Who Has Your Back?
2017

THE ELECTRONIC FRONTIER FOUNDATION'S SEVENTH ANNUAL REPORT ON

Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data

Nate Cardozo, Senior Staff Attorney

Andrew Crocker, Staff Attorney

Jennifer Lynch, Senior Staff Attorney

Kurt Opsahl, Deputy Executive Director and General Counsel

Rainey Reitman, Activism Director

July 2017

Authors: Nate Cardozo, Andrew Crocker, Jennifer Lynch, Kurt Opsahl, Rainey Reitman
With assistance from: Hugh D'Andrade, Gennie Gebhart

A publication of the Electronic Frontier Foundation, 2017

Table of Contents

Executive Summary

In this era of unprecedented digital surveillance and widespread political upheaval, the data stored on our cell phones, laptops, and especially our online services are a magnet for government actors seeking to track citizens, journalists, and activists.

In 2016, the United States government sent at least 49,868 requests to Facebook for user data. In the same time period, it sent 27,850 requests to Google and 9,076 to Apple.[1] These companies are not alone: where users see new ways to communicate and store data, law enforcement agents see new avenues for surveillance.

There are three safeguards to ensure that data we send to tech companies don't end up in a government database: technology, law, and corporate policies. Technology—including the many ways data is deleted, obscured, or encrypted to render it unavailable to the government—is beyond the scope of this report.[2] Instead, we'll focus on law and corporate policies. We'll turn a spotlight on how the policies of technology companies either advance or hinder the privacy rights of users when the U.S. government comes knocking,[3] and we'll highlight those companies advocating to shore up legal protections for user privacy.

Since the Electronic Frontier Foundation started publishing *Who Has Your Back* seven years ago, we've seen major technology companies bring more transparency to how and when they divulge our data to the government. This shift has been fueled in large part by public attention. The Snowden revelations of 2013 and the resulting public conversation about digital privacy served as a major catalyst for widespread changes among the privacy policies of big companies. While only two companies earned credit in all of our criteria in 2013 (at a time when the criteria were somewhat less stringent than today[4]), in our 2014 report, there were nine companies earning credit in every category.

Today, technology users expect tech companies to have transparency around government access to user data, and to stand up for user privacy when appropriate. And companies are increasingly meeting those expectations.

But there are still many companies that lag behind, fail to enact best practices around transparency, or don't prioritize standing up for user privacy.

The role of *Who Has Your Back* is to provide objective measurements for analyzing the policies and advocacy positions of major technology companies when it comes to handing data to the government. We focus on a handful of specific, measurable criteria

that can act as a vital stopgap against unfettered government access to user data. Through this report, we hope to galvanize widespread changes in the policies of technology companies to ensure our digital lives are not subject to invasive and undemocratic government searches.

2017 Results Table

	Follows industry-wide best practices	Tells users about government data requests	Promises not to sell out users	Stands up to NSL gag orders	Pro-user public policy: Reform 702
Adobe	★	★	★	★	★
airbnb	★			★	★
amazon.com	★				★
	★	★	★	★	
at&t	★				
COMCAST	★				
CREDO mobile	★	★	★	★	★
Dropbox	★	★	★	★	★
	★	★	★		★
Google	★	★	★		★
LinkedIn	★	★	★		★
lyft	★	★	★	★	★
Microsoft	★	★	★		★
Pinterest	★	★	★	★	★
slack	★		★	★	★
Snap Inc.	★		★		★
SONIC.	★	★	★	★	★
T-Mobile	★				
tumblr.	★	★			★
	★		★		★
UBER	★	★	★	★	★
verizon	★				
WhatsApp	★				★
WICKR	★	★	★	★	★
WordPress.com	★	★	★	★	★
YAHOO!	★	★	★		★

Major Findings and Trends

Our major findings include:

- **Every company we evaluate has adopted baseline industry best practices, such as publishing a transparency report and requiring a warrant before releasing user content to the government.**
- **Nine companies are receiving credit in all five categories: Adobe, Credo, Dropbox, Lyft, Pinterest, Sonic, Uber, Wickr, and Wordpress.**
- **The four lowest performing companies are all telecoms: AT&T, Comcast, T-Mobile, and Verizon.**
- **Amazon and WhatsApp's policies fall short of other similar technology companies.**

We are pleased to announce that nine companies earned stars in every category we evaluated in this year's report: **Adobe, Credo, Dropbox, Lyft, Pinterest, Sonic, Uber, Wickr** and **Wordpress**. Not only that, but each of these companies has a track record of defending user privacy. Lyft and Uber both earned credit in each of our categories for both years they have been in our report. Credo and Sonic have earned credit for standing up for transparency and user privacy in every category we evaluate for as long as they have been included in our report. The other all-star companies—Adobe, Dropbox, Pinterest, Wickr, and Wordpress—have improved their policies over the years, and are recognized repeatedly in this annual report for adopting the best practices around privacy and transparency.

Earning credit in every category year after year is no small feat. EFF has made important adjustments to our criteria each year to ensure that our criteria are strong yet practical, and to work to eliminate loopholes and uncertainty in language. For example, a company that received credit for providing users notice of government requests in 2011 needed simply to state that the company had a policy of providing users with notice. Over the years, this category has become increasingly more stringent, so that today this category requires that users be notified *before* data is handed to the government except in limited and defined circumstances (see *Overview of Criteria* below). The company must also promise to provide notice to the user after an emergency has been resolved or a gag order lifted. As a result, some companies that received credit in this category in the past find their policies do not meet the heightened standard.

Unfortunately, even as the industry as a whole has shifted toward transparency and privacy, there are many companies that are falling short. In particular, telecommunications companies like AT&T, Comcast, T-Mobile, and Verizon are failing to live up to larger tech industry practices. When it comes to adopting policies that prioritize user privacy over facilitating government data demands, the telecom industry for the most part has erred on the side of prioritizing government requests.

But telecommunications companies can do better. For example, Credo Mobile has repeatedly proven that telecom companies can adopt policies that earn credit in every category year after year. Similarly, Sonic, an ISP competitor to AT&T, Comcast, T-Mobile, and Verizon, has now earned credit in every category of EFF's annual report for five years.

We were disappointed that two technology companies fell short of other online services: Amazon and WhatsApp. While both companies have adopted industry-accepted best practices of requiring a warrant for content, publishing law enforcement guidelines, and publishing a transparency report, and while we applaud both companies for advocating for reforms to overbroad NSA surveillance, these two companies are not acting as leaders in other criteria that we examine. They don't have the strong public policies related to notifying users of government data requests that we have come to expect from tech companies, they don't publicly promise to request judicial review of NSLs, and they aren't meeting our criterion about not selling out users. We urge both Amazon and WhatsApp to improve their policies in the coming year so they match the standards of other major online services.

We are also concerned that too few companies are taking advantage of the powerful legal protections available to companies to protect user privacy. Congress created a new process in 2015 ensuring that technology companies have a right to request judicial review of the gag orders accompanying all National Security Letters (NSLs) that they receive. NSLs are akin to subpoenas requiring service providers—including technology companies, phone companies, and ISPs—to hand over data to the FBI about users' private communications and Internet activity. These orders are almost always accompanied by gag orders preventing the recipients from ever revealing the letter's existence and which have contributed to widespread abuse of this investigatory tool. Many companies are not yet taking full advantage of the newly enacted authority to request judicial review of the gag orders accompanying NSLs. Technology companies that had previously led the way on user transparency and privacy by earning credit in every one of EFF's categories—including Facebook, Google, and Twitter—have not yet publicly committed to requesting judicial review of all NSLs. In fact, fewer than half of the companies we evaluated have made this commitment: Adobe, Airbnb, Apple, Credo, Dropbox, Lyft, Pinterest, Slack, Sonic, Uber, Wickr, and Wordpress. We applaud these companies that have taken a public stand to ensure judicial oversight of gag orders and urge others within the technology space to do the same.

It's also clear that the technology industry is working to overhaul some of the fundamentally flawed laws in the United States around government access to user data. Twenty-one of the companies we evaluated have publicly called for significant reforms to Section 702, as enacted by the FISA Amendments Act of 2008. This is the law underpinning much of the NSA's mass surveillance of the Internet. In an ever-changing landscape of technology policy, it is not enough to sit on the sidelines; technology

companies can and should join their users in advocating for technology user rights in the halls of Congress.

Overview of Criteria

Only **publicly available** positions can qualify for credit in this report. Positions, practices, or policies that are conveyed privately or internal corporate standards, regardless of how laudable, are not factored into our decisions to award companies credit in any category.

Requiring public documentation serves several purposes. First, it ensures that companies cannot quietly change an internal practice in the future in response to government pressure, but must also change their publicly posted policies—which can be noted and documented. Second, by asking companies to put their positions in writing, we can examine each policy closely and prompt a larger public conversation about what standards tech companies should strive for. Third, it helps companies review one another's policies around law enforcement access, which can serve as a guide for startups and others looking for examples of companies standing up for user privacy.

In this report, we strive to offer ambitious but practical standards. To that end, we only include criteria that at least one technology company has already adopted. This ensures that we are highlighting existing and achievable best practices, rather than theoretical policies.

Each year, we review the criteria we used in prior years and make any adjustments that may be necessary to ensure the report is keeping pace with modern technology policy trends. A full explanation of the criteria from prior years is available in the full reports for each year.

We analyzed five criteria for this report.

1. Follows Industry-Wide Best Practices. This is a combined category that measures companies on three criteria (which were each listed separately in some earlier reports):

- The company must have a public, published policy requiring the government to obtain a warrant from a judge before the company discloses the content of user communications.
- The company must have published a transparency report since April 1, 2016, and the report should include useful data about how many times governments sought user data and how often the company provided user data to governments.
- The company must have public, published law enforcement guides explaining how it responds to data demands from the government.

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

2. Tells Users About Government Data Requests. To earn a star in this category, technology companies must promise to tell users when the U.S. government seeks their data in advance of turning over any data unless prohibited by law, in very narrow and defined emergency situations,[5] or unless doing so would be futile or ineffective.[6] Notice gives users a chance to defend themselves against overreaching government demands for their data, and thus we do not credit companies that delay notice to a user based on any other justification from an agency—for instance, where the agency claims notice might jeopardize an investigation, delay a trial, or otherwise deserves confidentiality. We recognize that in emergency situations involving danger of death or serious physical injury to any person, prior notice may not be possible. However, companies must have public-facing policies in place to give the user notice when the gag expires or the emergency is over.

