The Electronic Frontier Foundation's Fourth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data

by Nate Cardozo, Cindy Cohn, Parker Higgins, Kurt Opsahl, and Rainey Reitman

May 15, 2014

ELECTRONIC FRONTIER FOUNDATION
eff.org

Authors: Nate Cardozo, Cindy Cohn, Parker Higgins, Kurt Opsahl, Rainey Reitman

Design assistance: Hugh D'Andrade

A publication of the Electronic Frontier Foundation, 2014

Executive Summary

We entrust our most sensitive, private, and important information to technology companies like Google, Facebook, and Verizon. Collectively, these companies are privy to the conversations, photos, social connections, and location data of almost everyone online. The choices these companies make affect the privacy of every one of their users. So which companies stand with their users, embracing transparency around government data requests? Which companies have resisted improper government demands by fighting for user privacy in the courts and on Capitol Hill? In short, which companies have your back?

These questions are even more important in the wake of the past year's revelations about mass surveillance, which showcase how the United States government has been taking advantage of the rich trove of data we entrust to technology companies to engage in surveillance of millions of innocent people in the US and around the world. Internal NSA documents and public statements by government officials confirm that major telecommunications companies are an integral part of these programs. We are also faced with unanswered questions, conflicting statements, and troubling leaked documents which raise real questions about the government's ability to access to the information we entrust to social networking sites and webmail providers.

The legal landscape is unsettled. The Electronic Frontier Foundation and other organizations have filed constitutional challenges to mass surveillance programs. Both Congress and President Obama are negotiating legislative reform that could curtail or even end bulk surveillance programs, while other Congressional proposals would instead enshrine them into law. In multiple recent public opinion polls, the American people attest that they believe government surveillance has gone too far.

In the face of unbounded surveillance, users of technology need to know which companies are willing to take a stand for the privacy of their users.

In this fourth-annual report, EFF examines the publicly-available policies of major Internet companies—including Internet service providers, email providers, mobile communications tools, telecommunications companies, cloud storage providers, location-based services, blogging platforms, and social networking sites—to assess whether they publicly commit to standing with users when the government seeks access to user data. The purpose of this report is to allow users to make informed decisions about the companies with whom they do business. It is also designed to incentivize companies to adopt best practices, be transparent about how data flows to the government, and to take a stand for their users' privacy in Congress and in the courts whenever it is possible to do so.

The categories we evaluate in this report represent objectively verifiable, public criteria and so cannot and do not evaluate secret surveillance. We compiled the information in this report by examining each company's published terms of service, privacy policy, transparency report, and guidelines for law enforcement requests, if any. As part of our evaluation, we contacted each company to explain our findings and to give them an opportunity to provide evidence of improving policies and practices.

Evaluation Criteria

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

1. **Require a warrant for content of communications.** In this category, companies earn recognition if they require the government to obtain a warrant from a neutral magistrate and supported by probable cause before they will hand over the content of user communications to the government. This policy ensures that private messages stored by online services like Facebook, Google, and Twitter are treated consistently with the protections of the Fourth Amendment.[1]

2. **Tell users about government data requests.** To earn a star in this category, Internet companies must promise to tell users when the government seeks their data unless prohibited by law, in very narrow and defined emergency situations,[2] or unless doing so would be futile or ineffective.[3] Notice gives users a chance to defend themselves against overreaching government demands for their data. The best practice is to give users prior notice of such demands, so that they have an opportunity to challenge them in court, but we

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

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

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

also recognize that prior notice is not always possible, for instance in emergency situations.

3. **Publish transparency reports.** We award companies a star in this category if they publish useful data about how many times government sought user data and how often they provide user data to the government. Until recently, companies were not allowed to include national security requests in transparency reports, and such reporting is still strictly limited by the government, but the government has recently allowed the companies to provide some transparency about those requests.

4. **Publish law enforcement guidelines.** Companies get a star in this category if they make public their policies or guidelines explaining how they respond to data demands from the government, such as guides for law enforcement.

5. **Fight for users' privacy rights in courts.** This star recognizes companies who have publicly confirmed that they have resisted overbroad government demands for access to user content in court.[4]

6. **Publicly oppose mass surveillance.** Tech companies earn credit in this category by taking a public policy position opposing mass surveillance.

Results Summary: Transparency Reports, Notice to Users and Opposition to Mass Surveillance Become Industry Trends

Major Findings in 2014 Report:

- Apple, CREDO Mobile, Dropbox, Facebook, Google, Microsoft, Sonic, Twitter, and Yahoo Top Chart, Receive 6 Stars Each
- Apple, Adobe, Internet Archive, Credo, Dropbox Facebook, Foursquare, Google, LinkedIn, Lookout, Microsoft, Pinterest, Sonic, SpiderOak, Tumblr, Twitter, Wikimedia, Wickr, WordPress, and Yahoo Promise to Give Notice to Users,
- Apple, Yahoo Show Enormous Improvements in Government Access Policies
- Overwhelming Number of the Companies We Reviewed, even Major ISPs like AT&T, Verizon and Comcast Are Now Issuing Transparency Reports

[4] A lack of a star in this category shouldn't be considered a demerit—as we describe above, not all companies will be put in the position of having to defend their users before a judge, but those who do deserve special recognition.

- Majority of Tech Companies (but only one Telecom) Publicly Oppose Mass Surveillance
- CREDO Mobile Demonstrates That Telecom Companies Can Champion Transparency, Resistance to Government Access Requests
- Snapchat, AT&T, and Comcast Lag Behind Others in Industry
- In Wake of Snowden Disclosures, More Companies Revised Policies About Government Access to User Data

This year, we saw major improvements in industry standards for informing users about government data requests, publishing transparency reports, and fighting for the user in Congress. For the first time in our four years of Who Has Your Back reports, every company we reviewed earned credit in at least one category. This is a significant improvement over our original report in 2011, when neither Comcast, Myspace, Skype, nor Verizon received any stars.

These changes in policy were likely a reaction to the releases of the last year, which repeatedly pointed to a close relationship between tech companies and the National Security Agency. Tech companies have had to work to regain the trust of users concerned that the US government was accessing data they stored in the cloud. This seems to be one of the legacies of the Snowden disclosures: the new transparency around mass surveillance has prompted significant policy reforms by major tech companies.

We are pleased to announce that nine companies earned stars in every category: Apple, CREDO Mobile, Dropbox, Facebook, Google, Microsoft, Sonic, Twitter, and Yahoo. In addition, six companies earned stars in all categories except a court battle: LinkedIn, Pinterest, SpiderOak, Tumblr, Wickr, and WordPress. We are extremely pleased to recognize the outstanding commitment each of these companies has made to their users. CREDO Mobile, a new addition to this year's report, demonstrated through its exemplary policies that it is possible for a telecom to adopt best practices when it comes to transparency and resistance to government demands.

We added several other new companies to our report this year, including the Adobe, Internet Archive, Lookout, Pinterest, Snapchat, Wickr, and Wikimedia. Each of these companies has a significant user base and some hold huge amounts of sensitive user data that could be the target of invasive government investigations. Most of them scored quite well.

However, Snapchat stands out in this report: added for the first time this year, it earns recognition in only one category, publishing law enforcement guidelines. This is particularly troubling because Snapchat collects extremely sensitive user data,

including potentially compromising photographs of users. Given the large number of users and nonusers whose photos end up on Snapchat, Snapchat should publicly commit to requiring a warrant before turning over the content of its users' communications to law enforcement. We urge them to change course.

Improvements Since 2013

We saw two companies make enormous improvements in the last year: Apple and Yahoo.

In 2013, Apple earned only one star in our Who Has Your Back report. This year, Apple earns 6 out of 6 stars, making remarkable progress in every category.

Similarly, Yahoo jumped to earning credit in all 6 categories this year. Yahoo deserves special recognition because it fought a many-year battle with the Foreign Intelligence Surveillance Court, defending user privacy in a secret court battle that it was forbidden from discussing publicly until July of 2013,[5] but it also made great strides in other areas.

Microsoft also jumped to 6 stars, promising to give notice and in protecting a user in the courts.

Facebook has also made notable improvements over the years, moving from one star in 2011, to 1.5 stars in 2012, to 3 stars in 2013, and finally to 6 stars in this year's report.

Warrant for Content

We are pleased to note that more companies are publicly committed to requiring warrants from law enforcement before handing over user data, including for the first time Amazon, Apple, Verizon, and Yahoo. We were particularly impressed by the strong language in Tumblr's policies when it comes to warrants:

> 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…. Requests must

[5] Read more: https://www.eff.org/deeplinks/2013/07/yahoo-fight-for-users-earns-company-special-recognition

come from appropriate government or law enforcement officials; Tumblr will not respond to requests from other sources.

User Notification

The Who Has Your Back report was partially inspired by Twitter's fight to tell users that their data was being sought as part of the WikiLeaks investigation in 2010. Since then, we have rated companies on whether they promise to tell users about government demands for their data. More companies are promising to inform users about government data requests, including for the first time Facebook, Microsoft, Apple, Tumblr and Yahoo. And we're pleased that Google has revised its user notification policy to remove some vague language it had added last year. As a result, we reinstated Google's star in the notice category.

LinkedIn has particularly clear language describing its commitment to notify users of government data demands, and pointing out to law enforcement the proper legal mechanism to use when an investigation might require delayed notice:

> When our Members trust LinkedIn with information about their professional lives, they expect to have control over their data. Thus, LinkedIn's policy is to notify Members of requests for their data unless it is 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 process that specifically precludes Member notification, such as an order issued pursuant to 18 U.S.C. §2705(b).

Transparency Reports & Law Enforcement Guides

Annual transparency reports are also becoming a standard practice for major communications companies. In fact, almost all of the companies we examined have now published transparency reports. For the first time, we are seeing major telecom companies publishing transparency reports, including AT&T, Comcast, CREDO Mobile, and Verizon. We are particularly glad to see Facebook's recent transparency report, which we have anticipated for many years.

