonic.net/ceo/2014/04/28/2013-transparency-report/>

Tumblr

Law enforcement guidelines:

https://www.tumblr.com/docs/en/law_enforcement

Transparency report:

<https://www.tumblr.com/transparency>

Twitter

Law enforcement guidelines:

<https://support.twitter.com/articles/41949-guidelines-for-law-enforcement>

Transparency report:

<https://transparency.twitter.com/>

Privacy policy

<https://twitter.com/privacy?lang=en>

Verizon

Transparency report and law enforcement guide:

<http://transparency.verizon.com/us-report?/us-data>

<http://transparency.verizon.com/international-report>

Wickr

Law enforcement guide

https://wickr.com/wp-content/uploads/2014/06/Law-Enforcement-Guidelines_5.12.14.pdf

Transparency report:

<https://wickr.com/category/transparency-report/>

Privacy policy:

<https://wickr.com/privacy-policy/>

Wikimedia

Law enforcement guide:

https://wikimediafoundation.org/wiki/Requests_for_user_information_procedures_%26_guidelines#What_We_Require_From_You

Transparency report:

<https://transparency.wikimedia.org>

and

<https://transparency.wikimedia.org/content.html>

Data retention guidelines:

https://meta.wikimedia.org/wiki/Data_retention_guidelines

WordPress.com

Law enforcement guide:

<https://en.support.wordpress.com/disputes/legal-guidelines/>

Transparency report:

<http://transparency.automattic.com/>

Takedown demands:

<http://transparency.automattic.com/takedown-demands/>

Yahoo

Transparency report:

<https://transparency.yahoo.com/>

Law enforcement guide:

<https://transparency.yahoo.com/law-enforcement-guidelines/us/index.htm>

Content removals:

<https://transparency.yahoo.com/government-removal-requests/index.htm>

Users first statement:

<https://transparency.yahoo.com/users-first/index.htm>