This is the 2013 report. Be sure to see our most recent report for updated information.

See earlier Who Has Your Back? reports: 2011, 2012

Contents:

Download Report

Download the complete Who Has Your Back? 2013 report as a PDF.

Executive Summary

When you use the Internet, you entrust your conversations, thoughts, experiences, locations, photos, and more to companies like Google, AT&T and Facebook. But what do these companies do when the government demands your private information? Do they stand with you? Do they let you know what's going on?

In this annual report, the Electronic Frontier Foundation examined the policies of major Internet companies — including ISPs, email providers, 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 incentivize companies to be transparent about how data flows to the government and encourage them to take a stand for user privacy whenever it is possible to do so.

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. We also considered the company's public record of fighting for user privacy in the courts and whether it is a member of the Digital Due Process coalition, which encourages Congress to improve outdated communications law. Finally, we contacted each company to explain our findings and gave them an opportunity to provide evidence of improved policies and practices. These categories are not the only ways that a company can stand up for users, of course, but they are important and publicly verifiable. In addition, not every company has faced a decision about whether to stand up for users in the courts, but we wanted to particularly commend those companies who have done so when given with the opportunity.

Evaluation Criteria

This year, we evaluated companies on six criteria. This is a departure from previous years in which we evaluated four criteria but awarded half-stars in two of them.

This year, we divided the "Transparency" category from previous reports into two separate categories. In the past, we've given companies a half-star for publishing a transparency report on how often user data is given to the government and a half-star for publishing law enforcement guidelines on sharing data with the government. This year, we awarded a full star to recognize each of these two best practices.

In addition, we added a new category: requiring a warrant before disclosing contents of user communications to law enforcement. 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 doesn't officially apply to all jurisdictions. This year, we're awarding stars to companies that publicly commit to requiring a warrant when the government seeks user content.

For the 2013 report, we used the following six criteria to assess company practices and policies:

Require a warrant for content of communications. In this new category, companies earn recognition if they require the government to obtain a warrant supported by probable cause before they will hand over the content of user communications. 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.

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. This gives users a chance to defend themselves against overreaching government demands for their data.

Publish transparency reports. We award companies a star in this category if they publish statistics on how often they provide user data to the government.

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

Fight for users' privacy rights in courts. To earn recognition in this category, companies must have a public record of resisting overbroad government demands

for access to user content in court.[1]

Fight for users' privacy in Congress. Internet companies earn a star in this category if they support efforts to modernize electronic privacy laws to defend users in the digital age by joining the Digital Due Process Coalition.

Results Summary: New Industry Trends

We first published this report in 2011 to recognize exemplary corporate practices. We selected practices that at least one service provider was engaging in for each category we measured. Two years later, we're pleased to see that some of the best practices we've been highlighting in this campaign are becoming industry standards.

In particular, we see that more and more Internet companies are formally promising to give users notice of law enforcement requests for their information unless prohibited from doing so by law or court order. This year, the companies earning a star in this category include Dropbox, Foursquare, LinkedIn, Sonic.net, SpiderOak, Twitter, and WordPress. We were disappointed to see Google backslide in this category, introducing ambiguity into its policy and in the process losing the half-star it had earned in previous years.

Annual transparency reports are also becoming a standard practice for major Internet companies. We're thrilled to see a growing number of companies publishing transparency reports, and we especially commend Microsoft and Twitter for publishing their first transparency reports this year. We are also seeing a shift that we hope will be adopted across Internet companies more broadly: two Internet companies — Google and Microsoft — have published figures regarding National Security Letters, secretive government demands for user information that are typically accompanied by gag orders.

We also saw a dramatic increase in the number of companies publishing law enforcement guidelines. Seven companies — Comcast, Foursquare, Google, Microsoft, SpiderOak, Tumblr, and WordPress — earned stars in this category for the first time this year.