EFF believes that National Security Letters (NSLs)—secretive FBI orders for user data accompanied by a gag provision—are a violation of the Constitution. We are currently litigating a challenge to the NSL statute, and a federal district court recently held that NSL gags are unconstitutional but stayed the order while the government appeals. We think it is vital that companies are as forthcoming as legally allowable about these national security requests to help shed light on government abuses of contested surveillance powers.

Several companies, including Apple, AT&T, Comcast, Credo, Dropbox, Facebook, Google, Internet Archive, LinkedIn, Lookout, Microsoft, Pinterest, Tumblr, Verizon, Wickr, WordPress, and Yahoo deserve particular recognition for including information about national security requests, such as National Security Letters they have received (if any). While companies are gagged from discussing specifics about National Security Letters that they receive, they are now permitted to publish general information about how many NSLs were received in a year and how many accounts were affected. Several companies stated that they fought government demands brought under national security laws even while being gagged, fights that are particularly important since the secrecy means that users cannot stand up for themselves.

As with transparency reports, the overwhelmingly number of companies we examined have published their law enforcement guidelines, some directly and some, like Facebook and Microsoft, with a user-friendly interactive guide.

Fighting for Users in the Courts

One category we're tracking deserves special discussion: standing up for users in court. **It is important to note that not every company has been presented with an opportunity to go to court to challenge the government over user privacy and that sometimes companies are gagged when they do.** Some companies have never received an overbroad subpoena, others may have convinced the FBI to withdraw one, and still others may be subject to a gag—yet none of those circumstances would merit a star.

Thus, just because a particular company doesn't have a star in the fifth column, it doesn't necessarily mean that it doesn't have your back—it just means that we cannot verify that it has been put into a situation where it has needed to defend user privacy in court. At the same time, standing up for users in court is a vital check on overbroad government data demands. We want to recognize those companies that have fought for their users in court so they can receive credit and so their stories can inspire others.

In particular, this past year we finally learned that Yahoo had engaged in a multi-year battle in the secret FISA Court, though it did not receive a star for several years in our report because it was prevented for publicizing this fact. We also learned that Microsoft had resisted a request for user data stored in Ireland. We commend Yahoo, Microsoft, and other companies that have fought for user privacy in courts.

Fighting for Users in Congress

In years past, we have given credit for standing up in Congress to companies that participated in the Digital Due Process coalition, which encourages Congress to improve the outdated Electronic Communications Privacy Act. While this remains an important goal, in the wake of the Snowden revelations, this year focuses on the fight in Congress over mass surveillance. As a result, this year we are rating companies on whether they have taken a public policy position opposing mass warrantless surveillance.

This is because such positions are an important demonstration to users and because company participation, especially public participation, is so important for the Congressional debate given the key role that companies play in the government's surveillance strategy (both wittingly and unwittingly). It's also within reach for every company we track.

Mass surveillance of law-abiding users infringes on fundamental individual rights of free expression and privacy, and the specter of mass data collection threatens user trust all around the world. Every technology company should stand by its users and urge Congress to end warrantless mass surveillance programs once and for all. While this report only tracks response to US government demands, taking a stand against US government activity can also help companies stand strong against requests from foreign governments.

We are pleased to note that many of the major Internet companies and even some telecommunication companies have taken a public stand, many through the Reform Government Surveillance coalition but also through the StopWatchingUs coalition. WordPress (and its parent company Automattic), demonstrated leadership in demanding an end to mass spying by creating a WordPress plug-in that allowed users to opposing mass spying on their own WordPress blogs, in addition to issuing a public statement opposing warrantless surveillance.

Conclusions

This has been a watershed year for companies taking a stand for user privacy, with more companies than ever publishing transparency reports, law enforcement guides, and publicly opposing mass surveillance. But there is still room for growth.

Transparency reports have become the industry standard for major tech companies, but Adobe, Amazon, Foursquare, Myspace, Wikimedia and Snapchat have yet to publish a report.

Additionally, Comcast has grown into a leading ISP and is seeking to grow significantly with its purchase of Time Warner Cable. It should step up to be a leader in protecting its growing number of customers. AT&T and Verizon issued transparency reports, but remain near the bottom of the pack despite their key role in the communications infrastructure. Amazon has a tremendous amount of user data, both from its direct retail businesses and from its hosting services through Amazon Web Services, but it fails to let users, and potential users, evaluate their policies and understand how law enforcement seeks to gain access to data stored with them.

This report is encouraging, with many companies heading in the right direction, especially based on where we started in 2011. Yet the report also makes clear that the law has fallen woefully behind in protecting users as users increasingly rely on changing technologies. This past year confirmed that the government has been relying on legal uncertainties and technological innovations to push for as much access as possible to user information, stretching policy, statutory interpretation, and constitutional law past the breaking point.

Too often, technology companies are the weak link, providing the government with a honeypot of rich data. We must strengthen their ability to resist overbroad data demands and bring light to the flow of data from corporate servers to the government.

New Companies in the 2014 Report

Companies included in last year's report: Amazon, Apple, AT&T, Comcast, Dropbox, Facebook, Foursquare, Google, LinkedIn, Microsoft, MySpace, Sonic.net, SpiderOak, Twitter, Tumblr, Verizon, WordPress (Automattic, Inc.), Yahoo

New companies added to this year's report: Adobe, Internet Archive, CREDO Mobile, Lookout, Pinterest, Snapchat, Wickr, and Wikimedia

The Who Has Your Back report initially surveyed the practices of the largest US social networks, Internet Service Providers, telecommunications providers, and email providers. Over time, we've expanded the scope to include a number of other technology companies that maintain large quantities of user data ripe for government access demands, including location services, mobile services, and cloud storage providers.

This year, we are pleased to be adding several new companies to our report, including:

- **Adobe,** which maintains nearly a dozen user generated content sites, including cloud storage, webhosting and a social network;
- **CREDO Mobile**, an American mobile phone service virtual network operator;
- **Internet Archive**, a nonprofit digital library that provides access to historical web content through its Wayback Machine as well as archives of text, video, and audio content that may be of public interest;
- **Lookout**, a mobile phone security company that helps users secure their smartphones by providing information about other apps on their phones as well as phone finder services;
- **Snapchat,** a widely-used photo messaging app that allows users to share content with a limited number of recipients for a short period of time;
- **Wikimedia**, the parent organization of a range of projects, including Wikipedia, Wikibooks, and Wiktionary; and
- **Wickr,** which offers secure communication services for mobile devices.

In Depth: Specific Criteria and Changes for 2014

Here's a closer look at each of the categories we used to judge companies' commitments to transparency and user privacy in the face of government access requests.

Requiring a Warrant for Content

In this category, added to the report in 2013, companies earn recognition if they require the government to get a warrant supported by probable cause before they will hand over the contents of user communications.[6]

We have this category because we believe that the Fourth Amendment protects communications stored with service providers, and the government must have a search warrant before it can seize those messages. This view was upheld by the 2010 Sixth Circuit Court of Appeals decision in *United States v. Warshak*.[7] This decision was a critical victory for Internet privacy, but represents the holding of one appeals court—and thus is not binding legal precedent throughout the entire country.

---

[6] Under one key federal statute, the Stored Communications Act, the "contents" of a wire, oral, or electronic communication means "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

[7] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *see also* "Breaking News on EFF Victory: Appeals Court Holds That Email Privacy Protected by Fourth Amendment," EFF, Dec. 14, 2010, https://www.eff.org/deeplinks/2010/12/breaking-news-eff-victory-appeals-court-holds.

We award stars to companies that commit to following the *Warshak* standard nationwide. When companies require a warrant before turning over private messages to law enforcement, they ensure that private communications online are treated consistently with the protections the Fourth Amendment gives to communications that occur offline.

Telling Users About Government Data Requests

This category requires a company to make a public promise to let users know when the government seeks access to their data, unless providing notice is prohibited by law or a court order. We allow an exception to providing notice to the user in very narrow and defined emergency situations,[8] and in cases in which providing notice would be futile, for example when an account has been compromised or a device stolen and the only way to inform the user is to simultaneously (or only) inform the attacker.

The commitment to providing notice is crucial because it gives users a chance to defend themselves against—or to seek a remedy for—overreaching government requests. In most situations, a user is in a better position than a company to challenge a government request for personal information, and, of course, the user has more incentive to do so.

Promising to give notice is an important commitment to make, and means the company is not acting as a judge over the merits—the company doesn't have to evaluate the request, it merely has to pass on important information to the user. Companies don't have to give notice if the law or a court order prohibits it.

Ideally, notice should be provided prior to the user data being shared with the government in order to give the user an opportunity to seek legal counsel and oppose the access request, but we also recognize that prior notice is not always possible, for instance in a narrow range of emergency situations. While we believe that notice should eventually be provided once the emergency passes, for this year, as long as the emergency exception is very narrow,[9] we are not requiring the company to promise to give subsequent notice.

---

[8] The exceptions should not be significantly broader than the emergency exceptions provided in the Electronic Communications Privacy Act, 18 USC § 2702 (b)(8), which allows for voluntary disclosure when there is "danger of death or serious physical injury to any person."

[9] See fn. 8.

While we think companies should make this promise in their terms of service or privacy policies, we gave companies credit if they made it in another official, enforceable way, such as in law enforcement guidelines or transparency reports.

Publishing Transparency Reports

In order to earn a gold star in this category, companies must provide reports on how often they provide data to the government. Users make decisions every day about which companies they will entrust with their data. It's vital that companies are forthcoming about how often they hand that data to the government.

We evaluated whether companies publish the number of government demands they receive for user data, whether it's an official demand such as a warrant or an unofficial request. Google led the way in this category by issuing the very first transparency report, and the company continues to publish very useful reports twice a year.