3. Promises Not to Sell Out Users. To earn credit, a technology company must have a public policy that ensures data is not flowing to the government outside of its law enforcement guidelines—for example, through voluntary contracts or via a third party vendor who sells data to the government. We look for two things: first, some indication that the law enforcement guidelines fully describe data disclosures to the government; and second, that third parties (such as vendors and contractors) must adhere to the disclosure standards set forth by the company policies. Statements that indicate a company does not disclose user data to third parties will also suffice for the second part of our standard. We review corporate policies to ensure that there are no unusual exceptions for certain types of vendors, contractors, or other third parties who would then not be bound by the corporate policies. We allow exceptions for companies and third parties that, to the extent allowed by law, voluntarily share data with law enforcement or intelligence agencies directly for emergency access, to report crimes where the company or its customers are themselves victims, or to share computer security threat indicators.

4. Stands Up to NSL Gag Orders. Secret government requests for user data are a significant problem made all the worse by the indefinite gag orders that accompany them. Since the passage of the USA FREEDOM Act in mid-2015, companies have a new way to push back against one type of indefinite gag order: those accompanying National Security Letters (NSLs). To earn a star in this category, companies must publicly commit to invoking the available statutory procedures to have a judge review every indefinite NSL gag order the company receives.

5. Pro-User Public Policy: Reform 702. This year, Congress will be reviewing the surveillance powers of the National Security Agency, specifically considering whether to reauthorize Section 702, as enacted under the FISA Amendments Act of 2008. This provision of law is the legal lynchpin for the NSA's mass Internet surveillance that impacts the communications of countless Americans. We are awarding credit to companies that support reforming Section 702 in order to reduce the collection of information on innocent people. Public positions in support of allowing this provision of

law to expire completely will also receive credit, as this would also have the effect of reducing the surveillance of innocent people. Commitments must be formal, in the company's own name,[7] and either in writing or part of Congressional testimony. Only statements after June 2, 2015 will qualify.[8] Note that this category does not award credit for supporting reforms that do not reduce the collection of data on people (for example, reforms that increase transparency around surveillance practices), though we acknowledge that oversight and other reforms also serve an important role.

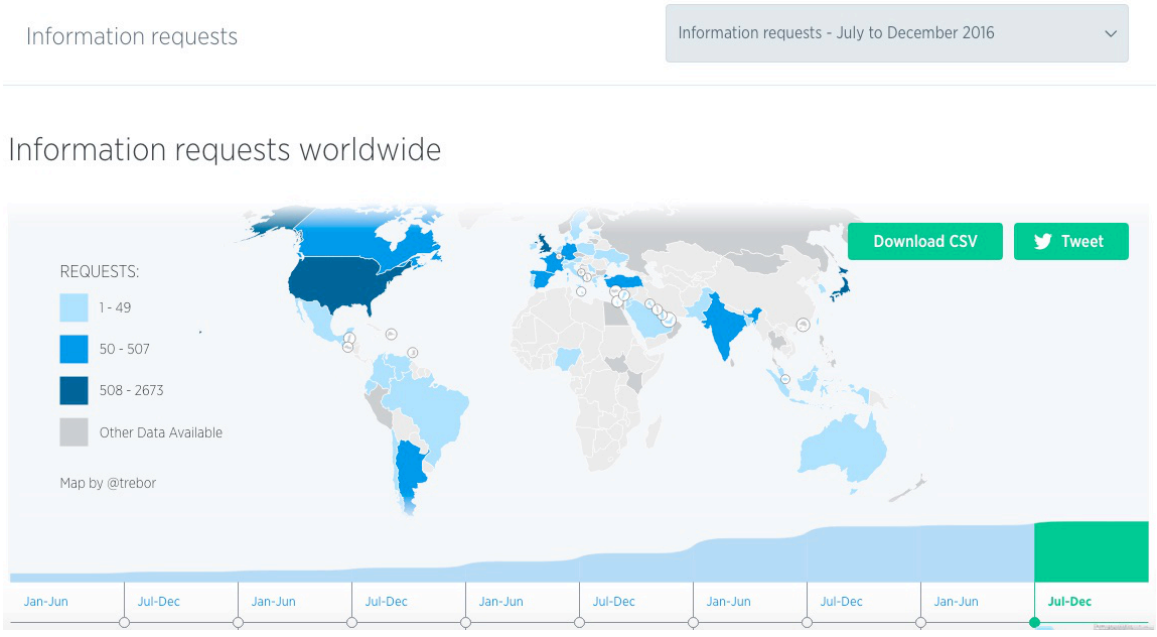
We expect this category to continue to evolve in the coming years, so that we can track industry players across a range of important privacy issues.

Deep Dive and Analysis of Select Corporate Policies

Follows Industry-Wide Best Practices

Over the last seven years, certain transparency practices that once seemed unusual have become the default. This year, all twenty-six of the companies we evaluated received credit for adopting industry-accepted best practices of publishing law enforcement guides, requiring a warrant before disclosing user content to the government, and publishing a transparency report.

However, there are some companies striving to make this information more useful and accessible. We are especially impressed by the transparency report from Twitter, which allows users to download a CSV of data, displays a month-by-month trend graph for government data requests on a per-country basis, and provides a map that showcases global trends in government data requests at a glance. It also provides a narrative analysis of interesting changes and trends in the data.



We also appreciate that many companies require a warrant not only for stored content such as videos and messages, but also for location data. Facebook's warrant requirement is a strong example of this:

> 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, timeline posts, and location information.

The warrant for content standard was inspired by the 2010 decision in *United States v. Warshak*, a case in which the Sixth Circuit Court of Appeals held that the Fourth Amendment protects email stored with email service providers, and the government must have a search warrant before it can seize those messages. This decision was critical for Internet privacy, but is only the opinion of one appeals court—and so is not binding throughout the entire country. When we first introduced the warrant for content standard to our *Who Has Your Back* report in 2013, many companies did not receive credit. We are glad to see that *every* company in our report now meets this standard.

Every company in our report also publishes law enforcement guidelines. These documents help provide a glimpse into the process and standards companies use for analyzing government requests for user data. It may, for example, indicate whether companies charge the government for providing user data. We encourage companies to charge money for fulfilling government requests for user data as this will serve as a small but measurable financial disincentive from submitting overly broad requests for user information.

Tells Users About Government Data Requests

Of the twenty-six companies we evaluated, sixteen promised to tell impacted users before surrendering data to the government. While companies could delay notification for a limited set of emergencies, a gag order, or when providing notice would be futile, companies had to commit to providing notice after the emergency was over or the gag had expired.

A particularly strong example of this type of notification policy is Pinterest's policy, which has clear, strong language indicating that notice will be provided after a court or emergency situation has expired:

> 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:
>
> - we are legally prohibited from providing notice (e.g. by an order under 18 U.S.C. § 2705(b));

- an emergency situation exists involving a danger of death or serious physical injury to a person;
- 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.

Wordpress has a similarly strong, clear policy, stating that it will give users a copy of the legal process and will provide a user with 7 days or more to legally challenge the order, and even provides additional delay if the user indicates she will be challenging the request:

> It is our policy to notify users and provide them with a copy of any civil or government legal process regarding their account or site (including formal requests for private information), unless we are prohibited by law or court order from doing so. In those cases, we will notify users and provide them with a copy of the legal process when the prohibition expires.
>
> If a request for information is valid, we will preserve the necessary information before informing the user. In most cases, upon notification to the user, that user will be provided with either 7 days or the amount of time before the information is due, whichever is later, during which time the user may attempt to quash or legally challenge the request. If, prior to the deadline, we receive notice from user that he or she intends to challenge a request, no information will be delivered until that process concludes. We also review the information requests received and may lodge our own challenge to the scope or validity of legal process received, on behalf of a user, whether or not the user pursues his/her own legal challenge.

Promises Not to Sell Out Users

This is the first year that we've included this criterion in our *Who Has Your Back* report, and we found a wide range of policies among technology companies.

This category was inspired by a policy promoted by Twitter late last year in the wake of a contentious U.S. presidential election that resulted in widespread political upheaval. Twitter's policy is designed to prevent its API developers from creating tools that could be utilized by the government for surveillance. This policy, promoted in 2016 but apparently extant prior to that, is in place even though Twitter accounts are public by default and commonly used for public discourse. Twitter's policy states:

> **To be clear:** We prohibit developers using the Public APIs and Gnip data products from allowing law enforcement — or any other entity — to use Twitter

> data for surveillance purposes. Period. The fact that our Public APIs and Gnip data products provide information that people choose to share publicly does not change our policies in this area. And if developers violate our policies, we will take appropriate action, which can include suspension and termination of access to Twitter's Public APIs and data products.

Other technology companies have followed Twitter's example. Microsoft offers especially strong language on this topic:

> Q: Do you enable third parties to assist governments in conducting voluntary surveillance of your customers?
> A: We are aware of reports that some providers have developed tools that third parties use to voluntarily assist governments in conducting surveillance of that provider's users. We do not design tools to enable voluntary surveillance of our users. If we ever provide third parties with access to data about our customers, we expect those third parties to handle that data appropriately, meaning that they should not assist governments in voluntary, widespread surveillance of users. Instead, these third parties should ensure that they only disclose personal data about users in compliance with applicable law or in response to valid legal orders.

Stands Up to NSL Gag Orders

EFF has challenged both NSLs and the gag orders that accompany them in court. In 2013 we won a landmark decision in the Northern District of California in which a federal judge declared one of the statutes underlying NSLs unconstitutional.

EFF has championed legislative reform in Congress to rein in NSLs. In 2015, substantive reforms to NSLs were included in a package of surveillance reforms known as the USA FREEDOM Act. Providers who receive NSLs are now allowed to request that the FBI initiate judicial review of NSL gag orders, which places a prior restraint on the company without judicial involvement. However, this check on overbroad NSL gag orders is only useful to the extent that companies choose to invoke it.

Tech companies should not be gagged from discussing government surveillance requests without a judge ever getting involved. Although the NSL statute remains unconstitutional in this regard, it still grants NSL recipients the right to request judicial review of every NSL gag order (a process known as "reciprocal notice"). Within the existing law, this is the right standard for technology companies.

This is the first year our *Who Has Your Back* report has encouraged companies to adopt a public policy of always requesting judicial review of NSL gag orders. Of the companies we examined, only twelve companies out of twenty-six met our standard.

Wordpress offered especially strong language, which includes a promise to publish a redacted version of the NSLs it receives:

> It is our policy to invoke the "reciprocal notice" procedure in 18 U.S.C. § 3511 for any national security letters (NSLs) served on Automattic. This process ensures that a court will review all non-disclosure orders issued with NSLs we may receive. If and when a non disclosure order is lifted, our policy is to share the contents of the NSL with any affected users (where possible), as well as to publish a redacted version of the NSL.