In the category of protecting user privacy in the courts, Google deserves special recognition this year for challenging a National Security Letter. Not every company has had the opportunity to defend user privacy in the courts, and sometimes companies will fight for users in court but be prevented from publicly disclosing this fact. However, we award a star in this category when a company goes above and beyond for its users, as Google did this year.

More companies are also fighting for user privacy on Capitol Hill as part of the Digital Due Process Coalition. Foursquare, Tumblr, and WordPress earned stars in this category for the first time in 2013.

We're happy to report that several of the companies included in last year's report have significantly improved their practices and policies concerning government access to user data. Comcast, Google, SpiderOak, and Twitter earned two new stars this year while Microsoft earned three new stars. Foursquare went from zero stars in 2012 to four in 2013.

Blogging platforms Tumblr and WordPress are new to the report this year, but are already making a strong showing. Tumblr earned recognition in three categories: publishing details about how it responds to law enforcement demands, requiring a warrant for content, and standing up for user privacy in Congress. We awarded WordPress stars in each of these categories, too, as well as a fourth star for promising to inform users about government access requests.

This year two companies received all six possible stars: Sonic.net and Twitter. We are extremely pleased to recognize the outstanding commitment each of these companies has made to public transparency around government access to user data.

While we are pleased by the strides these companies have made over the past couple years, there's plenty of room for improvement. Amazon holds huge quantities of information as part of its cloud computing services and retail operations, yet does not promise to inform users when their data is sought by the government, produce annual transparency reports, or publish a law enforcement guide. Facebook has yet to publish a transparency report. Yahoo! has a public record of standing up for user privacy in courts, but it hasn't earned recognition in any of our other categories. Apple and AT&T are members of the Digital Due Process coalition, but don't observe any of the other best practices we're measuring. ~~And this year — as in past years — MySpace and Verizon earned no stars in our report.~~ (Update, May 2, 2013: The report has been amended to grant Myspace two stars. See the full update below.) (Update, May 13, 2013: Myspace has reached out to us again to point us to a case where it pushed back in court against an overbroad government request for user data. We have further amended our report to give Myspace a third star.) We remain disappointed by the overall poor showing of ISPs like AT&T and Verizon in our best practice categories.

New Companies in the 2013 Report

Companies included in last year's report: Amazon, Apple, AT&T, Comcast, Dropbox, Facebook, Foursquare, Google, LinkedIn, Loopt, Microsoft, MySpace, Skype, Sonic.net, SpiderOak, Twitter, Verizon, Yahoo!
New companies added to this year's report: Tumblr, WordPress (Automattic, Inc.)
Companies removed from this year's report: Loopt, Skype (combined with Microsoft)

Our initial 2011 report surveyed the practices of the largest US social networks, ISPs, and email providers. We also included Apple and Skype, as these companies have great quantities of sensitive user data ripe for government access requests. In addition, we allowed the Internet at large to vote on a company to include in our chart, and based on that feedback we added Dropbox.

Last year, we wanted to highlight issues arising from government access to location data and the companies that collect that information. This concern prompted us to add location-based service providers Foursquare and Loopt to our report. This year we removed Loopt because it was acquired by another company and has been integrated into a mobile banking service.

In 2012 we also added cloud storage provider SpiderOak, which like Amazon and Dropbox provides cloud storage. Finally, we included LinkedIn because of their growing role as a social network and Sonic.net because of their courageous and creative efforts to serve as a model of an ISP that stands up for users.

This year, we added Tumblr and WordPress, creators of blogging tools that have been widely adopted by users.

In Depth: Specific Criteria and Changes for 2013

Here's a closer look at each of the categories we used to judge companies' commitment to transparency and user privacy in the face of government access requests and the changes we saw in 2013.

Requiring a Warrant for Content

This category, added for the first time to this report in 2013, was inspired in part by Facebook's requirement that law enforcement obtain a warrant when seeking the content of user communications. In this new category, 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.[2]

This category is inspired by the 2010 decision in United States v. Warshak, a case in which the Sixth Circuit Court of Appeals held that the Fourth Amendment protects emails stored with email service providers, and the government must have a search warrant before it can seize those messages.[3] This decision is a critical victory for Internet privacy, but is the holding of one appeals court — and so is not binding legal precedent throughout the entire country.