A number of companies now publish information about national security requests, including National Security Letters and FISA court orders. Recipients of National Security Letters are typically subject to gag orders issued by the FBI alone—without judicial oversight—that forbid them from ever revealing the letters' existence to their boards of directors and all but a few employees, much less the public. Similarly, recipients of FISA court orders are also barred from discussing the orders they receive.

However, in January 2014 the government announced a policy that allows companies to report national security requests in broad bands of 1000, starting at zero. So a company can report receiving 0-999 NSLs or 1000-1999 FISA orders. If the company combines all forms of national security data demands into one bunch, the bands can be 250, again starting at zero.

While only full disclosure of all kinds of government requests for user information will fully inform the public, companies that disclose as much as they can about these requests still advance the public's understanding of these often dangerous and much-abused government powers. Until the courts reach a final consensus on the constitutionality of these gags on speech, these reports provide a small but vital level of public transparency around otherwise secretive legal instruments.

Publishing Law Enforcement Guidelines

We also evaluated whether companies publish their guidelines for law enforcement requests for user data. Law enforcement guides might provide insight into issues such as:

- Whether a company requires a warrant for content;

- What types of data a company retains, and what kind of legal process the company requires for law enforcement to obtain various kinds of information;
- How long data is generally held by the company, and how long will it be held in response to a retention request;
- Whether the company has an exception for specific emergency or other kinds of disclosures; and
- Whether the company asks for reimbursement for the costs incurred in complying with a request for data.

These published guidelines help us better understand what standards and rules law enforcement must follow when they seek access to sensitive user data on a variety of different platforms. They also help companies avoid receiving improper requests in the first place, by educating law enforcement about what they can and cannot obtain, and the standards that must be met.

Fighting for Users' Privacy in Court

Companies earn recognition in this category by going to court to fight for their users' privacy interests in response to government demands for information — companies that have actually participated as litigants and made legal arguments defending their users' privacy rights. Such an action is powerful proof of a company's commitment to user privacy and its willingness to fight back when faced with an overbroad government request.

Of course some companies may not have had occasion to defend users' rights in court, others may successfully push back on overreaching law enforcement demands informally thus avoiding a court battle. Still others may be bound by the secrecy of gag orders accompanying National Security Letters, or imposed by court orders or statutes, leaving them unable to disclose the efforts they have made to protect their users' interests. **As a result, the lack of a star in this category should *not* be interpreted as a statement that the company failed to stand up for users.** Instead, this category serves as special recognition for companies that were faced with a decision to defend user privacy in court, took action to defend that privacy, and could publicly disclose at least something about their efforts, even if it's just the fact of having fought in court.

The majority of the companies listed have a known, publicly available court challenge to a government access demand. However, some companies have provided us with documentation of their legal challenges which otherwise may not be publicly available. Others have agreed to publicly acknowledge their legal challenge in general terms, without violating the gag or sealing order that may be applicable. We credit any of these with a star in this category.

Fighting for Users' Privacy in Congress

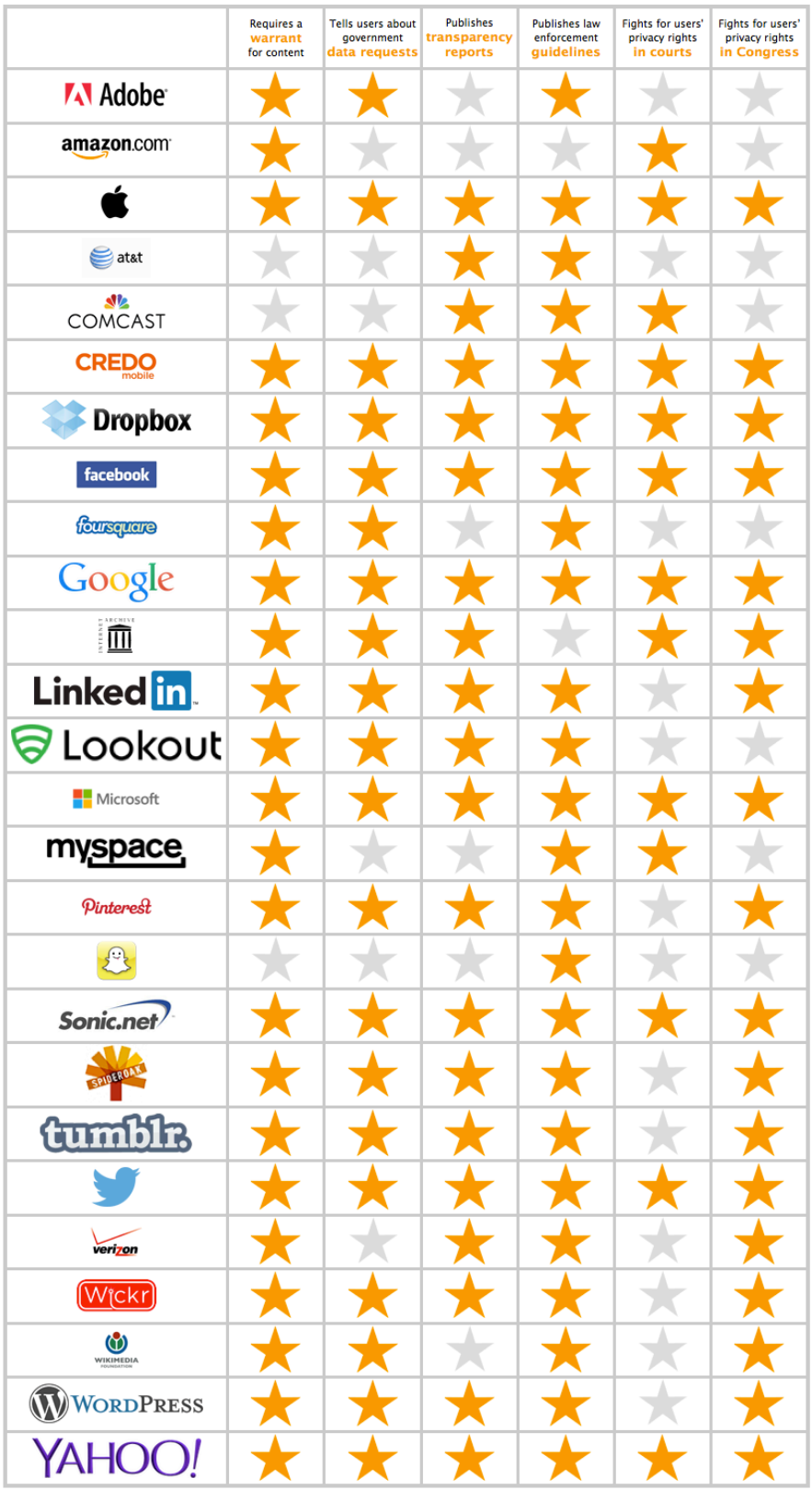
While company policies are important, we shouldn't be dependent on them to protect our privacy. The law should clearly protect the privacy of users even as technologies change. This is particularly important in the wake of the recent disclosures about mass surveillance, which show how far the government's interpretation of the law has wandered from the statutory language and Congressional intent and how extensively the government has manipulated the legal language to try to provide leeway for surveillance abuses.

As the final category of our report, we evaluate whether companies are working for lasting, permanent improvements in the law to safeguard their users' privacy.

In years past, we have given credit for standing up in Congress to companies that participated in the Digital Due Process coalition, which encourages Congress to improve the outdated Electronic Communications Privacy Act. While this remains an important goal, there is far more to be done to safeguard our digital data. We are retiring the Digital Due Process membership as a criterion, rewarding companies instead for a public statement clearly opposing mass surveillance. For example, companies can sign onto a coalition letter, join a coalition, publish their own document, or integrate a statement into their formal policies objecting to bulk data collection and calling for reform of the law. However, simply calling for additional transparency around surveillance, rather than opposing mass surveillance itself, does not qualify for a star in this category. Transparency is important, but this category is for fighting for the users directly.

The public statements of multiple companies opposing mass surveillance can help provide political will and incentives for members of Congress to take meaningful action to end bulk collection. It also encourages users to get involved. This is particularly important right now, as Congress considers multiple legislative proposals regarding NSA surveillance reform.

2014 Results Table



Company Results

Adobe

Adobe earns three stars in this year's Who Has Your Back report. This is Adobe's first year in the Who Has Your Back Report, and it has already adopted a number of practices worth commendation. In particular, the company requires a warrant for content and promises to notify users of government data requests. It also publishes its law enforcement guides.

However, Adobe has yet to publish a transparency report and has not yet publicly opposed mass surveillance. Adobe has room for improvement in both categories.

Warrant for content. Adobe requires a warrant before giving content to law enforcement, stating in its law enforcement guidelines:

> However, we 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.

Inform users about government data demands. Adobe promises to tell users about government data demands, stating:

> 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, such as when we receive a Delayed Notice Order under 18 USC Section 2705(b).

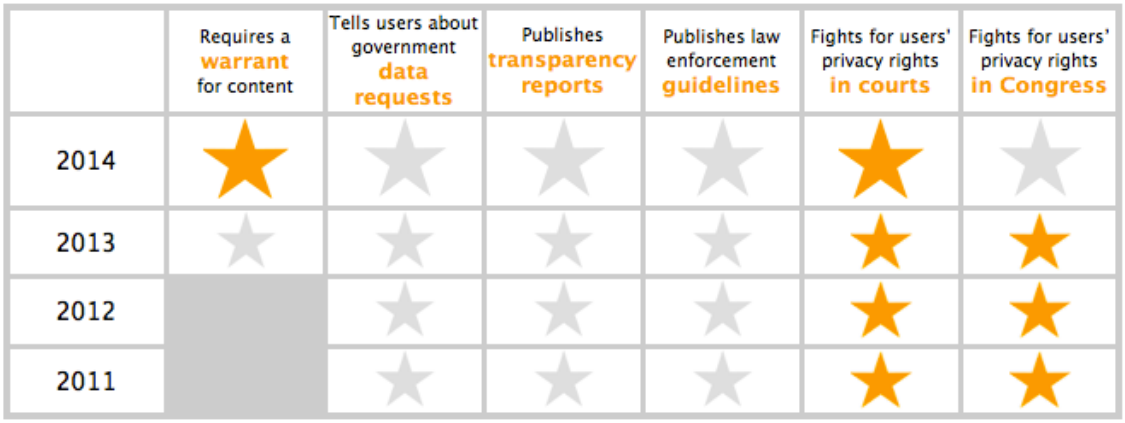
Publish transparency report. Adobe has never published a transparency report showing government requests for data.