Apple also has a strong policy related to reciprocal notice:

> In addition, if Apple receives a National Security Letter (NSL) from the U.S. government that contains an indefinite gag order, Apple will notify the government that it would like the court to review the nondisclosure provision of the NSL pursuant to USA FREEDOM. The government then has 30 days to let the court know why the nondisclosure should remain in effect or can let Apple know that the nondisclosure no longer applies. If Apple receives notice that the nondisclosure no longer applies, it will notify the affected customer(s) pursuant to Apple's customer notice policies.

Pro-User Public Policy: Reform 702

Every year, we dedicate one category to a public policy position of a company. In prior years, we have acknowledged positions such as working to update and reform the Electronic Communications Privacy Act, opposing government backdoors in cryptography, and opposing mass surveillance.

As Congress considers this year whether to reauthorize Section 702, we are rating technology companies on whether they stand against Internet surveillance that impacts millions of innocent Internet users, both in the United States and abroad.

For the better part of a decade, EFF has been fighting unconstitutional Internet surveillance by the NSA in the courts. We encourage Congress to let this overbroad and much-criticized surveillance authority expire entirely at the end of this year. We also recognize that many believe that the reauthorization process is a key legislative moment to enact larger reforms against NSA surveillance. As our legislators examine these authorities, it is important that they remember that these programs are fundamentally flawed because they collect data on hundreds of millions of law-abiding technology users. It is impossible to bring these surveillance programs in alignment with the constitution without addressing this overbroad data collection.

We are thus awarding credit to those companies who are helping shape the public debate around NSA surveillance by urging Congress to reduce the collection of data on innocent people. We offered credit for companies that supported reforms to limit data collection under 702 as well as for companies who supported letting the law expire entirely.

The technology community was largely united in its call to Congress. Twenty-one of the twenty-six companies we evaluated received credit in this category. Most of these companies signed a letter to the Judiciary Committee Chairman that supported a range of substantive reforms to Section 702, including reforms to rein in data collection as well as additional oversight and transparency.

It should come as no surprise that technology companies want to see real limitations on NSA data collection. Their users can hardly be expected to continue to entrust their most sensitive information to the tech industry when they fear wholesale copies of that information could end up in NSA databases. NSA surveillance programs have also endangered tech efforts to expand into overseas markets, with European regulators questioning U.S. surveillance policies and hesitating over American companies entering European markets with U.S. privacy policies.

Raising the Floor

As we look back on seven years of reporting on the privacy policies and law enforcement guidelines of major technology companies, *Who Has Your Back* offers users a lot of hope. Public scrutiny has helped raise the floor on technology companies, so that every company we evaluated in 2017 has adopted at least some of the practices that were considered envelope-pushing in 2011. Innovation is not just for technology products, but also for the privacy and transparency practices of Silicon Valley.

There's still significant work to be done to defend user privacy and shed light on government attempts to surveil our digital lives. We offer this report as a tool for helping us get there.

Company Reports

Adobe

Adobe earns five stars in this year's report. This is Adobe's third year in *Who Has Your Back*, and it has adopted all of the industry best practices we recognize in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Adobe promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Adobe also forbids third parties from allowing Adobe user data to be used for surveillance purposes. We applaud Adobe's policies related to transparency and user privacy.

Follows industry-wide best practices. Adobe publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its transparency report:

> **No Customer Content Disclosed Without A Search Warrant:** Adobe does not disclose customer content stored in our cloud services (such as photos, videos or documents) unless we receive a search warrant issued upon a showing of probable cause under relevant state or federal law. We received search warrants in all 29 matters where we disclosed customer content.

And 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.

Tells users about government data requests. Adobe promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> 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 (DNO) 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. Please make sure any DNO you serve on Adobe is time-limited and expires on a specific date or after a specific period (such as 90 or 180 days).

And in its transparency report:

> **No Delaying Customer Notice Unless We Are Legally Obligated To Do So:** As we did last year, this year we rejected a number of requests from governments to delay notice to our users because the requests were made informally. We only delay notice to our customers where we are legally obligated to do so -- for example, when we receive a delayed notice order (DNO) issued by a court. We then notify our customer of the government request for their data after the DNO expires.

Promises not to sell out users. Adobe prohibits third parties from allowing Adobe user data to be used for surveillance purposes. From its law enforcement guidelines:

> Valid legal process is required before disclosure.

Adobe's privacy policy states:

> Adobe works with companies that help us run our business. These companies provide services such as delivering customer support, processing credit card payments, and sending emails on our behalf. In some cases, these companies have access to some of your personal information in order to provide services to you on our behalf. They are not permitted to use your information for their own purposes.

Adobe's requirement for legal process before disclosing user data plus its prohibition against third parties using information for their own purposes is the basis for our reading that Adobe's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Adobe requests review by a judge. From its law enforcement guidelines:

> Indefinite DNOs are not constitutionally valid and we challenge them in court.

Pro-user public policy: Reform 702. Adobe has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Adobe was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Airbnb

Airbnb earns three stars in this year's report. This is Airbnb's second year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Airbnb has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. However, there is room for improvement. We urge Airbnb to commit to providing prior notice to users about government data requests, and only delaying notice for limited reasons. We also urge Airbnb continue to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing Airbnb user data to be used for surveillance purposes.

Follows industry-wide best practices. Airbnb publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> 1. For content of communications, a search warrant issued under the procedures described in the US Federal Rules of Criminal Procedure (or equivalent state warrant procedures) is required.

Tells users about government data requests. Airbnb promises to provide advance notice to users about government data demands, but does not make clear whether it will inform users of government requests after a gag has been lifted or an emergency resolved. In addition, its exceptions for delaying notification are broader than physical bodily harm. It states in its law enforcement guidelines:

> Please note that Airbnb, Inc. has a policy of using commercially reasonable efforts to notify users in the United States when we receive legal process from a third party requesting user data. Generally, except where a court order (and not just the request for information itself) requires delayed notification or no notification, or except where notification is otherwise prohibited by law or where we, in our sole discretion, believe that providing notice would be futile, ineffective or would create a risk of injury or bodily harm to an individual or

> group, or to our property, we will endeavor to provide reasonable prior notice to the relevant user of the request for user data in the event the user wishes to seek appropriate protective relief.

Promises not to sell out users. Airbnb does not explicitly state that it prohibits third-party access to its user data, nor does it say that third parties are prohibited from allowing Airbnb user data to be used for surveillance purposes. As a result, our reading of Airbnb's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Airbnb requests review by a judge. From its law enforcement guidelines:

> Consistent with its policy of providing users notice of government-issued legal process for user data, Airbnb will request that the government initiate judicial review of any non-disclosure order issued in connection with a national security letter and has done so for any such letter it has received (if any).

Pro-user public policy: Reform 702. Airbnb has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Aibnb was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Amazon

Amazon earns two stars in this year's report. This is Amazon's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Amazon also supports substantive reforms to rein in NSA surveillance. However, there is room for improvement. We urge Amazon to promise to inform users before disclosing their data to the government and to create a public policy for requesting judicial review of all National Security Letters. We urge Amazon to continue to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing Amazon user data to be used for surveillance purposes.

Follows industry-wide best practices. Amazon publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course. Amazon distinguishes between content and non-content information. We produce noncontent information only in response to valid and binding subpoenas. We do not produce content information in response to subpoenas. We may produce non-content and content information in response to valid and binding search warrants.

Tells users about government data requests. Amazon promises to provide advance notice to users about government data demands, but does not make clear that it will provide notice after a gag order expires or an emergency is over, stating in its law enforcement guidelines:

> Unless it is prohibited from doing so or has clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.

Promises not to sell out users. Amazon does not explicitly state that it prohibits third-party access to its user data, nor does it say that third parties are prohibited from allowing Amazon user data to be used for surveillance purposes. Its privacy notice states:

> **Protection of Amazon.com and Others:** We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

As a result, our reading of Amazon's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Amazon does not have a public policy of requesting judicial review of all National Security Letters it receives. From its transparency report:

> National security requests include National Security Letters ("NSLs") and court orders issued under the Foreign Intelligence Surveillance Act ("FISA"). Our responses to these requests depend on the nature of the request. Amazon objects to overbroad or otherwise inappropriate national security requests as a matter of course.

Pro-user public policy: Reform 702. Amazon has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Amazon was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Apple

Apple earns four stars in this year's report. This is Apple's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Apple promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and explicitly states that third parties are forbidden from allowing Apple user data to be used for surveillance purposes. We urge Apple to support substantive reforms to rein in NSA surveillance.

Follows industry-wide best practices. Apple publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating on its government information requests page:

> We apply the highest U.S. legal standard, and we require a search warrant for all U.S. requests for content.

From its law enforcement guidelines:

> For all requests from government and law enforcement agencies within the United States for content, with the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), Apple will only provide content in response to a search warrant issued upon a showing of probable cause.

From its most recent transparency report:

> Any government agency seeking customer content from Apple must obtain a search warrant issued upon a showing of probable cause.

Tells users about government data requests. Apple promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> Q: Do you notify users of legal process?

> A: Yes, Apple's notice policy applies to account requests from law enforcement, government and private parties. Apple will notify customers and account holders unless there is a non-disclosure order or applicable law prohibiting notice, or where Apple, in its sole discretion, reasonably believes that such notice may pose immediate risk of serious injury or death to a member of the public, the case relates to a child endangerment matter, or where notice is not applicable to the underlying facts of the case.

It also states in its law enforcement guidelines:

> Apple will notify customers/users when their Apple account information is being sought in response to legal process from government, law enforcement, or third parties, except where providing notice is explicitly prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), by applicable law or where Apple, in its sole discretion, believes that providing notice creates a risk of injury or death to an identifiable individual, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.
>
> After 90 days Apple will provide delayed notice for emergency disclosure requests except where notice is prohibited by court order or 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 or in situations where the case relates to child endangerment. Apple will provide delayed notice for requests after expiration of the non-disclosure period specified in a court order unless Apple, in its sole discretion, reasonably 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.

Promises not to sell out users. Apple prohibits third parties from allowing Apple user data to be used for surveillance purposes. In its government information requests page, Apple states:

> We contractually require our service providers to follow the same standard we apply to government information requests for Apple data.

In its law enforcement guidelines, Apple states:

> Apple is committed to maintaining the privacy of the users of Apple products and services ("Apple users"). Accordingly, information about Apple users will not be released without valid legal process.

Notably, Apple has language in its privacy policy that is not as strong:

> It may be necessary – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence – for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.