We award stars to companies that commit to following the Warshak rule. When companies require a warrant before turning over private messages to law enforcement, they are ensuring that private user communications are treated consistently with the protections of the Fourth Amendment to the Constitution.

Though this is the first year we have evaluated companies in this category, it is clear that many companies require warrants for content. This year, we recognize eleven of the eighteen companies for adopting this policy: Dropbox, Facebook, Foursquare, Google, LinkedIn, Microsoft, Sonic.net, SpiderOak, Tumblr, Twitter, and WordPress.

We are particularly impressed by the firm stance Facebook takes in its understanding of what constitutes user content, which they state publicly includes both semi-public data like wall posts as well as location data. Facebook's policy states:

> 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.

Accessed on April 24, 2013.

Telling Users About Government Data Requests

This category requires a company to make a public promise to let users know when the government comes knocking, unless giving notice is prohibited by law or a court order. This commitment is important because it gives users a chance to defend themselves against 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 should be an easy commitment to make — the company doesn't have to take a side, it merely has to pass on important information to the user. And 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.

Ideally, we think companies should make this promise in their terms of service and privacy policies, although we gave companies credit if they made it in another official way, such as in law enforcement guidelines.

Several leading Internet companies formally promise to give users notice about law enforcement requests for their information unless prohibited by law. This year, Foursquare and WordPress joined the ranks of Dropbox, LinkedIn, Sonic.net, SpiderOak, and Twitter in earning a star.

Unfortunately, we were disappointed to see Google's statement introduce a new ambiguity. In prior years, EFF had recognized Google with a half-star for informally promising to give users notice of law enforcement demands where possible.[4]

However, this year Google stated in an official policy:

> We notify users about legal demands when appropriate, unless prohibited by law or court order.

Accessed on April 24, 2013.

The nebulous language of "when appropriate" is not the firm commitment that should be the gold standard for transparency around handing data to the government. While we're disappointed by Google's decision to make its policy language so open-ended, we hope the strong commitments made by other major Internet companies will inspire Google to adopt a clearer public stance in the years to come.

For example, Twitter's policy, as outlined in its Guide for Law Enforcement, states:

> Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order.

Accessed on April 24, 2013.

Another example of a strong commitment to transparency can be found in LinkedIn's FAQ for users, which states:

> Will LinkedIn notify members of requests for account data?
>
> Yes. 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).

Accessed on April 24, 2013.

Publishing Transparency Reports

In order to earn a gold star in 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 user 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 and continues to publish its Transparency Report.

But we're happy to report that this is now becoming a widespread practice. Last year we recognized Dropbox, LinkedIn, Sonic.net, and SpiderOak as well as Google for their transparency reports. This year, we are adding two more companies to the list: Microsoft and Twitter, both of which are publishing transparency reports for the first time.

Google and Microsoft deserve special recognition for including figures on National Security Letters in their reports.

The FBI's authority to issue secretive National Security Letters was expanded under the PATRIOT Act, allowing the FBI to get telephone, Internet, financial, credit, and other personal records about anybody without court approval as long as it believes the information could be relevant to an authorized terrorism or espionage investigation. 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 coworkers, their friends, or even their family members, much less the public.

Google and Microsoft have helped advance the public's understanding of this dangerous and much-abused government power by publishing general information about the numbers of these orders each has received. While these general reports do not provide exact numbers, they provide a small but vital level of public transparency around this secretive legal instrument.

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 emergency or other kinds of disclosures

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.

Twitter led the way in this category, becoming the first company to receiving recognition in 2011 for publishing its guidelines for law enforcement. Last year, Dropbox, Facebook, LinkedIn, and Sonic.net joined in. And this year, Comcast, Foursquare, Google, Microsoft, SpiderOak, Tumblr, and WordPress all published law enforcement guidelines, as well.