Publish law enforcement guides. Adobe publishes its guidelines for law enforcement seeking access to user data.

Fight for users privacy in courts. Adobe does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Adoble's lack of star in this category should not be seen as a demerit

Oppose mass surveillance. Adobe has not publicly opposed mass surveillance through a written statement.

Amazon



Amazon earns two stars in this year's Who Has Your Back report. Amazon should be commended for repeatedly fighting in court to protect the privacy of its users' book purchases and for requiring a warrant before giving data to the government. However, Amazon has not publicly adopted industry best practices in other categories, such as providing notice to users about government data requests.

While other tech companies reacted to recent disclosures about mass surveillance by publishing transparency reports and publicly advocating for reform of surveillance law, Amazon has stayed largely silent. When it comes to transparency about its practices Amazon has fallen behind its peers in the tech industry.

Warrant for content. Amazon receives credit in this category because of the testimony of its Vice President for Global Public Policy, Paul Misener, before the House Judiciary Committee in 2010[10]: "With respect to the content of electronic communications, we believe that ECPA requires law enforcement authorities to obtain a search warrant to compel disclosure. We do not release information without valid process and have not disclosed content without a search warrant."

Inform users about government data demands. Amazon does not promise to tell users about government data demands.

Publish transparency report. Amazon has never published a transparency report showing government requests for data.

Publish law enforcement guides. Amazon does not publish its guidelines for law enforcement seeking access to user data.

[10] Amazon provided the full transcript of the testimony to EFF.

Fight for users privacy in courts. Amazon earns a star for repeatedly fighting to protect the privacy of its users' book purchases in the face of both federal and state government demands.

Oppose mass surveillance. Amazon has not publicly opposed mass surveillance through a written statement.

Apple

Apple earned credit in all 6 categories in this year's Who Has Your Back report. Apple's rating is particularly striking because it had lagged behind industry competitors in prior years, earning just one star in 2011, 2012, and 2013. Apple shows remarkable improvement in its commitments to transparency and privacy.

Warrant for content. Apple requires a warrant before providing content to law enforcement. Specifically, in its November transparency report it stated: "As we have explained, any government agency demanding customer content from Apple must get a court order."

Inform users about government data demands. Apple promises to tell users if the government seeks their data. According to its soon-to-be-published policy:

> Apple will notify its customers when their personal information is being sought in response to legal process except where providing notice is prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), or by applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment.

Publish transparency report. Apple published its first transparency report in November 2013, indicating by country how many legal requests it had received, complied with, and how many accounts are affected. Apple includes information about FISA court orders under Section 215 in its transparency report.

Publish law enforcement guides. Apple publishes its law enforcement guidelines.

Fight for users privacy in courts. Apple is adding the following statement to its transparency report update, scheduled for May 2014.

> If there is any question about the legitimacy or scope of the court order, we challenge it and have done so in the past year.

Oppose mass surveillance. Apple is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

AT&T

AT&T took positive steps toward embracing greater transparency this year, but fell far short of standing up for user privacy. This year, AT&T published its first transparency report and law enforcement guidelines. However, AT&T continues its long pattern of failing to stand by users against overbroad government data demands. It does not have a policy of requiring a warrant before providing content to the government, and it has no policy of informing users of government data requests.

It is particularly disappointing to see AT&T silent on the issue of mass surveillance. In 2006, EFF sued AT&T for its cooperation and collaboration with the NSA spying program, which was confirmed by whistleblower documents. In 2008, Congress passed retroactive immunity for AT&T, which ended our case but not the telecom's participation in mass surveillance.

Warrant for content. AT&T does not specify that a warrant is required to access content.

Inform users about government data demands. AT&T does not promise to tell users about government data demands.

Publish transparency report. AT&T published its first transparency report in 2014. It includes information about National Security Letters and FISA court orders in its transparency report.

Publish law enforcement guides. AT&T publishes its law enforcement guidelines, earning a star in this category for the first time.

Fight for users privacy in courts. AT&T does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over

user privacy but may be legally prevented from ever publicly discussing those efforts. AT&T's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. AT&T has not publicly opposed mass surveillance through a written statement.

Comcast

Comcast earns 3 stars in this year's Who Has Your Back report. We are pleased to recognize that Comcast published its first transparency report showing the amount and types of government requests for consumer information. This is a vital step for transparency and worthy of commendation. However, Comcast has not yet adopted best practices like requiring a warrant for content or providing notice to users about government data requests.

We are also disappointed that Comcast has not joined other technology companies in publicly opposing mass surveillance.

Warrant for content. Comcast does not specify that a warrant is required to access content.

Inform users about government data demands. Comcast does not promise to tell users about government data demands.

Publish transparency report. Comcast published its first transparency report in March 2014. It includes information about National Security Letters and FISA orders.

Publish law enforcement guides Comcast publishes its law enforcement guidelines.

Fight for users privacy in courts. Comcast fought an IRS subpoena on behalf of its users in 2003. This refers to *United States v. Comcast Cable Comm.,* No. 3-03-0553 (M.D. Tenn. 2003). Comcast provided EFF with a transcript of the hearing.

Oppose mass surveillance. Comcast has not publicly opposed mass surveillance through a written statement.

CREDO Mobile

	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
2014	★	★	★	★	★	★

CREDO earned 6 stars in this year's Who Has Your Back report, receiving recognition in every category.

Though this is CREDO Mobile's first year in the report, it has demonstrated that telecom companies can defend user privacy and embrace meaningful transparency, just as other major technology companies do. CREDO is particularly notable because it was the first major American telecom company to publish a transparency report, paving the way for other companies such as AT&T and Verizon.

Warrant for content. CREDO Mobile requires a warrant before giving content to law enforcement, stating:

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

Inform users about government data demands. CREDO Mobile promises to tell users if their data is sought by the government, stating:

> It is our policy to notify our customers, whenever allowed by law, of the existence of a governmental request for their information.

Publish transparency report. In 2014, CREDO Mobile became the first telecom company[11] to publish a transparency report.

Publish law enforcement guides. CREDO publishes its law enforcement guidelines.

Fight for users privacy in courts. CREDO states in its law enforcement guidelines "If there is any question about the legitimacy or scope of the legal process, we challenge it in court and have done so."

[11] http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/09/the-first-phone-company-to-publish-a-transparency-report-isnt-att-or-verizon/

Oppose mass surveillance. CREDO is a member of the Stopwatching.us coalition, which states:

> This dragnet surveillance violates the First and Fourth Amendments of the U.S. Constitution, which protect citizens' right to speak and associate anonymously, guard against unreasonable searches and seizures, and protect their right to privacy. We are calling on Congress to take immediate action to halt this surveillance and provide a full public accounting of the NSA's and the FBI's data collection programs.

In addition, CREDO has stated in its transparency report:

> CREDO supports the repeal the USA PATRIOT Act of 2001 and the FISA Amendments Act of 2008, and the passage of Rep. Rush Holt's Surveillance State Repeal Act. Until full repeal can be achieved, CREDO has worked specifically to reform the worst abuses of both acts. This includes fighting to roll back the National Security Letter (NSL) provisions of the USA PATRIOT Act, and fighting to make FISA Court opinions public so that the American people know how the secret FISA court is interpreting the law. CREDO endorses the USA Freedom Act and the Amash Amendment, both aimed at halting the indiscriminate dragnet sweeping up the phone records of Americans. CREDO also opposes Senator Feinstein's FISA Improvements Act which would codify the NSA's unconstitutional program of surveillance by bulk collection.

Dropbox

Since its inclusion in our Who Has Your Back report in 2012, Dropbox has consistently demonstrated strong transparency around government data requests and a commitment to protecting the privacy of its users. This year is no exception, with Dropbox setting a strong example for other cloud storage companies.

We are particularly pleased to see Dropbox requiring a warrant before providing content to law enforcement and publicly opposing mass surveillance.

Warrant for content. Dropbox requires a warrant in order to access content, stating:

> Dropbox will not provide user content, whether in files or otherwise, without a search warrant (or an equivalent legal obligation supported by probable cause) that requires the content to be disclosed.

Inform users about government data demands. Dropbox promises to tell users about government demands for data, stating:

> Dropbox's policy is to provide notice to users about law enforcement requests for their information prior to complying with the request, unless prohibited by law.
>
> We might delay notice in cases involving the threat of death or bodily injury, or the exploitation of children

Publish transparency report. Dropbox publishes a transparency report.

Publish law enforcement guides. Dropbox publishes its law enforcement guides.

Fight for users privacy in courts. Dropbox stated in its 2013 transparency report: "Dropbox has also fought for users' privacy rights in the judicial system. Specifically, Dropbox fought against a warrant in a sealed proceeding."

Oppose mass surveillance. Dropbox is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

Facebook

Facebook earns 6 stars in this year's Who Has Your Back report.

Facebook published its first transparency report in 2013, bringing it into alignment with companies like Twitter and Google. We are especially pleased to see Facebook promising to inform users of government data requests. We are pleased to see Facebook adopting more transparency around law enforcement access. Facebook was also one of the original members of the Reform Government Surveillance coalition, which opposes dragnet surveillance and champions reform of surveillance law.

Warrant for content. Facebook requires a warrant for content, stating:

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

Inform users about government data demands. Facebook's law enforcement guidelines make a commitment to notify users of data requests:

> 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. 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.

Publish transparency report. Facebook published its first transparency report in 2013.