Nonetheless, based on the clear and prominent placement of the legal process requirement in the law enforcement guidelines, and the clear and prominent commitment to ensure Apple service providers adhere to Apple's government information requests policy when providing data to the government, our reading of Apple's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Apples requests review by a judge. From its government information requests page:

> In addition, if Apple receives a National Security Letter (NSL) from the U.S. government that contains an indefinite gag order, Apple will notify the government that it would like the court to review the nondisclosure provision of the NSL pursuant to USA FREEDOM. The government then has 30 days to let the court know why the nondisclosure should remain in effect or can let Apple know that the nondisclosure no longer applies. If Apple receives notice that the nondisclosure no longer applies, it will notify the affected customer(s) pursuant to Apple's customer notice policies.

Pro-user public policy: Reform 702. Apple has not publicly called for reforms to Section 702 to curtail the surveillance of innocent people.

AT&T

AT&T earns one star in this year's report. This is AT&T's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. However, there is room for improvement. We urge AT&T to promise to inform users before disclosing their data to the government, create a public policy of requesting judicial review of all National Security Letters, and support substantive reforms to rein in NSA surveillance. We urge AT&T to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing AT&T user data to be used for surveillance purposes.

Follows industry-wide best practices. AT&T publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its most recent transparency report:

> Except in emergency circumstances, a search warrant or probable cause court order is required for all real-time precise location information (like GPS) and realtime content (such as content obtained through wiretaps). Stored content (like stored text and voice messages) generally also requires a warrant.

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

Promises not to sell out users. AT&T does not explicitly prohibit third-party access to its user data, nor does it say that third parties are prohibited from allowing AT&T user data to be used for surveillance purposes.

From its privacy policy:

> **2. Do you share my Personal Information internally?**
> Yes. Our products and services are developed, managed, marketed and sold by a variety of our affiliated companies. We may share Personal Information

internally, including with affiliated companies that may have different privacy policies. When we do this we require the affiliated company or companies to protect the Personal Information in a way consistent with this Privacy Policy. We may also combine Personal Information with data derived from an application that has a different privacy policy. When we do that, this Privacy Policy applies to the combined data set.…

Are there any other times when you might provide my Personal Information to other non-AT&T companies or entities?
Yes. We share your Personal Information with other, non-AT&T companies that perform services for us, like processing your bill. Because we take our responsibility to safeguard your Personal Information seriously, we do not allow those companies to use it for any purpose other than to perform those services, and we require them to protect it in a way consistent with this Privacy Policy. Companies that perform these services may be located outside the United States or the jurisdiction where you reside. If your Personal Information is shared with these companies, it could be accessible to government authorities according to the laws that govern those jurisdictions. There are also occasions when we provide Personal Information to other non-AT&T companies or other entities, such as government agencies, credit bureaus and collection agencies, without your consent. Some examples include sharing to:

- Comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements, and to enforce our legal rights or defend against legal claims;
- Obtain payment or make refunds for products and services that appear on your AT&T billing statements, including the transfer or sale of delinquent accounts or refund obligations to third parties for collection or payment.
- Enforce our agreements and protect our rights or property;
- Assist with identity verification and e-mail address validation;
- Respond to lawful requests by public authorities, including to meet national security or law enforcement requirements;
- Notify, respond or provide information (including location information) to a responsible governmental entity in emergency or exigent circumstances or in situations involving immediate danger of death or serious physical injury; and
- Notify the National Center for Missing and Exploited Children of information concerning child pornography of which we become aware through the provision of our services.

AT&T makes a clear statement that third parties with whom it shares users' personal information are required to adhere to the standards of AT&T's privacy policy. AT&T also outlines in its policies how it responds to various types of government data demands,

and makes clear it rejects other data requests from the government. However, AT&T includes a carve-out in its privacy policy to "assist with identity verification and e-mail address validation" as well as "respond to lawful requests by public authorities, including to meet national security or law enforcement requirements." As a result, our reading of AT&T's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. AT&T does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. AT&T has not publicly called for reforms to Section 702 to curtail the surveillance of innocent people.

Comcast

Comcast earns one star in this year's report. This is Comcast's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. However, there is room for improvement. We urge Comcast to promise to inform users before disclosing their data to the government, create a public policy of requesting judicial review of all National Security Letters, and support substantive reforms to rein in NSA surveillance. We urge Comcast to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing Comcast user data to be used for surveillance purposes.

Follows industry-wide best practices. Comcast publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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.

Tells users about government data requests. Comcast does not promise to provide advance notice to users about government data demands. Its published policy reads:

> The contents of email communications in storage will only be produced in response to a state or federal warrant. In such situations where the communications have been in storage for 180 days or less, this may be done by without notice by law enforcement to the subscriber by law enforcement. For email communications in storage for over 180 days, notice to the subscriber by law enforcement is required.

Promises not to sell out users. Comcast does not explicitly prohibit third-party access to its user data, nor does it say that third parties are prohibited from allowing Comcast user data to be used for surveillance purposes. As a result, our reading of Comcast's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Comcast does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Comcast has not publicly called for reforms to Section 702 to curtail the surveillance of innocent people.

CREDO Mobile

CREDO earns five stars in this year's report. This is CREDO's third year in *Who Has Your Back*, and it has adopted all of the industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. CREDO promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. CREDO also explicitly forbids third parties from allowing CREDO user data to be used for surveillance purposes. We applaud CREDO's policies related to transparency and user privacy.

Follows industry-wide best practices. CREDO publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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.

Tells users about government data requests. CREDO promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> **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.

It also clarifies in a footnote of its transparency report how it understands emergency requests:

> CREDO evaluates emergency requests to ensure they satisfy the requirements of 18 USC § 2702(c)(4) and/or (b)(8).

Promises not to sell out users. CREDO explicitly prohibits third parties from allowing CREDO user data to be used for surveillance purposes. It states in its transparency report:

> CREDO requires law enforcement entities to obtain a U.S. subpoena, court order, or warrant in order to obtain CREDO customer information and does not voluntarily provide third parties special access to user data for the purpose of surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, CREDO requests review by a judge. From its transparency report:

> In the case of NSLs, CREDO is committed to using all available statutory procedures to ensure that each request to CREDO accompanied by an indefinite gag is reviewed by a judge. CREDO has fought for the right to disclose each NSL it has received in the past and will continue to do so.

Pro-user public policy: Reform 702. CREDO has said it would not support reauthorizing Section 702 as it is currently written, stating in a recent transparency report:

> We are working for full repeal of the USA PATRIOT Act and FISA Amendments Act.

And:

> CREDO opposed reauthorization of the PATRIOT Act's Section 215 before the USA Freedom Act was passed (a bill CREDO opposed) and opposes the reauthorization of FISA Section 702 as it is currently written.

Dropbox

Dropbox earns five stars in this year's report. This is Dropbox's sixth year in *Who Has Your Back*, and it has adopted all of industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Dropbox promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Dropbox also explicitly forbids third parties from allowing Dropbox user data to be used for surveillance purposes. We applaud Dropbox's policies related to transparency and user privacy.

Follows industry-wide best practices. Dropbox publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement handbook:

> Dropbox will only provide user content, whether in files or otherwise, in response to a search warrant.

Tells users about government data requests. Dropbox promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement handbook:

> Dropbox's policy is to provide notice to users about all 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. If you have a legal basis to delay Dropbox from notifying the user in a particular case, please provide legal justification (such as a court order) when serving the subpoena or warrant. Once the basis for the non-disclosure has expired, we will give notice to the user.

Promises not to sell out users. Dropbox prohibits third parties from allowing Dropbox user data to be used for surveillance purposes. From its government data request principles:

> We've seen reports that governments have been tapping into data center traffic of

> certain service providers. We've also seen reports that service providers have tools designed to give law enforcement access to user data directly or via third parties. Dropbox opposes these activities and would fight any attempt to require us to participate in them. Governments should always request user data by contacting online services directly and presenting legal process. This allows services like Dropbox to scrutinize the data requests and resist where appropriate.

As a result, our reading of Dropbox's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Dropbox requests review by a judge. From its government data request principles:

> We believe in providing notice to our users when a government requests their information and have fought in court to do so. However, government requests frequently include a court-granted non-disclosure order, which prohibits us from giving notice to the affected user. In cases where we receive a non-disclosure order, we notify the user when it has expired. Dropbox is also committed to following the USA FREEDOM Act. This ensures that courts have the opportunity to review non-disclosure obligations for any National Security Letters we may receive. We believe services like Dropbox should always be permitted to provide notice to affected users, and will continue advocating for this important goal.

Pro-user public policy: Reform 702. Dropbox has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Dropbox was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Facebook

Facebook earns four stars in this year's report. This is Facebook's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Facebook promises to inform users before disclosing their data to the government and supports substantive reforms to rein in NSA surveillance. Facebook also explicitly states that third parties are forbidden from allowing Facebook user data to be used for surveillance purposes. We urge Facebook to create a public policy of requesting judicial review of all National Security Letters.

Follows industry-wide best practices. Facebook publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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, timeline posts, and location information.

Tells users about government data requests. Facebook promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> 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 also 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.

Promises not to sell out users. Facebook prohibits third parties from allowing Facebook user data to be used for surveillance purposes. Its platform policy reads:

> Protect the information you receive from us against unauthorized access, use, or disclosure. For example, don't use data obtained from us to provide tools that are used for surveillance.

And its privacy policy reads:

> **Vendors, service providers and other partners.** We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.

As a result, our reading of Facebook's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Facebook does not have a public policy of requesting judicial review of all National Security Letters it receives.

However, Facebook does read the NSL statute very narrowly, stating:

> We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

While Facebook does not qualify for a star in this section, we applaud its reading of the statute, especially the fact that it does not turn over IP address information in response to an NSL.

Pro-user public policy: Reform 702. Facebook has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Facebook was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform

would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens...

Google

Google earns four stars in this year's report. This is Google's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Google promises to inform users before disclosing their data to the government and supports substantive reforms to rein in NSA surveillance. Google prohibits third parties from allowing Google user data to be used for surveillance purposes. We urge Google to create a public policy of requesting judicial review of all National Security Letters.

Follows industry-wide best practices. Google publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its legal process page:

> 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.

Tells users about government data requests. Google promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires. The following language is not yet live on Google's site as of the date of publication, but will be posted in July 2017 on its legal process page:

> If you receive a legal request concerning my account, will you tell me about it?
>
> 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 unless such notification is prohibited by law. We will provide delayed notice to users after a legal prohibition is lifted, such as when a statutory or court ordered gag period has expired. We might not give notice when, in our sole discretion, we believe that notice would be counterproductive or exceptional circumstances exist involving danger of death or serious physical injury to any person. In such cases, we will provide delayed notice if we later determine that those circumstances no longer exist. In cases where the account in question is an enterprise hosted account, notice may go to the domain administrator, or the end user, or both.