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 filed briefs and made legal arguments defending their users' privacy rights. This is a powerful testimony about a company's commitment to user privacy and their 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, and 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 when it had the chance. 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 to publicly disclose their efforts.

We have recognized the efforts of several companies in defending user privacy in court. Yahoo! earned its star for fighting the Justice Department's attempt to seize a user's email without probable cause, causing the government to back down and withdraw its demand. Amazon's star was for repeatedly fighting to protect the privacy of its users' book purchases in the face of both federal and state government demands. Comcast earned its star for challenging an IRS subpoena[5] on behalf of its users in 2003. Twitter earned a star last year for standing up for its users in the Harris case. And Sonic.net was recognized for challenging a government demand in the WikiLeaks investigation.

Google has now earned a star in this category on multiple occasions, though we examined three specifically:

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 , and

Challenging a National Security Letter.

The importance of Google's challenge to the National Security Letter cannot be understated. These letters are very common, but very few service providers are known to have challenged them in court (EFF has been involved in such challenges before, and currently represents one NSL recipient whose identity remains under seal). Because of the government's demands for secrecy, service providers are simply the only ones who can stand up and push back, and we hope Google's example will inspire others.

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 protect it too, even as technologies change. And the companies that hold our data should stand with users in making the necessary legal updates. That's why the "Who Has Your Back?" campaign urges companies to join the movement working for lasting, permanent improvements in the law — an industry-wide raising of the bar for user privacy — by joining the Digital Due Process coalition (DDP). Members of DDP are working to set legal standards that uphold due process, privacy, and law enforcement effectiveness — like requiring search warrants from the government when it seeks private communications and information, and requiring the government to prove to a court that the data being requested is relevant to actual, authorized law enforcement action.

We are pleased to see that the majority of the companies in our report are members of DDP. This includes seven companies who were members in 2011 (Amazon, Apple, AT&T, Dropbox, Facebook, Google, and Microsoft) as well as four[6] members added in 2012 (LinkedIn, Sonic, SpiderOak, and Twitter). This year, we're pleased to recognize three more companies for their commitment to updating outdate privacy laws: Foursquare, Tumblr, and WordPress (through its parent company, Automattic, Inc.).

Conclusion

There are many ways to safeguard the privacy of individuals from government overreach. EFF has long engaged in impact litigation, educational initiatives, innovative technology projects, and policy advocacy both domestically and internationally to ensure that governments are held to high standards when it comes to accessing sensitive information about us. The foundation of these standards — which ensure our communications and private affairs are not subject to arbitrary government access — are the Fourth Amendment, decades of privacy law, and many years of case law. But in today's increasingly digital world, online service providers serve as the guardians of our most intimate data — from email content to location information to our social and family connections. The policies adopted by these corporations will have deep and lasting ramifications on whether individual Internet users can communicate free from the shadow of government surveillance.

Readers of this year's annual privacy and transparency report should be heartened, as we are, by the improvements major online service providers made over the last year. While there remains room for improvement in areas such as the policies of location service providers and cellphone providers like AT&T and Verizon, certain practices — like publishing law enforcement guidelines and regular transparency reports — are becoming standard industry practice for Internet companies. And we are seeing a growing, powerful movement that comprises civil liberties groups as well as major online service providers to clarify outdated

privacy laws so that there is no question government agents need a court-ordered warrant before accessing sensitive location data, email content, and documents stored in the cloud.

Updates and Corrections

May 2, 2013: Since the publication of our original report, which did not grant Myspace any stars, a representative from the company has notified us about previously published law enforcement guidelines. Because those guidelines are publicly available, and because they require a warrant for the content of communications, we have amended our report to give Myspace the two relevant stars.

May 13, 2013: Myspace has reached out to us again to point us to a case where it pushed back in court against an overbroad government request for user data. We have further amended our report to give Myspace a third star.

Relevant Links

Here are some of the links we used in making our assessments about the companies included in this report. These links were accessed on April 24, 2013.