Publish law enforcement guides. Facebook publishes its law enforcement guidelines.

Fight for users privacy in courts. Facebook confirms that they have fought a government data request in court, and made the following public statement to that effect:

> Facebook has also gone to court to fight against overbroad law enforcement requests, but at least in the United States, that litigation has generally been under seal to protect both the integrity of the law enforcement investigation and the privacy of the people whose data was at risk.[12]

Oppose mass surveillance. Facebook is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

[12] https://www.facebook.com/joesullivan/posts/10152441754851103

Foursquare

Foursquare earns 3 stars in this year's Who Has Your Back report.

We are pleased to see Foursquare continue to uphold strong standards around informing users about government demands for their data. However, Foursquare has yet to issue a transparency report, which has become standard for most of the technology companies we evaluated. It also has yet to take a public stand opposing mass surveillance. While far from the bottom of the barrel, Foursquare has room to grow when it comes to transparency about government data requests.

Warrant for content. Foursquare requires a warrant for content, stating:

> A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of other user data, not including contents of communications, which may include photographs and other electronic communication information in addition to the basic user data identified above.
>
> A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant showing of probable cause is required to produce stored contents such as tips, check-ins, photographs and location information.

Inform users about government data demands. Foursquare promises to tell users about government demands for data:

> Foursquare will notify users of requests for their data unless it is 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 process establishing that notice is prohibited. Furthermore, if the request draws attention to an ongoing violation of our terms of use, we may take action to prevent any further

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

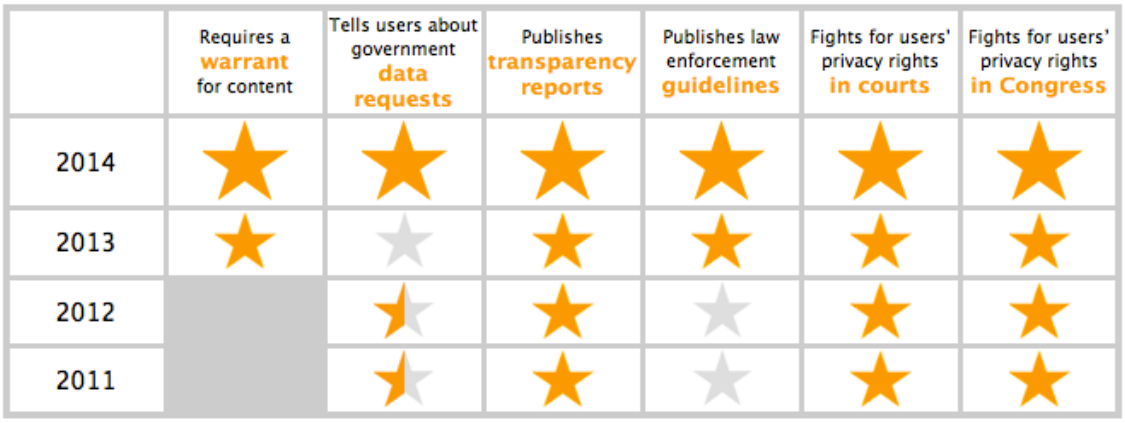
Publish transparency report. Foursquare does not publish a transparency report.

Publish law enforcement guides Foursquare publishes its law enforcement guides.

Fight for users privacy in courts. Foursquare does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Foursquare's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Foursquare has not publicly opposed mass surveillance.

Google



Google earns 6 stars in this year's Who Has Your Back report.

Google has long led the way in transparency reports, creating detailed reports on government access requests long before other tech companies began doing so. Their transparency report continues to be detailed and granular. We are also pleased that Google is strengthening its language around providing notice to users about government data requests, and has publicly opposed mass surveillance.

Warrant for content. Google requires a warrant before providing content to law enforcement. Specifically, it states in its policy:

> 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.

Google tells us that they plan to clarify that this requirement applies to requests under FISA and for National Security Letters, which are not strictly under ECPA.

Inform users about government data demands. In 2011 and 2012, Google earned a half-star for providing notice to users about government requests for their data because the policy was part of a blog post[13] rather than a formal privacy policy. In 2013, Google lost its half-star when it adjusted its formal policy language,

[13] Chief Legal Officer David Drummond had written in a blog post "Whenever we can, we notify users about requests that may affect them personally." This was also reflected in the apps administration policy, which stated "Google complies with valid legal process. It is Google's policy to notify users before turning over their data whenever possible and legally permissible." See: http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html

weakening it significantly to say simply "We notify users about legal demands when appropriate, unless prohibited by law or court order."

This year, Google earns a star for a policy that is currently in effect and will be published in July:[14]

> 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. This gives the user an opportunity to file an objection with a court or the requesting party. If the request appears to be legally valid, we will take steps to preserve the requested information before we notify the user.
>
> There are a few exceptions to this policy:
> - A statute, court order or other legal limitation may prohibit Google from telling the user about the request;
> - We may not give notice in exceptional circumstances involving danger of death or serious physical injury to any person;
> - We may not give notice when we have reason to believe that the notice wouldn't go to the actual account holder, for instance, if an account has been hijacked.
>
> We review each request we receive before responding to make sure it satisfies applicable legal requirements and Google's policies. In certain cases we'll push back regardless of whether the user decides to challenge it legally.

Publish transparency report. Google was the first tech company we reviewed to publish a transparency report, and continues to be a leader in providing detailed, useful information about government data requests, their compliance rates, and affected accounts. They also provide data about National Security Letters.

Publish law enforcement guides. Google publishes its law enforcement guides.

Fight for users privacy in courts. Google has fought for user privacy on multiple occasions, including resisting a Justice Department subpoena for search logs in 2006, reportedly going to court to defend the privacy of a user whose information was sought in the WikiLeaks investigation[15], and challenging a National Security Letter[16].

---

[14] Provided by Google to EFF for publication in this report.

[15] http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html

[16] http://www.bloomberg.com/news/2013-04-04/google-fights-u-s-national-security-probe-data-demand.html

Oppose mass surveillance. Google is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

Internet Archive

The Internet Archive earned 5 stars in this year's Who Has Your Back report, a very strong showing for its first year in the report. The Internet Archive earns particular recognition for its court challenge to a National Security Letter. In 2008 EFF and the ACLU defended the Internet Archive from an unconstitutional National Security Letter. Because NSLs come with a gag order, most recipients are unable to ever reveal their existence. However, the Internet Archive fought back and won the right to speak publicly about the letter, a case that has become one of the few well-documented cases of NSL use.

Warrant for content. Internet Archive requires a warrant for content, stating:

> The Internet Archive requires a search warrant before disclosing to law enforcement the contents of non-public user communications.

Inform users about government data demands. Internet Archive promises to tell users if the government seeks their data. According to its policy:

> The Internet Archive attempts to notify users about criminal subpoenas or other formal requests seeking their non-public data unless prohibited by law or if doing so would be futile or ineffective.

Publish transparency report. Internet Archive published a report about government data requests, the degree to which the Archive complied with the requests, and the number of accounts targeted. It included information about national security requests.

Publish law enforcement guides The Internet Archive does not publish a guide for law enforcement on how to request data.

Fight for users privacy in courts In December 2007 the Internet Archive along with its co-counsel American Civil Liberties Union and Electronic Frontier Foundation filed a lawsuit challenging a national security letter issued to the Archive. (*Internet Archive et al v. Mukasey et al,* No. 07-6346-CW (N.D. Cal)). The lawsuit was filed under seal due to the strict non-disclosure rules imposed by the national security letter authority. In April 2008 the government formally withdrew

the unconstitutional letter and settled the case. In May 2008, the Court unsealed the case allowing the Archive's story to become public for the first time.[17]

Oppose mass surveillance. Internet Archive opposes mass surveillance, stating[18]:

> Our position is that governments should limit surveillance to specific, known users for lawful purposes and not undertake bulk collection of non-public communications data.

[17] https://www.eff.org/cases/archive-v-mukasey

[18] http://archive.org/about/faqs.php#1006

LinkedIn

LinkedIn made a very strong showing in this year's report, earning 5 stars. It uses unquestionably strong language in its policies requiring a warrant before giving content to law enforcement and for informing users about government demands for their data. It has also opposed mass surveillance and published both law enforcement guidelines and a transparency report.

While LinkedIn does not receive credit for fighting for user privacy in the courts, this should not be held against it. Many companies do not have an opportunity to fight in court against an overbroad government data demand, or may be barred from discussing those legal challenges publicly.

Warrant for content. LinkedIn requires a warrant for content, stating:

> LinkedIn strongly believes that all data, whether analog or digital, whether stored on personal computers or in the cloud, is subject to full Fourth Amendment protection, no less than documents stored in a file cabinet or in a desk drawer. Thus, given our members' expectations of privacy, we require a search warrant to produce all content, including without limitation, Connections.

Inform users about government data demands. LinkedIn promises to tell users about government data demands, stating:

> When our Members trust LinkedIn with information about their professional lives, they expect to have control over their data. Thus, LinkedIn's policy is to notify Members of requests for their data unless it is 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 process that precludes Member notification, such as an order issued pursuant to 18 U.S.C. §2705(b).

Publish transparency report. LinkedIn publishes a transparency report.

Publish law enforcement guides. LinkedIn publishes its law enforcement guides.

Fight for users privacy in courts. LinkedIn does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. LinkedIn's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. LinkedIn is member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

Lookout

This is Lookout's first year in the Who Has Your Back report, and it earns 4 stars for a number of practices worthy of commendation. It has strong language requiring a warrant for all content and promises to inform users when their data is sought by the government. While Lookout does not receive credit for fighting for user privacy in the courts, this should not be held against it. Many companies do not have an opportunity to fight in court, or may be barred from discussing those legal challenges publicly.

However, Lookout has not publicly opposed mass surveillance. More and more companies are taking a public stance against bulk surveillance; it is time for Lookout to do the same.