> 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. If the request appears to be legally valid, we will endeavor to make a copy of the requested information before we notify the user.

Promises not to sell out users. Google prohibits third parties from allowing Google user data to be used for surveillance purposes.

From its FAQ on law enforcement access:

> **Does Google give governments direct access to user data?**
> We require that requests for user data be sent to Google directly and not through any sort of "back door" direct access by the government. Our legal team reviews each and every request, and frequently pushes back when requests are overly broad or don't follow the correct process. We have taken the lead in being as transparent as possible about government requests for user information.

From its developer agreement:

> You are not permitted to access, aggregate, or analyze Google user data if the data will be displayed, sold, or otherwise distributed to a third party conducting surveillance.

As a result, our reading of Google 's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Google does not have a public policy of requesting judicial review of all National Security Letters it receives.

However, Google does read the NSL statute narrowly, stating:

> Under the Electronic Communications Privacy Act (ECPA) 18 U.S.C. section 2709, the FBI can seek 'the name, address, length of service, and local and long distance toll billing records' of a subscriber to a wire or electronic communications service. The FBI can't use NSLs to obtain anything else from Google, such as Gmail content, search queries, YouTube videos or user IP addresses.

While Google does not qualify for a star in this section, we applaud its reading of the statute, especially the fact that it does not turn over IP address information in response to an NSL.

Pro-user public policy: Reform 702. Google has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Google was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

LinkedIn

LinkedIn earns four stars in this year's report. This is LinkedIn's fifth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. LinkedIn promises to inform users before disclosing their data to the government and supports substantive reforms to rein in NSA surveillance. LinkedIn also explicitly states that third parties are forbidden from allowing LinkedIn user data to be used for surveillance purposes. We urge LinkedIn to create a public policy of requesting judicial review of all National Security Letters.

Follows industry-wide best practices. LinkedIn publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> We require a search warrant to produce any Member Content responsive to law enforcement Data Requests.

Tells users about government data requests. LinkedIn promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> 7. Will LinkedIn notify Members of Requests for account data?
> Yes. 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. Please note that nondisclosure orders should be as narrow in scope and duration as circumstances permit, and that LinkedIn does not provide advance notice to the Requesting party that a nondisclosure order is expiring; it is up to the Requesting party to calendar the nondisclosure period and to keep LinkedIn apprised of any modifications or extensions.

Promises not to sell out users. LinkedIn explicitly prohibits third parties from allowing LinkedIn user data to be used for surveillance purposes. From its transparency report:

> We know that our members' concerns over surveillance extend to the private sector as well. When it comes to data about LinkedIn members, we set limits on data use to ensure that our customers and participants in our API programs share our goals and put our members first. Such limits prohibit using or sharing LinkedIn information for surveillance purposes.

As a result, our reading of LinkedIn's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. LinkedIn does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. LinkedIn has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. LinkedIn was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Lyft

Lyft earns five stars in this year's report. This is Lyft's second year in *Who Has Your Back*, and it has adopted all of the industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Lyft promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Lyft also explicitly forbids third parties from allowing Lyft user data to be used for surveillance purposes. We applaud Lyft's policies related to transparency and user privacy.

Follows industry-wide best practices. Lyft publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> We will require a warrant for requests for content of communications between Users or for prospective location data.

Tells users about government data requests. Lyft promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> It is our policy to provide notice to Users before producing their information in response to a criminal investigation by law enforcement unless (i) we are prohibited by law from doing so, (ii) we have reason to believe the subject's Lyft account has been compromised such that the notice would go to the wrong person, or notice would otherwise be counterproductive or would create a risk to safety, or (iii) it is an emergency request and prior notice would be impractical (in which case we may provide notice after the fact). Law enforcement officials who do not want their request disclosed should provide an appropriate court order or process establishing that notice is prohibited, or provide sufficient detail for Lyft to determine whether a request falls into one of the exceptions above. Regulatory or other non-criminal requests for information are not within the scope of this policy.

> **In the event that information is provided subject to a gag order or disclosed pursuant to an emergency request, Lyft will provide notice to its users of these government demands if Lyft is thereafter notified that the gag order or the emergency has expired.**

And it also states in its law enforcement guidelines:

> We have a process for evaluating requests on an emergency basis where an emergency situation exists involving an immediate threat of death or serious bodily harm to a person. Requestors must email LER@lyft.com with the subject line 'Emergency Disclosure Request' and describe in detail the nature of the emergency. We review these requests on a case-by-case basis. Please note that we will only review and respond to emergency requests from law enforcement, and will not respond to emergency requests sent to this address by non-law enforcement officials. Non-law enforcement officials aware of an emergency situation should immediately and directly contact local law enforcement officials

Promises not to sell out users. Lyft prohibits third parties from allowing Lyft user data to be used for surveillance purposes. In its developer agreement, it states:

> You will not… use the Platform or Service to investigate, track or surveil Lyft Users, or to obtain information on Lyft Users, information on Lyft Users, in a manner that would require valid legal process.

As a result, our reading of Lyft's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Lyft requests review by a judge. From its law enforcement guidelines:

> Lyft will challenge any National Security Letter it receives, and will require the government to obtain an order from a court requiring its compliance.

Pro-user public policy: Reform 702. Lyft has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Lyft was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the

imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens...

Microsoft

Microsoft earns four stars in this year's report. This is Microsoft's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Microsoft promises to inform users before disclosing their data to the government and supports substantive reforms to rein in NSA surveillance. Microsoft also explicitly states that third parties are forbidden from allowing Microsoft user data to be used for surveillance purposes. We urge Microsoft to create a public policy of requesting judicial review of all National Security Letters.

Follows industry-wide best practices. Microsoft publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement requests report:

> 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.

Tells users about government data requests. Microsoft promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires. The following language is not yet live on Microsoft's site as of the date of publication, but will be posted in July 2017 on its legal process page:

> **Does Microsoft notify users of its consumer services, such as Outlook.com, when law enforcement or another governmental entity in the U.S. requests their data?** Yes. 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 when we determine that the circumstances that caused us to withhold

notice at the time the request was made has expired (e.g., a valid court order prohibiting customer notification expires).

Promises not to sell out users. Microsoft prohibits third parties from allowing Microsoft user data to be used for surveillance purposes. Its law enforcement requests report states:

> **Q: Do you enable third parties to assist governments in conducting voluntary surveillance of your customers?**
> **A:** We are aware of reports that some providers have develop tools that third parties use to voluntarily assist governments in conducting surveillance of that provider's users. We do not design tools to enable voluntary surveillance of our users. If we ever provide third parties with access to data about our customers, we expect those third parties to handle that data appropriately, meaning that they should not assist governments in voluntary, widespread surveillance of users. Instead, these third parties should ensure that they only disclose personal data about users in compliance with applicable law or in response to valid legal orders.

As a result, our reading of Microsoft's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Microsoft does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Microsoft has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Microsoft was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Pinterest

Pinterest earns five stars in this year's report. This is Pinterest's third year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Pinterest promises to inform users before disclosing their data to the government and supports substantive reforms to rein in NSA surveillance. Pinterest also prohibits third parties from allowing Pinterest user data to be used for surveillance purposes and has instituted a public policy of requesting judicial review of all National Security Letters it receives. We applaud Pinterest's policies related to transparency and user privacy.

Follows industry-wide best practices. Pinterest publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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.

Tells users about government data demands. Pinterest promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> 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:
>
> - we are legally prohibited from providing notice (e.g. by an order under 18 U.S.C. § 2705(b));
> - an emergency situation exists involving a danger of death or serious physical injury to a person;
> - 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.

Promises not to sell out users. Pinterest prohibits third parties from allowing Pinterest user data to be used for surveillance purposes.

From its developer guidelines:

> You're responsible for following all laws, regulations and industry codes, as well as our terms and policies, including our community guidelines and privacy policy.

And:

> Our developer API should only be used for direct-to-consumer integrations that help people discover and do what they love.

From its law enforcement guides:

> **What does Pinterest require to produce user information?**
> **For U.S. Law Enforcement**
>
> You must obtain a valid subpoena, court order or search warrant ("Law Enforcement Request") to compel Pinterest to provide any user's information. To compel Pinterest to provide any user's content, you must obtain a valid search warrant.

As a result, our reading of Pinterest's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Pinterest requests review by a judge. From its law enforcement guidelines:

> If we receive a National Security Letter (NSL) from the U.S. government that includes an indefinite non-disclosure order, our policy is to ask the government to seek judicial review of the order pursuant to the USA FREEDOM Act.

Pro-user public policy: Reform 702. Pinterest has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Pinterest was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the

imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens...

Slack

Slack earns four stars in this year's report. This is Slack's second year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Slack has a published policy of requesting judicial review of all National Security Letters and supports substantive reforms to rein in NSA surveillance. Slack also prohibits third parties from allowing Slack user data to be used for surveillance purposes. We call on Slack to inform users before disclosing their data to the government.

Industry-wide best practices. Slack publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> Slack requires a search warrant issued by a court of competent jurisdiction (a federal court or a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants) to disclose Customer Data.

Tells users about government data demands. Slack promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, but it allows for a broad set of exceptions to this policy, stating in its law enforcement guidelines:

> Slack will notify Customer before disclosing any of Customer's Customer Data so that the Customer may seek protection from such disclosure, unless Slack is prohibited from doing so or there is a clear indication of illegal conduct or risk of harm to people or property associated with the use of such Customer Data. If Slack is legally prohibited from notifying Customer prior to disclosure, Slack will take reasonable steps to notify Customer of the demand after the nondisclosure requirement expires.

Hence, Slack does not earn credit in this category.

Promises not to sell out users. Slack prohibits third parties from allowing Slack user data to be used for surveillance purposes. From its law enforcement guidelines:

> Slack is committed to the importance of trust and transparency for the benefit of our Customers and does not voluntarily provide governments with access to any data about users for surveillance purposes.

In addition, its data request policy states:

> **Requests for Customer Data by Individuals**
> Third parties seeking access to Customer Data should contact the Customer regarding such requests. The Customer controls the Customer Data and generally gets to decide what to do with all Customer Data.

Its terms of service state:

> **Compelled Access or Disclosure**
> The Receiving Party may access or disclose Confidential Information of the Disclosing Party if it is required by law; provided, however, that the Receiving Party gives the Disclosing Party prior notice of the compelled access or disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the access or disclosure.