Amazon

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

http://www.amazon.com/gp/help/customer/display.html/?nodeId=508088

http://www.aclu.org/blog/free-speech-technology-and-liberty/victory-north-carolina-settles-acluamazon-privacy-case

Apple

https://www.apple.com/privacy/

https://www.apple.com/legal/terms/site.html

AT&T

http://www.att.com/gen/privacy-policy?pid=13692#collect

Comcast

http://www.comcast.com/Corporate/Customers/Policies/Policies.html

http://www.comcast.com/Corporate/Customers/Policies/CustomerPrivacy.html

http://www.comcast.com/Corporate/Customers/Policies/HighSpeedInternetAUP.html

http://xfinity.comcast.net/privacy/2013-03/

http://xfinity.comcast.net/privacy/

http://cdn.comcast.com/~/Media/Files/Legal/Law%20Enforcement%20Handbook/Comcast%20Xfinity%202012%20Law%20Enforcement%20Handbook%20v022112.pdvs=1

Dropbox

https://dl.dropbox.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html

https://www.dropbox.com/transparency

Facebook

https://www.facebook.com/full_data_use_policy#inforeceived

https://www.facebook.com/help/473784375984502/

https://www.facebook.com/safety/groups/law/guidelines/

Foursquare

https://foursquare.com/legal/privacy

https://foursquare.com/legal/terms

http://support.foursquare.com/attachments/token/i3zateimclhxngy/?name=4sq+Law+Enforcement+Requests.pdf

Google

http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html

https://support.google.com/a/bin/answer.py?hl=en&answer=107818

http://www.google.com/transparencyreport/governmentrequests/

https://www.google.com/transparencyreport/userdatarequests/legalprocess/

LinkedIn

https://help.linkedin.com/app/answers/detail/a_id/21733

http://help.linkedin.com/app/answers/detail/a_id/16880

http://www.linkedin.com/legal/privacy-policy

http://www.linkedin.com/legal/user-agreement

Microsoft

http://privacy.microsoft.com/en-us/fullnotice.mspx#EHC

https://www.microsoft.com/About/Legal/EN/US/IntellectualProperty/Copyright/default.aspx

https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/#FAQs1

MySpace

https://www.myspace.com/Help/Privacy?pm_cmp=ed_footer

http://myspace.desk.com/customer/portal/articles/526170-law-enforcement-support

Sonic.net

http://corp.sonic.net/ceo/2012/04/13/transparency-report/

https://wiki.sonic.net/wiki/Category:Policies#Privacy

https://wiki.sonic.net/wiki/Legal_Process_Policy

SpiderOak

https://spideroak.com/privacy_policy

https://spideroak.com/blog/20120507010958-increasing-transparency-alongside-privacy

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

https://spideroak.com/law_enforcement/

Twitter

https://twitter.com/privacy

https://twitter.com/tos

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

https://transparency.twitter.com/

Tumblr

http://www.tumblr.com/policy/en/privacy

http://www.tumblr.com/policy/en/terms_of_service

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

Verizon

http://www22.verizon.com/about/privacy/policy/

http://www.verizon.net/policies/vzcom/tos_popup.asp

WordPress

http://en.support.wordpress.com/disputes/legal-guidelines/

Yahoo!

http://info.yahoo.com/privacy/us/yahoo/details.html#3

http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html

https://www.eff.org/deeplinks/2010/04/government-backs-down-yahoo-email-privacy-case

---

A lack of a star in this category shouldn't be considered a demerit—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.

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).

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," Dec, 14, 2010.

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 states, "Google complies with valid legal process. It is Google's policy to notify users before turning over their data whenever possible and legally permissible."

Note: this refers to United States v. Comcast Cable Comm., No. 3-03-0553 (M.D. Tenn. 2003). We do not have link to this case but Comcast provided EFF with a transcript of the hearing, which upon review has met our standards.

Note that last year we also included Loopt, but have subsequently removed them from the annual report. See discussion in the "New Companies in the 2013 Report" section.