Warrant for content. Lookout requires a warrant before giving data to the government, stating:

> A search warrant issued under the procedures described in the U.S. Federal Rules of Criminal Procedure (or equivalent state criminal procedure laws) is required to compel the disclosure of any account contents.

Inform users about government data demands. Lookout promises to tell users if their data is sought by the government, stating:

> Lookout's policy is to notify users of requests for their information prior to disclosure, except in the following circumstances: where providing notice is prohibited by the legal process, court order, or applicable law; or (a) in emergency cases where notice could create a risk of injury or death to an identifiable individual or group of individuals, or (b) the emergency case involves potential harm to minors. In such cases, we might delay notice to our users.

Publish transparency report. Lookout publishes a transparency report.

Publish law enforcement guides. Lookout publishes its law enforcement guides.

Fight for users privacy in courts. Lookout does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Lookout's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Lookout does not publicly oppose mass surveillance.

Microsoft

Microsoft earns 6 stars in this year's Who Has Your Back report. We are pleased to see Microsoft requiring a warrant before handing user data to the government[19] and publicly opposing mass surveillance. Microsoft is also updating its policies to notify users about government requests for their data. We're pleased to give Microsoft credit for challenging a government data demand in court. And finally, we are particularly impressed by Microsoft's transparency report, which includes a special report about National Security Letters and FISA court orders.

Warrant for content. Microsoft requires a warrant for content, stating:

> We require a court order or warrant before we consider releasing a customer's content data;

Inform users about government data demands. Microsoft has this policy, currently in effect, of informing users about government demands for their data[20]:

> Does Microsoft notify users of its free consumer services, such as Outlook.com, when law enforcement or another governmental entity 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

[19] In 2012, Microsoft searched the content of a Hotmail account on its own, and provided the results to law enforcement. After this came to light, and the subsequent criticism, Microsoft renounced this practice, and promised to refer similar matter to law enforcement, who could obtain a warrant. Read more: https://www.eff.org/deeplinks/2014/03/reforming-terms-service-microsoft-changes-its-policy-access-user-data

[20] Provided by Microsoft to EFF for publication in this report.

by law. We may also withhold notice in emergencies, where notice could result in harm (e.g., child exploitation investigations), or where notice would be counterproductive (e.g., where the user's account has been hacked).

Publish transparency report. Microsoft publishes a transparency report. In addition, it has published a special report providing general information about the FISA orders and National Security Letters it has received, an important step toward transparency that all companies should adopt.

Publish law enforcement guides. Microsoft publishes its law enforcement guides.

Fight for users privacy in courts. Microsoft has publicly challenged a government demand for user data for *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, dated April 25, 2014.[21]

Oppose mass surveillance. Microsoft is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

[21] http://pdfserver.amlaw.com/nlj/microsoft-warrant-sdny.pdf

Myspace

Myspace receives stars in 3 categories this year. We are pleased to see it requires a warrant for content and has a history of fighting for user privacy in courts. However, Myspace lags behind competitors in publishing transparency reports and providing notice to users about government requests for their data. Myspace also has not taken a public stand opposing mass surveillance.

Warrant for content. Myspace requires a warrant for content, stating:

> Myspace requires a search warrant issued under the procedures of the Federal Rules of Criminal Procedure or equivalent state warrant procedures, based upon a showing of probable cause, to compel disclosure of the content of user communications.

Inform users about government data demands. Myspace does not promise to tell users about government data demands.

Publish transparency report. Myspace does not publish a transparency report.

Publish law enforcement guides Myspace publishes its law enforcement guidelines.

Fight for users privacy in courts In 2007, Myspace fought for user privacy in court. It provided EFF with a brief from its legal challenge; we reviewed the case and it meets the standards for this category. Note that our 2011 and 2012 reports did not reflect this case because we did not learn of it until 2013. However, we are now crediting Myspace with a star for every year of our report, since the actual legal challenge was in 2007.

Oppose mass surveillance. Myspace has not publicly opposed mass surveillance.

Pinterest

This is our first year including Pinterest in this report, and we are pleased to recognize its commitments to transparency and user privacy with 5 stars. Pinterest has adopted industry best practices around requiring a warrant for content, providing notice to users about government data requests, releasing transparency reports, and publishing its law enforcement guides. Pinterest has also publicly opposed mass surveillance.

While Pinterest has not earned credit for opposing a government access request in court, this should not be seen as a mark against the company; many companies do not have an opportunity to push back against an overbroad legal request and other companies fight for user privacy but are barred from discussing their efforts publicly.

Warrant for content. Pinterest requires a warrant for content, stating:

> We won't provide any user's content unless you obtain a valid search warrant.

Inform users about government data demands. Pinterest promises to tell users about government demands for their data:

> Yes, we notify users by providing them with a complete copy of the Law Enforcement Request before producing their information to law enforcement, unless prohibited by court order that is issued in accordance with 18 U.S.C. § 2705(b) or applicable statute. The delayed order notice should specify an approximate delayed notice time period (e.g. 180 days).
>
> *Note: Officer authored affidavits, descriptions, cover letters or similar statements are not sufficient to preclude notice to our users. You must provide a court order issued in accordance with 18 U.S.C. § 2705(b) or cite an applicable statute if you wish to prohibit user notice of your Law Enforcement Request. Please contact us if you have any questions regarding this.*

Publish transparency report. Pinterest publishes a transparency report.

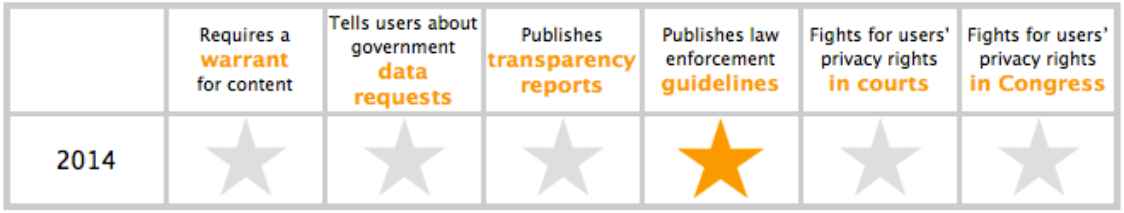
Publish law enforcement guides. Pinterest publishes its law enforcement guidelines.

Fight for users privacy in courts. Pinterest does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Pinterest's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Pinterest publicly opposes mass surveillance, stating:

> Consistent with these law enforcement guidelines, Pinterest requires all requests for user information to be limited to specific and known users for lawful purposes. Pinterest has not and does not participate in the collection of bulk user information at the government's request. Pinterest supports reforms to limit bulk surveillance requests.

Snapchat



Snapchat earns only one star in this year's report, making it one of the lowest scoring companies we reviewed this year. It does not keep pace with industry competitors when it comes to transparency around data requests, giving users notice when their data is sought by the government, or requiring a warrant for user content. Snapchat also does not publicly oppose mass surveillance.

Warrant for content. Snapchat does not require a warrant for content.

Inform users about government data demands. Snapchat does not promise to tell users if their data is sought by the government.

Publish transparency report. Snapchat does not publish a transparency report.

Publish law enforcement guides. Snapchat publishes law enforcement guidelines.

Fight for users privacy in courts. Snapchat does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Snapchat's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Snapchat does not publicly oppose mass surveillance.

Sonic

Since its inclusion in our Who Has Your Back report in 2012, Sonic has received credit in every category we evaluated. This year is no exception: Sonic earns a commendable 6 stars for their strong commitments to transparency and user privacy. Sonic sets a strong example for other ISPs. Sonic earns special accolades for fighting against an overreaching government demand for user data as part of the investigation into WikiLeaks.

Warrant for content. Sonic requires a warrant in order to access content, stating:

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

Inform users about government data demands. Sonic promises to tell users about government demands for data, stating:

> Sonic.net will notify customer of upon receipt for criminal legal process unless confidentiality is specifically required by the order. Please obtain a sealed order if confidential treatment is required.

Publish transparency report. Sonic publishes a transparency report.

Publish law enforcement guides. Sonic publishes its law enforcement guides.

Fight for users privacy in courts. Sonic challenged a government demand in the WikiLeaks investigation.[22]

Oppose mass surveillance. Sonic signed onto a coalition letter that urged the government to "focus intelligence collection on terrorists, spies and other agents of foreign powers, rather than on everyone else." The signers of the letter also stated,

[22] http://online.wsj.com/news/articles/SB10001424052970203476804576613284007315072

"We oppose legislation that codifies sweeping bulk collection activities. We look forward to working with you on the USA FREEDOM Act and other legislation designed to protect the privacy of Internet users while permitting appropriately targeted intelligence surveillance necessary to protect against terrorism."[23]

[23] https://www.cdt.org/files/pdfs/surveillance-sign-on-final-11-21-13.pdf

SpiderOak

SpiderOak earns 5 stars in this year's report. It has demonstrated a strong commitment to transparency around government data requests and respect for its users' privacy. Specifically, SpiderOak requires a warrant for access to content, gives notice to users when their data is sought by the government, publishes a transparency report detailing government data requests, and publishes its law enforcement guides. In addition, it has publicly opposed mass surveillance.

While SpiderOak does not receive a star for fighting for user privacy in courts, this does not reflect badly on the company: Many companies do not have an opportunity to challenge an overbroad government demand or may be barred from discussing their legal challenges.

Warrant for content. SpiderOak requires a warrant for content, stating:

> To obtain non-public information about a SpiderOak user, law enforcement requests must provide valid legal process for the type of information sought (e.g. a subpoena, court order, or warrant). SpiderOak will not disclose any information unless a valid search warrant has been issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause.

Inform users about government data demands. SpiderOak promises to tell users about government data requests, stating:

> SpiderOak's policy is to notify a user of a request for their personal data stored on our servers prior to disclosure unless prohibited from doing so by statute or court order [e.g. U.S.C. § 2705(b)].

Publish transparency report. SpiderOak publishes transparency reports.

Publish law enforcement guides. SpiderOak publishes its law enforcement guidelines.