As a result, our reading of Slack's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Slack requests review by a judge. From its law enforcement guidelines:

> In addition, if Slack receives a National Security Letter with an indefinite non-disclosure requirement, Slack will initiate procedures for judicial review pursuant to 18 U.S.C. § 3511.

Pro-user public policy: Reform 702. Slack has publicly called for reforms to Section 702 to curtail the surveillance of innocent people, stating in its transparency report:

> We support codifying reforms to Section 702 of the Foreign Intelligence Surveillance Act expiring this year in order to reduce the overly broad collection of information.

Snap Inc.

Snap Inc.

Snap Inc. (previously known as Snapchat) earns three stars in this year's report. This is Snap's third year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Snap also supports substantive reforms to rein in NSA surveillance and has a public policy forbidding third parties from allowing Snap user data to be used for surveillance purposes. However, there is room for improvement. While Snap promises to inform users before disclosing their data to the government, it does not publicly promise to provide delayed notice when prior notice was impossible due to emergency or a gag order. Snap also does not have a published policy of requesting judicial review of all National Security Letters.

Follows industry-wide best practices. Snap publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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.

Tells users about government data demands. Snap promises to provide advance notice to users about government data demands, but does not commit to providing delayed notice after a gag order expires, stating in its law enforcement guidelines:

> It is our policy to notify Snapchat users when we receive legal process seeking their records, information, or content. We recognize two exceptions to this policy. First, we will not notify users of legal process where providing notice is prohibited by a court order issued under 18 U.S.C. § 2705(b) or by other legal authority. Second, where we, in our sole discretion, believe an exceptional circumstance exists, such as cases involving child exploitation or the threat of imminent death or bodily injury, we reserve the right to forgo user notice.

Promises not to sell out users. Snap prohibits third parties from allowing Snap user data to be used for surveillance purposes. From its transparency report:

> And to be perfectly clear: We do not voluntarily provide any government with access to user data for surveillance purposes, whether directly or through third parties.

As a result, our reading of Snap's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Snap does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Snap has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Snap was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Sonic

Sonic earns five stars in this year's report. This is Sonic's fifth year in *Who Has Your Back*, and it has adopted all of the industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Sonic promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Sonic also explicitly forbids third parties from allowing Sonic user data to be used for surveillance purposes. We applaud Sonic's policies related to transparency and user privacy.

Follows industry-wide best practices. Sonic publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> Sonic will not provide user content without a U.S. search warrant.

Tells users about government data demands. Sonic promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> Sonic 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.

Promises not to sell out users. Sonic explicitly states that it does not sell data to third parties and that it does not voluntarily provide user data to the government for surveillance purposes. According to its blog post "Privacy Matters":

> Sonic never sells our member information or usage data, nor do we voluntarily provide government or law enforcement with access to any data about users for surveillance purposes.

As a result, our reading of Sonic's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Sonic requests review by a judge. From its law enforcement guidelines:

> If and when Sonic receives any indefinite sealed legal process precluding notifying a Sonic customer, including a national security letter gag, Sonic will and does invoke statutory procedures to have a judge review.

Pro-user public policy: Reform 702. Sonic opposes the reauthorization of Section 702. In its blog post "Privacy Matters" it states:

> Sonic is also against the re-authorization of Section 702 (the law behind the PRISM and Upstream programs). Governments and other entities should not collect huge quantities of phone, email or other internet usage data directly from the physical infrastructure of any communications provider.

T-Mobile

T-Mobile earns one star in this year's report. This is T-Mobile's first year in *Who Has Your Back*. While it has adopted some industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests, there is much room for improvement. T-Mobile does not promise to inform users before disclosing their data to the government, nor does it have a published policy of requesting judicial review of all National Security Letters it receives. We urge T-Mobile to support substantive reforms to rein in NSA surveillance. We also urge it to continue to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing T-Mobile user data to be used for surveillance purposes.

Follows industry-wide best practices. T-Mobile publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, publishing the following chart in its most recent transparency report:

Types of Information Requested	Minimum Required Legal Process	Legal Standard (Generally)
Subscriber Information (e.g., information a customer provides when signing up for service, such as name and address)	Subpoena	Based on determination that the information sought is relevant to a criminal investigation
Historical Call Detail Information (e.g., noncontent information about calls or text messages made in the past, such as start time, duration, numbers called)	Subpoena	Based on determination that the information sought is relevant to a criminal investigation
Emergency Information (e.g., location information, call detail, content, in emergencies)	Certification from Law Enforcement/Public Safety Answering Points	Good faith belief by the carrier of an emergency

Real Time (prospective) Call Detail Information, Non-content (Pen register/trap and trace) (e.g., information on incoming and outgoing phone numbers for a specific phone/mobile device, time transmitted, duration of the call)	Pen Register Court Order	Relevant and material to an ongoing investigation
Historical Cell Site Location Information (e.g., location of towers that a phone/mobile device used in the past over a specific period of time)	Court Order or Warrant*	Relevant and material to an ongoing criminal investigation
Real Time (prospective) Audio content (e.g., phone conversation)	Wiretap Court Order	Probable cause, reasonable grounds to suspect that a crime has been committed. Only for certain serious crimes
Real Time (prospective) Content (e.g., text messages)	Wiretap Court Order	Probable cause, reasonable grounds to suspect that a crime has been committed. Only for certain serious crimes
Real Time Location (e.g., approximate location of a phone/mobile device)	Search Warrant	Probable cause, reasonable grounds to suspect that a crime has been committed
Historical Cell Tower Dump Information (e.g., list of phone numbers which used a specific tower during a specific period of time)	Search Warrant	Probable cause, reasonable grounds to suspect that a crime has been committed
Stored Content (e.g., saved voicemail message)	Search Warrant	Probable cause, reasonable grounds to suspect that a crime has been committed

**Depends on the applicable jurisdiction.*

Tells users about government data demands. T-Mobile does not promise to provide advance notice to users about government data demands.

Promises not to sell out users. T-Mobile does not explicitly state that it prohibits third-party access to its user data, nor does it say that third parties are prohibited from allowing T-Mobile user data to be used for surveillance purposes. Its privacy policy includes:

> **When We Share Information Collected About You**
>
> - We do not sell your name, address or phone number to others outside the T-Mobile corporate family to market those companies' products or services.
> - **Transactions.** We may provide your information to third-party service providers to process transactions or otherwise provide you service, such as billing companies or shipping services, or when roaming on another carrier's network…
> - **For Legal Process and Protection.** We will provide customer information where necessary to comply with the law, such as disclosure of your information to a law enforcement agency for your safety or the safety of others, or when compelled by subpoena or other legal process.
> - **De-Identified Data.** We may provide your de-identified information to third parties for marketing, advertising, or other purposes.

As a result, our reading of T-Mobile's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. T-Mobile does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. T-Mobile has not publicly called for reforms to Section 702 to curtail the surveillance of innocent people.

Tumblr

Tumblr earns three stars in this year's report. This is Tumblr's fourth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Tumblr promises to inform users before disclosing their data to the government, and supports substantive reforms to rein in NSA surveillance. However, there is room for improvement. Tumblr does not have a published policy of requesting judicial review of all National Security Letters it receives. In addition, we urge Tumblr to continue to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing Tumblr user data to be used for surveillance purposes.

Follows industry-wide best practices. Tumblr publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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.

Tells users about government data demands. Tumblr promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> 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.

Promises not to sell out users. Tumblr does not explicitly state that it prohibits third-party access to its user data, nor does it say that third parties are prohibited from allowing Tumblr data to be used for surveillance purposes. Its privacy policy reads, in part:

> That said, we also reserve the right to access, preserve, and disclose any information as we reasonably believe is necessary, in our sole discretion, to (i) satisfy any law, regulation, legal process, governmental request, or governmental order, (ii) enforce this Privacy Policy and our Terms of Service, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security, trust and safety, or technical issues (including exchanging information with other companies and organizations for the purposes of improving security and preventing fraud, spam, and malware), (iv) respond to user support requests, or (v) protect the rights, property, health or safety of us, our users, any third parties or the public in general, including but not limited to situations involving possible violence, suicide, or self-harm.

As a result, our reading of Tumblr's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Tumblr does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Through its parent company Yahoo, Tumblr has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Yahoo was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Twitter

Twitter earns three stars in this year's report. This is Twitter's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Twitter forbids third parties from using Twitter user data for surveillance purposes, and it supports substantive reforms to rein in NSA surveillance. However, there is room for improvement. We urge Twitter to create a public policy of requesting judicial review of all National Security Letters it receives, and improving its user notification process in the event of a government data disclosure request.

Follows industry-Wide Best Practices. Twitter publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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.

Tells users about government data demands. Twitter promises to provide advance notice to users about government data demands, but does not commit to providing delayed notice after an emergency is over or a gag order has expired. Instead, in its law enforcement guidelines, Twitter says 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 regarding imminent threat to life; child sexual exploitation; terrorism). We may also provide post-notice to affected users when prior notice is prohibited.

We urge Twitter to go further and promise to give all users notice of government attempts to access their data.

Promises not to sell out users. Twitter explicitly states that it prohibits third parties from allowing Twitter user data to be used for surveillance purposes. From its blog post about its developer policies:

> **To be clear:** We prohibit developers using the Public APIs and Gnip data products from allowing law enforcement — or any other entity — to use Twitter data for surveillance purposes. Period. The fact that our Public APIs and Gnip data products provide information that people choose to share publicly does not change our policies in this area. And if developers violate our policies, we will take appropriate action, which can include suspension and termination of access to Twitter's Public APIs and data products.

As a result, our reading of Twitter's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Twitter does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Twitter has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Twitter was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Uber

Uber earns five stars in this year's report. This is Uber's second year in *Who Has Your Back*, and it has adopted all of the industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Uber promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Uber also explicitly forbids third parties from allowing Uber user data to be used for surveillance purposes. We applaud Uber's policies related to transparency and user privacy.

Follows industry-wide best practices. Uber publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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 our disclosure of certain communications between people using Uber or GPS location information. Exceptions to these requirements may be available for emergency and exigent requests, where a user has provided consent, or - for requests that do not require a warrant - where other legal or regulatory standards apply.

Tells users about government data demands. Uber promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> Notice of Requests
> Uber's policy is to notify riders and driver-partners of law enforcement requests for their information before disclosure, whenever possible, with exceptions for emergencies, exigent requests, when we have a good faith belief that notice would be counterproductive or would create a risk to safety, or when we are prohibited from doing so by law (i.e., by statutory prohibition or court order). Law enforcement officials seeking non-disclosure of legal requests should provide relevant details concerning their investigation so that we may determine whether

> the request falls into one of these exceptions. In all other circumstances, law enforcement must obtain a non-disclosure order. If Uber receives a request for disclosure that is not governed by existing law or an accompanying non-disclosure order, we will give law enforcement the opportunity to seek court-ordered non-disclosure before we provide notice. Please be sure that the non-disclosure order states that notice is prohibited for a specified period of time. Upon receipt of an appropriate court order, we 7n. Where available, Uber will take advantage of the statutory provisions of 18 U.S.C. § 3511(b)(1)(A) to have non-disclosure requirements reviewed by a court.

And:

> Emergency and Exigent Requests
> We have a process for evaluating requests on an emergency or exigent basis where there is an emergency or exigency that involves protecting a rider, driver-partner, or third party who has been physically harmed or stopping illegal activity that poses an immediate threat of physical harm, or in cases of verifiable time-sensitive investigations. Requestors must submit an Emergency Request through the Law Enforcement Portal at https://lert.uber.com. We require a description of the nature of the emergency or urgency, including details about the nature of the alleged actual or threatened physical harm or exigency, and we review these requests on a case-by-case basis. We may provide responsive information when we have a good faith belief that doing so may protect riders, driver-partners, others, Uber, or otherwise assist with an exigent investigation. Once the emergency or exigency has passed, we require law enforcement to follow up with the appropriate legal process and we may require law enforcement to obtain appropriate legal process for any initial or additional disclosure. To facilitate our review, law enforcement should provide as much detail about the incident or emergency as possible.

Promises not to sell out users. Uber prohibits third parties from allowing Uber user data to be used for surveillance purposes.

In a recent Medium post, it stated:

> Editor's note (April 2017): Since our initial publication in April 2016, we've updated our Transparency Report with half-yearly data to make sure riders can know the extent of our regulatory data reporting and law enforcement requirements in the U.S., and more recently, Canada. Uber works with city, state, and provincial officials to make sure that data requests follow the recommendations outlined above. Uber maintains guidelines that define the process for law enforcement authorities to obtain information from Uber in accordance with our terms, policies, and applicable law, and any efforts to use

> regulatory reports, or publicly available Uber tools, for purposes of rider surveillance are inconsistent with these guidelines.

As a result, our reading of Uber's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSLs. When receiving a National Security Letter with an indefinite gag order, Uber requests review by a judge. From its law enforcement guidelines:

> Where available, Uber will take advantage of the statutory provisions of 18 U.S.C. § 3511(b)(1)(A) to have non-disclosure requirements reviewed by a court.

Pro-user public policy: Reform 702. Uber has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Uber was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Verizon

Verizon earns one star in this year's report. This is Verizon's sixth year in *Who Has Your Back*, and it has adopted some industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. However, there is much room for improvement. We urge Verizon to promise to inform users before disclosing their data to the government, create a public policy of requesting judicial review of all National Security Letters, and publicly support substantive reforms to rein in NSA surveillance. We also urge Verizon to continue to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing Verizon user data to be used for surveillance purposes.

Follows industry-wide best practices. Verizon publishes a combined transparency report with integrated law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its transparency report:

> We are compelled to provide contents of communications to law enforcement relatively infrequently. Under the law, law enforcement may seek communications or other content that a customer may store through our services, such as text messages or email. Verizon only releases such stored content to law enforcement with a probable cause warrant; we do not produce stored content in response to a general order or subpoena.

Tells users about government data demands. Verizon does not promise to notify users about government data demands.

Promises not to sell out users. Verizon does not prohibit third parties from allowing Verizon user data to be used for surveillance purposes.

Its privacy policy states:

> Verizon uses vendors and partners for a variety of business purposes such as to help us offer, provide, repair, restore and bill for services we provide. We share information with those vendors and partners when it is necessary for them to perform work on our behalf. For example, we may provide your credit card information and billing address to our payment processing company solely for the purpose of processing payment for a transaction you have requested. We require that these vendors and partners protect the customer information we provide to them and limit their use of Verizon customer data to the purposes for which it was provided. We do not permit these types of vendors and partners to use this information for their own marketing purposes.

And:

> We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as:
>
> - to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law; in cases involving danger of death or serious physical injury to any person or other emergencies;
> - to protect our rights or property, or the safety of our customers or employees;
> - to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of or subscription to our products and services and to protect our network, services, devices and users from such use…

While we appreciate the stronger language around vendors and partners, the exceptions Verizon has to this policy (including "to protect our rights" and "protect against… unauthorized or unlawful use of or subscription to our products and services") are overly broad and add uncertainty to the policy. As a result, our reading of Verizon's public-facing policies does not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Verizon does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Verizon has not publicly called for reforms to Section 702 to curtail the surveillance of innocent people.

WhatsApp

WhatsApp earns two stars in this year's report. This is Whatsapp's second year in *Who Has Your Back*, and it has adopted several industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. WhatsApp, through its parent company Facebook, also supports substantive reforms to rein in NSA surveillance. However, there is room for improvement. We urge WhatsApp to promise to inform users before disclosing their data to the government and create a public policy of requesting judicial review of all National Security Letters. We also urge WhatsApp to continue to clarify its policies related to third-party access of its user data, either by making explicit that there is no third-party access or by stating explicitly that third parties are forbidden from allowing WhatsApp user data to be used for surveillance purposes.

Follows industry-wide best practices. WhatsApp's parent company Facebook publishes a transparency report that includes data about government requests for WhatsApp data. WhatsApp publishes law enforcement guidelines. It requires a warrant before giving user 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 "about" information, profile photos, group information, and address book, if available. WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages, and undelivered messages are deleted from our servers after 30 days. WhatsApp offers end-to-end encryption for our services, which is on by default.

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

Promises not to sell out users. WhatsApp does not explicitly state that it prohibits third-party access to its user data, nor does it say that third parties are prohibited from allowing WhatsApp user data to be used for surveillance purposes. According to its privacy policy:

> When we share information with third-party providers, we require them to use your information in accordance with our instructions and terms or with express permission from you.

Notably, the sharing of data "in accordance with our instructions" is overly broad and vague. As a result, our reading of WhatsApp's public-facing policies would not prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. WhatsApp does not have a public policy of requesting judicial review of all National Security Letters it receives

Pro-user public policy: Reform 702. Through its parent company Facebook, WhatsApp has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Facebook was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Wickr

Wickr earns five stars in this year's report. This is Wickr's third year in *Who Has Your Back*, and it has adopted all of the industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Wickr promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Wickr also explicitly forbids third parties from allowing Wickr user data to be used for surveillance purposes. We applaud Wickr's policies related to transparency and user privacy.

Follows industry-Wide Best Practices. Wickr publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

> Requests for the contents of communications require a valid search warrant from an agency with proper jurisdiction over Wickr. However, our response to such a request will reflect that the content is not stored on our servers or that, in very limited instances where a message has not yet been retrieved by the recipient, the content is encrypted data which is indecipherable.

Tells users about government data demands. Wickr promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> **Will Wickr Notify Users of Requests for Account Information?**
> Wickr's policy is to notify users of requests for their account information prior to disclosure including providing user with a copy of the request, unless we are prohibited by law from doing so. As soon as legally permitted to do so, we will notify our users of requests for their information.

And according to its privacy policy:

> We will always notify our users of any third party requests for their information unless we are legally prohibited from doing so. As soon as legally permissible, we will notify our users of requests for their information. We require a warrant before handing over the contents of communications; however, because of the nature of our technology, the contents of communications will be encrypted and undecipherable if obtained.

Promises not to sell out users. Wickr prohibits third-party access to its user data, stating in its privacy policy:

> We do not share any user information we have with third parties, with the exception of the third-party service with whom we share your phone number for the sole purpose of sending you an SMS confirmation if you choose to associate your phone number with your Wickr ID. Please note that the provision of a phone number is completely at the user's discretion.

As a result, our reading of Wickr's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Wickr requests review by a judge. From a recent blog post on responding to government information requests:

> Should we receive an NSL gag order, we are committed to invoking the available statutory procedures to ensure judicial review of such order.

Pro-user public policy: Reform 702. Wickr has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. From a recent blog post outlining its stance on government surveillance:

> As it is critical to rebuild the trust between government and citizens, we support codifying reforms to Section 702 of the Foreign Intelligence Surveillance Act expiring this year in order to reduce the collection of information on innocent people.

Wordpress

Wordpress earns five stars in this year's report. This is Wordpress's fourth year in *Who Has Your Back*, and it has adopted all of the industry best practices we measure in this report, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Wordpress promises to inform users before disclosing their data to the government, has a published policy of requesting judicial review of all National Security Letters, and supports substantive reforms to rein in NSA surveillance. Wordpress also explicitly forbids third parties from allowing Wordpress user data to be used for surveillance purposes. We applaud Wordpress's policies related to transparency and user privacy.

Follows industry-Wide Best Practices. Wordpress publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user 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).

Tells users about government data demands. Wordpress promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> It is our policy to notify users and provide them with a copy of any civil or government legal process regarding their account or site (including formal requests for private information), unless we are prohibited by law or court order from doing so. In those cases, we will notify users and provide them with a copy of the legal process when the prohibition expires.
>
> If a request for information is valid, we will preserve the necessary information before informing the user. In most cases, upon notification to the user, that user will be provided with either 7 days or the amount of time before the information

> is due, whichever is later, during which time the user may attempt to quash or legally challenge the request. If, prior to the deadline, we receive notice from user that he or she intends to challenge a request, no information will be delivered until that process concludes. We also review the information requests received and may lodge our own challenge to the scope or validity of legal process received, on behalf of a user, whether or not the user pursues his/her own legal challenge.

Promises not to sell out users. Wordpress prohibits third parties from allowing Wordpress user data to be used for surveillance purposes. According to its law enforcement guidelines:

> We do not voluntarily provide governments with access to data about users (private or public) for law enforcement, intelligence gathering, or other surveillance purposes.

And its developer agreement requires that developers:

> [A]gree not to:...display, distribute, or otherwise make available content or data to governmental entities for intelligence gathering or surveillance purposes.

As a result, our reading of Wordpress's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. When receiving a National Security Letter with an indefinite gag order, Wordpress requests review by a judge. From its national security transparency report:

> It is our policy to invoke the "reciprocal notice" procedure in 18 U.S.C. § 3511 for any national security letters (NSLs) served on Automattic. This process ensures that a court will review all non-disclosure orders issued with NSLs we may receive. If and when a non disclosure order is lifted, our policy is to share the contents of the NSL with any affected users (where possible), as well as to publish a redacted version of the NSL.