Fight for users privacy in courts. SpiderOak does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. SpiderOak's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. SpiderOak signed onto a coalition letter that urged the government to "focus intelligence collection on terrorists, spies and other agents of foreign powers, rather than on everyone else." The signers of the letter also stated,

> "We oppose legislation that codifies sweeping bulk collection activities. We look forward to working with you on the USA FREEDOM Act and other legislation designed to protect the privacy of Internet users while permitting appropriately targeted intelligence surveillance necessary to protect against terrorism."[24]

[24] https://www.cdt.org/files/pdfs/surveillance-sign-on-final-11-21-13.pdf

Tumblr

Tumblr earns 5 stars in this year's report, a strong showing. It uses strong language in its policies requiring a warrant before giving content to law enforcement and for informing users about government demands for their data. It has also opposed mass surveillance and published both law enforcement guidelines and a transparency report.

While Tumblr does not receive credit for fighting for user privacy in the courts, this should not be held against it. Many companies do not have an opportunity to fight in court against an overbroad government data demand, or may be barred from discussing those legal challenges publicly.

Warrant for content. Tumblr requires a warrant for content, stating:

> 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.
>
> Requests must come from appropriate government or law enforcement officials; Tumblr will not respond to requests from other sources.

Inform users about government data demands. Tumblr promises to tell users about government data demands, stating:

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

> exploitation of a child, Tumblr may elect not to provide prior user notice. If an investigation involves such an exceptional circumstance, law enforcement should provide a description of the circumstances for us to evaluate.

Publish transparency report. Tumblr publishes a transparency report.

Publish law enforcement guides. Tumblr publishes its law enforcement guides

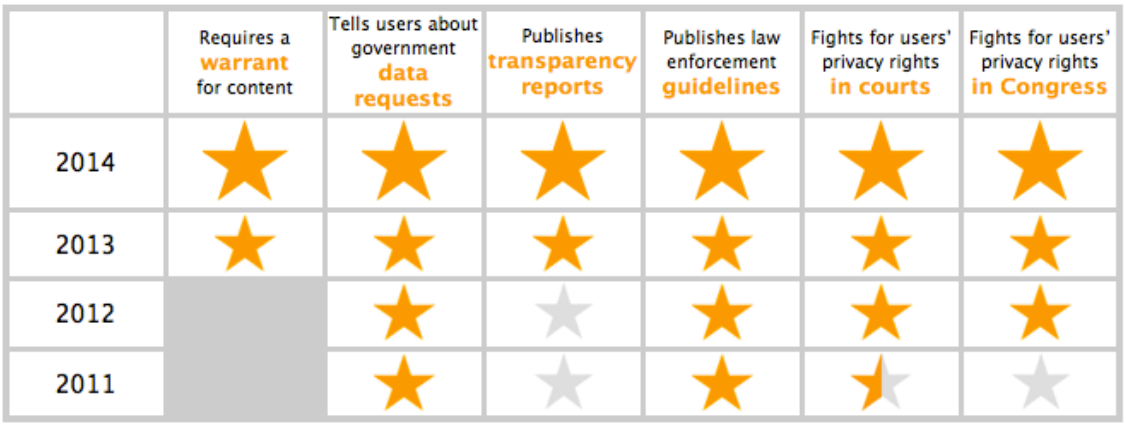
Fight for users privacy in courts. Tumblr does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Tumblr's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Tumblr signed onto a coalition letter that urged the government to "focus intelligence collection on terrorists, spies and other agents of foreign powers, rather than on everyone else." The signers of the letter also stated,

> "We oppose legislation that codifies sweeping bulk collection activities. We look forward to working with you on the USA FREEDOM Act and other legislation designed to protect the privacy of Internet users while permitting appropriately targeted intelligence surveillance necessary to protect against terrorism."[25]

[25] https://www.cdt.org/files/pdfs/surveillance-sign-on-final-11-21-13.pdf

Twitter



Twitter demonstrated its commitment to user privacy and transparency around government data requests, earning a total of 6 stars in this year's report. It uses strong language in its policies requiring a warrant before giving content to law enforcement and for informing users about government demands for their data. It has also opposed mass surveillance and published both law enforcement guidelines and a transparency report.

Warrant for content. Twitter requires a warrant before giving data to the government, stating:

> Requests for the contents of communications (e.g., Tweets, DMs, photos) require a valid U.S. search warrant

Inform users about government data demands. Twitter promises to tell users if their data is sought by the government, stating:

> Will Twitter Notify Users of Requests for Account Information? Yes. Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies; account compromises).

Publish transparency report. Twitter publishes a transparency report.

Publish law enforcement guides. Twitter publishes its law enforcement guides.

Fight for users privacy in courts. Twitter earns a full star this year for standing up for its users in *People v. Harris*.[26] It had previously earned a half-star for standing up for users in relation to the WikiLeaks investigation.

Oppose mass surveillance. Twitter is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

[26] https://www.eff.org/deeplinks/2012/05/twitter-fights-back-against-ny-judges-sweeping-order

Verizon

Verizon earns four stars in this year's report. It showed marked improvement this year, publishing its law enforcement guidelines and transparency report for their first time. Verizon should also be commended for requiring a warrant before handing user content to law enforcement.

Verizon earns its star in opposing mass surveillance for coming out strongly in support of the USA Freedom Act. We're pleased to see this company that has been subject to 215 orders, support the efforts to end bulk surveillance of telephone records.

While Verizon has made remarkable progress in the last year, it has room to improve. In particular, Verizon has yet to adopt a policy of informing users when the government seeks their data. This is the area Verizon should focus on improving in the coming year.

Warrant for content. Verizon requires a warrant for content, stating:

> Stored content refers to communications or other data that our users create and store through our services, such as text messages, email or photographs. We require a warrant before disclosing stored content to law enforcement, absent an emergency involving the danger of death or serious physical injury
>
> Verizon only releases such stored content to law enforcement with a warrant; we do not produce stored content in response to a general order or subpoena. Last year, we received approximately 14,500 warrants for stored content.
>
> As explained above, law enforcement may also present a wiretap order to obtain access to the content of a communication as it is taking place, which they did about 1,500 times last year.

Inform users about government data demands. Verizon does not promise to inform users about government demands for their data.

Publish transparency report. Verizon published its first transparency report this year. In addition, it has published general information about the FISA orders and National Security Letters it has received, an important step toward transparency that all companies should adopt.

Publish law enforcement guides. Verizon publishes its law enforcement guides.

Fight for users privacy in courts. Verizon does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Verizon's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Verizon has publicly opposed mass surveillance through a written statement:

> Verizon supports the bipartisan USA Freedom Act because it will achieve the important goals of ending Section 215 bulk collection of communications data, heightening privacy protections and increasing transparency.

Wickr

Wickr earns five stars in this year's Who Has Your Back report, its first year as part of our review. Wickr gets credit for promising to tell users about government requests for their data, for publishing a transparency report, and for publishing its law enforcement guidelines. Wickr also receives credit for requiring a warrant for content and for publicly opposing mass surveillance.

Warrant for content. Wickr requires a warrant for content, stating:

> Contents of Communications Requires a Search Warrant
>
> Requests for the contents of communications require a valid search warrant from an agency with proper jurisdiction over Wickr.

Inform users about government data demands. Wickr promises to inform users about government data requests, stating:

> If it is legal and possible for us to do so, we will notify you of any request for your information before we preserve or disclose it, so that you have an opportunity to obtain counsel.

Publish transparency report. Wickr publishes a transparency report. Wickr includes information about FISA requests in this report.

Publish law enforcement guides. Wickr publishes its law enforcement guidelines.

Fight for users privacy in courts. Wickr does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Wickr's lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. Wickr is a member of the Stopwatching.us coalition, which states:

> This dragnet surveillance violates the First and Fourth Amendments of the U.S. Constitution, which protect citizens' right to speak and associate anonymously,

guard against unreasonable searches and seizures, and protect their right to privacy. We are calling on Congress to take immediate action to halt this surveillance and provide a full public accounting of the NSA's and the FBI's data collection programs.

Wikimedia

Wikimedia earns four stars in this year's Who Has Your Back report, its first year as part of our review. Wikimedia gets credit for promising to tell users about government requests for their data and for publishing its law enforcement guidelines. Wikimedia also receives credit for requiring a warrant for content. Finally, we are especially pleased to see Wikimedia taking a public stance against mass surveillance.

While Wikimedia has not received credit for publishing a transparency report, it has stated in conversations with us that it plans to publish one this year.

Warrant for content. Wikimedia requires a warrant for content, stating:

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

In a footnote, Wikimedia adds "For the avoidance of doubt, we believe a warrant is required by the 4th Amendment to the United States Constitution, which prohibits unreasonable search and seizure and overrides conflicting provisions in ECPA. We believe that the ECPA needs to be updated so that equivalent protections are granted to electronic communications and documents that have already been granted to the physical documents one keeps at home or in their office. To that end, we are a member of the Digital Due Process Coalition to help in that effort."

Inform users about government data demands. Wikimedia promises to inform users about government data requests, stating:

> When we receive your request, we will notify and provide a copy of your request to the affected user(s) at least 10 calendar days before we disclose the requested information, provided that (1) we have contact information for the affected user(s); (2) disclosing your request will not create or increase a

> credible threat to life or limb; and (3) we are not otherwise prohibited by law or an order from a US court of competent jurisdiction, such as an order issued pursuant to 18 U.S.C. § 2705(b), from doing so.

Publish transparency report. Wikimedia has informed us that it will be publishing its first transparency report in July.

Publish law enforcement guides. Wikimedia publishes its law enforcement guidelines.

Fight for users privacy in courts. Wikimedia does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. Wikimedia's lack of star in this category should not be seen as a demerit

Oppose mass surveillance: Wikimedia publicly opposes mass surveillance. In May 2014, Wikimedia endorsed the 13 International Principles on the Application of Human Rights to Communications Surveillance[27], which posits that any benefits of surveillance of communications must be weighing against the harm that would be caused to individual rights. In announcing its support for these principles, Wikimedia stated[28]:

> Privacy on the Internet is closely connected to our mission to disseminate free knowledge. We strive to provide a platform for users from all over the world to exercise their free expression right to share and study educational content… We want community members to feel comfortable when working on the projects. And we strongly oppose mass surveillance by any government or entity.

[27] https://en.necessaryandproportionate.org/text

[28] http://blog.wikimedia.org/2014/05/09/opposing-mass-surveillance-on-the-internet/

WordPress

WordPress earns 5 stars in this year's report, demonstrating a commitment to transparency around government data requests and a respect for its users' privacy. We are pleased to see WordPress publishing a transparency report, in addition to publishing law enforcement guides, providing notice to users when the government seeks their data, and requiring a warrant for content. WordPress deserves special accolades for their public role in opposing mass surveillance: in addition to signing a coalition letter opposing bulk data collection, WordPress created a plug-in that made it easy for anyone with a WordPress blog to speak out against dragnet spying.

While WordPress does not receive credit for fighting for user privacy in the courts, this should not be held against it. Many companies do not have an opportunity to fight in court against an overbroad government data demand, or may be barred from discussing those legal challenges publicly.

Warrant for content. WordPress requires a warrant for content, stating:

> 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).

Inform users about government data demands. WordPress promises to tell users about government demands for their data:

> 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 requests for private information), unless we are prohibited by law or court order from doing so.

Publish transparency report. WordPress publishes a transparency report. Notably, WordPress includes a special section on nation security requests, which presumably encompass National Security Letters and FISA court orders.

Publish law enforcement guides. WordPress publishes its law enforcement guidelines.

Fight for users privacy in courts. WordPress does not earn credit in this category. However, it should be noted that many companies never have an opportunity to challenge a government data request. Others may fight lengthy legal battles over user privacy but may be legally prevented from ever publicly discussing those efforts. WordPress' lack of star in this category should not be seen as a demerit.

Oppose mass surveillance. WordPress signed onto a coalition letter that urged the government to "focus intelligence collection on terrorists, spies and other agents of foreign powers, rather than on everyone else." The signers of the letter also stated "We oppose legislation that codifies sweeping bulk collection activities. We look forward to working with you on the USA FREEDOM Act and other legislation designed to protect the privacy of Internet users while permitting appropriately targeted intelligence surveillance necessary to protect against terrorism."[29]

[29] https://www.cdt.org/files/pdfs/surveillance-sign-on-final-11-21-13.pdf

Yahoo

Yahoo made big policy changes in the last year, resulting in it earning all six stars in this year's report. Yahoo requires a warrant to access user data, publishes its law enforcement guides and transparency report, and publicly opposes mass surveillance. Yahoo earns particular credit because it has repeatedly fought for user privacy in courts, including a many-year battle in the secret FISC court.

Warrant for content. Yahoo requiring a warrant for content, stating:

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

Inform users about government data demands. Yahoo promises to tell users if the government seeks their data, stating:

> 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.

Publish transparency report. Yahoo publishes a transparency report.

Publish law enforcement guides. Yahoo publishes law enforcement guidelines.

Fight for users privacy in courts. Yahoo has a record of repeatedly challenging government requests for user data. In 2007, Yahoo fought back against an order to produce user data under the Protect America Act, challenging the legality of the order in the Foreign Intelligence Surveillance Court, the secret court that grants

government applications for surveillance. And when the order was upheld by the FISC, Yahoo appealed the decision to the Foreign Intelligence Surveillance Court of Review, a three-judge appellate court established to review decisions of the FISC.[30]

Oppose mass surveillance: Yahoo is a member of the Reform Government Surveillance Coalition, which affirms that "governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."

[30] https://www.eff.org/deeplinks/2013/07/yahoo-fight-for-users-earns-company-special-recognition

References and Helpful Links

Reform Government Surveillance
https://www.reformgovernmentsurveillance.com/

Stopwatching.us
https://optin.stopwatching.us/

Coalition Letter Against Mass Surveillance
https://www.cdt.org/files/pdfs/surveillance-sign-on-final-11-21-13.pdf

Adobe
http://www.adobe.com/legal/compliance/law-enforcement.html

Amazon
http://www.amazon.com/gp/help/customer/display.html/?nodeId=508088
http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496

Apple
https://www.apple.com/legal/more-resources/law-enforcement/
http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf
https://www.apple.com/legal/more-resources/law-enforcement/

AT&T
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/partial-or-no-data-provided.html
http://www.att.com/gen/privacy-policy?pid=13692#collect
http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport/total-u-s--criminal-and-civil-litigation-demands-.html

Comcast
http://xfinity.comcast.net/privacy/2012-04/
http://www.comcast.com/Corporate/Customers/Policies/CustomerPrivacy.html
http://corporate.comcast.com/comcast-voices/comcast-issues-first-transparency-report
http://cdn.comcast.com/~/Media/Files/Legal/Law%20Enforcement%20Handbook/Comcast%20Xfinity%202012%20Law%20Enforcement%20Handbook%20v022112.pdf?vs=1

CREDO Mobile
http://www.credomobile.com/misc/guidelines.aspx
http://www.credomobile.com/misc/transparency.aspx

Dropbox
https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html
https://www.dropbox.com/transparency
https://www.dropbox.com/transparency/principles

Facebook
https://www.facebook.com/safety/groups/law/guidelines/
https://www.facebook.com/about/government_requests
https://www.facebook.com/safety/groups/law/guidelines/

Foursquare
http://support.foursquare.com/attachments/token/i3zateimclhxngy/?name=4sq+Law+Enforcement+Requests.pdf
https://foursquare.com/legal/privacy
https://foursquare.com/legal/terms
http://support.foursquare.com/entries/21508305-Law-Enforcement-Data-Request-Guidelines

Google
https://www.google.com/transparencyreport/userdatarequests/legalprocess/
https://www.google.com/transparencyreport/
http://www.google.com/transparencyreport/userdatarequests/
http://www.google.com/transparencyreport/userdatarequests/US/
http://www.google.com/transparencyreport/removals/government/US/
http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_kinds_of_data

Internet Archive
http://archive.org/about/faqs.php#Law_Enforcement_Requests
http://archive.org/about/faqs.php#1007
http://archive.org/about/faqs.php#1006

LinkedIn
http://help.linkedin.com/ci/fattach/get/2730181/0/filename/LinkedIn%20Law%20Enforcement%20Guidelines.pdf
https://www.linkedin.com/legal/transparency

Lookout
https://www.lookout.com/le-guide
https://www.lookout.com/legal/privacy-policy
https://www.lookout.com/transparency/report-2013

Microsoft
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
http://privacy.microsoft.com/en-us/fullnotice.mspx#EHC
https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/
http://pdfserver.amlaw.com/nlj/microsoft-warrant-sdny.pdf

Myspace
https://www.askmyspace.com/t5/Articles/Law-Enforcement-Guidelines/bap/38505
https://myspace.com/pages/privacy
https://www.askmyspace.com/t5/Articles/Law-Enforcement-Guidelines/bap/38505

Pinterest
http://help.pinterest.com/en/articles/law-enforcement-guidelines
https://help.pinterest.com/en/articles/transparency-report-archive
https://help.pinterest.com/en/articles/transparency-report-archive

Snapchat
http://www.mrcac.org/content/uploads/2013/02/Snapchat_Law_Enforcement_Guide_12112.pdf (leaked)
http://www.snapchat.com/static_files/lawenforcement.pdf

Sonic.net
https://wiki.sonic.net/wiki/Legal_Proccess_Policy
https://wiki.sonic.net/wiki/Legal_Process_Policy#Customer_Notification_Policy
https://corp.sonic.net/ceo/2014/04/28/2013-transparency-report/

SpiderOak
https://spideroak.com/law_enforcement/
https://spideroak.com/privacy_policy
https://spideroak.com/law_enforcement/
https://blog.spideroak.com/20130404171036-increasing-transparency-alongside-privacy-2013-report

Tumblr
http://www.tumblr.com/docs/en/law_enforcement
http://transparency.tumblr.com/

Twitter
http://support.twitter.com/articles/41949-guidelines-for-law-enforcement
https://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/41949-guidelines-for-law-enforcement
https://transparency.twitter.com/

Verizon
http://transparency.verizon.com/us-data
http://www22.verizon.com/about/privacy/policy/
http://transparency.verizon.com/us-data
http://transparency.verizon.com/us-data/national-security
http://publicpolicy.verizon.com/blog/entry/verizon-supports-the-bipartisan-usa-freedom-act

Wikimedia
http://wikimediafoundation.org/wiki/Requests_for_user_information_procedures_%26_guidelines
http://wikimediafoundation.org/wiki/Requests_for_user_information_procedures_%26_guidelines#Notifying_Our_Users_of_Your_Request
http://wikimediafoundation.org/wiki/Requests_for_user_information_procedures_%26_guidelines#Notifying_Our_Users_of_Your_Request
http://blog.wikimedia.org/2014/05/09/opposing-mass-surveillance-on-the-internet/

Wickr
https://www.mywickr.com/en/privacypolicy.php
https://www.mywickr.com/en/downloads/Wickr-Transparency-Report-5.9.2014.pdf
https://www.mywickr.com/en/downloads/Law-Enforcement-Guidelines_5.12.14.pdf

WordPress
http://transparency.automattic.com/legal-guidelines/
http://en.support.WordPress.com/disputes/legal-guidelines/
http://transparency.automattic.com
http://transparency.automattic.com/legal-guidelines/

Yahoo

http://info.yahoo.com/transparency-report/us/law-enforcement-guidelines/
https://transparency.yahoo.com/law-enforcement-guidelines/us/index.html
http://info.yahoo.com/privacy/us/yahoo/details.html
http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html
http://info.yahoo.com/transparency-report/