Pro-user public policy: Reform 702. Wordpress has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Automattic, Wordpress's parent company, was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform

would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens...

Yahoo

Yahoo earns four stars in this year's report. This is Yahoo's sixth year in *Who Has Your Back*, and it has adopted a number of industry best practices, including publishing a transparency report, requiring a warrant for content, and publishing its guidelines for law enforcement requests. Yahoo promises to inform users before disclosing their data to the government and supports substantive reforms to rein in NSA surveillance. Yahoo also forbids third parties from allowing Yahoo user data to be used for surveillance purposes. However, there's room for improvement. We urge Yahoo to create a public policy of requesting judicial review of all National Security Letters it receives.

Follows industry-wide best practices. Yahoo publishes a transparency report and law enforcement guidelines. It requires a warrant before giving user content to law enforcement, stating in its law enforcement guidelines:

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

Tells users about government data demands. Yahoo promises to provide advance notice to users about government data demands, including delayed notice after a gag order expires, stating in its law enforcement guidelines:

> **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.

Promises not to sell out users. Yahoo prohibits third parties from allowing Yahoo user data to be used for surveillance purposes. Its Flickr API terms state:

> You shall not… Knowingly use Flickr APIs to enable any law enforcement entity to investigate, track or surveil Flickr users or their Content, as defined in the Yahoo Terms of Service.

As a result, our reading of Yahoo's public-facing policies would prohibit it from sharing data to be used for surveillance.

Stands up to NSL gag orders. Yahoo does not have a public policy of requesting judicial review of all National Security Letters it receives.

Pro-user public policy: Reform 702. Yahoo has publicly called for reforms to Section 702 to curtail the surveillance of innocent people. Yahoo was a signatory on a joint letter sent to the House Judiciary Committee Chairman and published on the Computer & Communications Industry Association website, which stated:

> As you consider reforms to Section 702, we recommend that you adopt the following changes. First, reauthorization legislation should codify recent changes made to "about" collection pursuant to NSA's Upstream program. This reform would merely codify changes already embraced by the U.S. government with the imprimatur of the Foreign Intelligence Surveillance Court (FISC) to correct deficiencies that implicate the constitutional rights of U.S. citizens…

Links and Additional Resources

Joint letter calling for 702 reform:
https://www.ccianet.org/wp-content/uploads/2017/05/702-letter-201705-FINAL.pdf

Adobe
Law enforcement guidelines:
https://www.adobe.com/legal/lawenforcementrequests.html
Transparency report:
https://www.adobe.com/legal/lawenforcementrequests/transparency.html
Privacy policy:
https://www.adobe.com/privacy.html

Airbnb
Law enforcement guidelines:
https://www.airbnb.com/help/article/960/how-does-airbnb-respond-to-data-requests-from-law-enforcement
Transparency report:
http://transparency.airbnb.com

Amazon
Law enforcement guidelines:
http://do.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf
Transparency report:
http://do.awsstatic.com/certifications/Transparency_Report.pdf
Privacy notice:
https://www.amazon.com/gp/help/customer/display.html?nodeId=468496
Conditions of Use:
https://www.amazon.com/gp/help/customer/display.html?nodeId=508088

Apple
Law enforcement guidelines:
https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf
Transparency report:
https://www.apple.com/privacy/transparency-reports/
Government information requests page:
https://www.apple.com/privacy/government-information-requests/
Privacy policy:
https://www.apple.com/privacy/privacy-policy/

AT&T
Transparency reports:

http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html
http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2017-Transparency-Report.pdf
Privacy policy:
http://about.att.com/sites/privacy_policy

Comcast
Law enforcement handbook:
http://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx
Transparency report:
http://corporate.comcast.com/comcast-voices/comcast-releases-third-transparency-report

CREDO Mobile
Law enforcement guide:
http://www.credomobile.com/law-enforcement-guidelines
Transparency report:
http://www.credomobile.com/transparency

Dropbox
Law enforcement handbook:
https://dl.dropboxusercontent.com/s/chy2h514ht8j2hz/Dropbox%20Law%20Enforcement%20Handbook.pdf?dl=0
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/country/United%20States/2016-H1/
Platform policy:
https://developers.facebook.com/policy/
Privacy policy:
https://www.facebook.com/policy.php

Google
Transparency report:
https://www.google.com/transparencyreport/
Legal process page:
https://www.google.com/transparencyreport/userdatarequests/legalprocess/
FAQ on law enforcement access:

https://www.google.com/transparencyreport/userdatarequests/faq/
Developer agreement:
https://developers.google.com/terms/api-services-user-data-policy

LinkedIn
Law enforcement data request guidelines:
https://www.linkedin.com/help/linkedin/answer/16880?lang=en
Transparency report:
https://www.linkedin.com/legal/transparency
Data request guidelines:
https://help.linkedin.com/ci/fattach/get/6682760/0/filename/Law_Enforcement_Guidelines_11_15_2015_9C7C.pdf

Lyft
Law enforcement guidelines:
https://help.lyft.com/hc/en-us/articles/214218437-Law-Enforcement-Requests
Transparency report:
https://lyft-assets.s3.amazonaws.com/helpcenter/Drive%20With%20Lyft/Lyft%20Transparency%20Report%20-%202015%20(1).pdf
Developer agreement:
https://developer.lyft.com/v1/docs/lyft-developer-platform-terms-of-use

Microsoft
U.S. National Security Order Requests:
https://www.microsoft.com/en-us/about/corporate-responsibility/fisa
Transparency report:
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

Pinterest
Law enforcement guidelines:
https://help.pinterest.com/en/articles/law-enforcement-guidelines
Transparency report:
https://help.pinterest.com/en/articles/transparency-report
Developer guidelines:
https://policy.pinterest.com/en/developer-guidelines

Slack
Data request policy:
https://slack.com/user-data-request-policy
Transparency report:
https://slack.com/transparency-report
Terms of service:
https://slack.com/terms-of-service/user

Snap Inc.
Law enforcement guidelines:
https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf
Transparency report:
https://www.snap.com/en-US/privacy/transparency/

Sonic
Law enforcement guidelines:
https://wiki.sonic.net/images/0/05/Sonic.net_Legal_Process_Policy.pdf
Transparency report:
https://corp.sonic.net/ceo/2017/03/29/2016-transparency-report/
"Privacy Matters" blog post:
https://corp.sonic.net/ceo/2017/03/29/privacy-matters/

T-Mobile
Transparency report:
https://newsroom.t-mobile.com/content/1020/files/2015TransparencyReport.pdf
Privacy policy:
https://www.t-mobile.com/company/website/privacypolicy.aspx

Tumblr
Law enforcement guidelines:
https://www.tumblr.com/docs/en/law_enforcement
Transparency report:
https://www.tumblr.com/transparency
Privacy policy:
https://www.tumblr.com/policy/en/privacy

Twitter
Law enforcement guidelines:
https://support.twitter.com/articles/41949-guidelines-for-law-enforcement
Transparency report:
https://transparency.twitter.com/
Blog post about developer policies:
https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html
Letter to the ACLU:
https://www.aclunc.org/docs/20161212_twitter_letter_to_aclu.pdf

Uber
Law enforcement guidelines:
https://www.uber.com/legal/data-requests/guidelines-for-law-enforcement-united-states/en-US/
Transparency report:

https://transparencyreport.uber.com
Blog post about regulatory data requests on Medium:
https://medium.com/uber-under-the-hood/guard-rails-for-regulatory-data-requests-9f2a46ec3c27

Verizon
Transparency report and law enforcement guide:
https://www.verizon.com/about/portal/transparency-report/us-report/
Privacy policy:
https://www.verizon.com/about/privacy/privacy-policy-summary

WhatsApp
Law enforcement guidelines:
https://faq.whatsapp.com/en/general/26000050
About the transparency report:
https://govtrequests.facebook.com/about/
Transparency report:
https://govtrequests.facebook.com/
Privacy policy:
https://www.whatsapp.com/legal/#privacy-policy-information-you-and-we-share

Wickr
Law enforcement guidelines:
https://wickr.com/legal-process-guidelines
Transparency report:
https://wickr.com/about-us/blog/2017/01/01/wickr-transparency-report
Privacy policy:
https://www.wickr.com/privacy-policy
Blog post about responding to government information requests:
https://support.wickr.com/hc/en-us/articles/115007884208-How-does-Wickr-respond-to-government-requests-for-user-information-
Blog post about stance on surveillance:
https://support.wickr.com/hc/en-us/articles/115007849408-What-is-Wickr-s-stance-on-surveillance-

Wordpress
Law enforcement guidelines:
https://en.support.wordpress.com/report-blogs/legal-guidelines/
Transparency report:
http://transparency.automattic.com/
National security transparency report:
https://transparency.automattic.com/national-security/
Developer guidelines:
https://developer.wordpress.com/guidelines/

Yahoo
Law enforcement guidelines:
https://transparency.yahoo.com/law-enforcement-guidelines
Transparency report:
https://transparency.yahoo.com/
Flickr API Terms:
https://www.flickr.com/services/api/tos/

1 See: Facebook's 2016 U.S. law enforcement requests data (https://govtrequests.facebook.com/country/United%20States/2016-H2/); Google's 2016 U.S. user information requests data (https://www.google.com/transparencyreport/userdatarequests/US/); and Apple's 2016 reports on government information requests (https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf and https://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf).

2 EFF has produced other reports examining the best practices for securing and encrypting data, and continues to investigate this topic. Visit https://www.eff.org/issues/security to learn more.

3 Note that this report is focused on policies relevant to United States law enforcement access. EFF has partnered with organizations based in Brazil, Chile, Colombia, Mexico, Paraguay, and Peru to produce similar reports about telecommunications company policies in those countries.

4 Every year, we make changes to our criteria in order to ensure that they reflect evolving best practices for the industry, meaning that the standards have gotten stronger every year. The exception to this was 2016, when we introduced a new slate of companies in the gig economy to our report and thus awarded stars for the emerging best practices in that industry. For a full discussion of the criteria applied, please read the explanation of the criteria in prior reports.

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

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

7 Some of the Internet services listed in this report are part of another corporate entity also listed in this report, such as Tumblr (owned by Yahoo) or WhatsApp (owned by Facebook). In those instances, the parent company's public position will suffice for credit for both. However, we do not credit statements made by trade groups even if individual companies are members.

8 This was the day that the USA FREEDOM Act was enacted into law. Comments made prior to this date would have been more likely to introduce the prior Congress when considering that set of NSA reforms, rather than the current reform debate.