



2012: When the Government Comes Knocking, Who Has Your Back?

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

By

Marcia Hofmann, Rainey Reitman, Cindy Cohn

May 31, 2012

ELECTRONIC FRONTIER FOUNDATION
eff.org

Table of Contents

Executive Summary	3
<i>Results Summary</i>	4
2012 Results	6
New Companies in the 2012 Report	7
In Depth: Specific Criteria and the Changes for 2012	8
<i>Promising to Inform Users About Law Enforcement Requests</i>	8
<i>Transparency: Publishing Statistics on Law Enforcement Requests and Law Enforcement Guidelines</i>	9
<i>Defending Privacy in Court</i>	10
<i>Defending Privacy in Congress</i>	11
Conclusion	11
Appendix	12

Authors: Marcia Hofmann, Rainey Reitman, Cindy Cohn

Editor: Parker Higgins

Web formatting assistance: John Ericson

A publication of the Electronic Frontier Foundation, 2012

2012: When the Government Comes Knocking, Who Has Your Back? The Electronic Frontier Foundation's Second Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data is licensed under a [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).



Executive Summary

When you use the Internet, you entrust your online conversations, thoughts, experiences, locations, photos, and more to companies like Google, AT&T and Facebook. But what happens when the government demands that these companies to hand over your private information? Will the company stand with you? Will it tell you that the government is looking for your data so that you can take steps to protect yourself?

The Electronic Frontier Foundation examined the policies of 18 major Internet companies — including email providers, ISPs, cloud storage providers, and social networking sites — to assess whether they publicly commit to standing with users when the government seeks access to user data. We looked at their terms of service, privacy policies, and published law enforcement guides, if any. We also examined their track record of fighting for user privacy in the courts and whether they're members of the Digital Due Process coalition, which works to improve outdated communications law. Finally, we contacted each of the companies with our conclusions and gave them an opportunity to respond and provide us 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.

While some Internet companies have stepped up for users in particular situations, it's time for all companies that hold private user data to make public commitments to defend their users against government overreach. The purpose of this report is to incentivize companies to be transparent about what data flows to the government and encourage them to take a stand for user privacy when it is possible to do so.

We evaluated each company based on the following criteria:

1. **A public commitment to inform users when their data is sought by the government.**

To earn a star in this category, Internet companies must promise to tell users when their data is being sought by the government unless prohibited by law. This gives users a chance to defend themselves against overreaching government demands for their data.

2. **Transparency about when and how often companies hand data to the government.**

This category has two parts. Companies earn a half-star in this category if they publish statistics on how often they provide user data to governments worldwide. Companies also earn a half-star if they make public any policies they have about sharing data with the government, such as guides for law enforcement. (If a company doesn't have law enforcement guidelines at all, though, we don't hold

that against them). Companies that publish both statistics and law enforcement guidelines receive a full star.

3. **Fight for users' privacy rights in the 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. 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.

4. **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

We are pleased to see that service providers across the board are increasingly adopting the best practices we've been highlighting in this campaign. We first published this report last year to recognize exemplary practices that at least one service provider was engaging in for each category we measured. This year, it appears that publishing law enforcement guidelines, formally promising to give users notice when possible, and publishing transparency reports are on their way to becoming standard practices for industry leaders, and several more service providers are pushing for privacy protections in the courts and on Capitol Hill.

We're also happy to report that several of the companies included in last year's report have stepped up their game. Facebook, Dropbox and Twitter have each upgraded their practices in the past year and earned additional stars. Comcast drew our attention to a case in which they went to bat for user privacy, and so it earned a star, too.

Some of the new companies we've added to the report are neck-and-neck with the competition. LinkedIn and SpiderOak, like Dropbox, have each earned recognition in three categories: promising to inform users about government access requests, transparency about how and when data goes to the government, and standing up for user privacy in Congress. None of them has a publicly available record of standing up in court for users. However, that's not something that all companies have had the opportunity to do, and sometimes companies will defend users in court but be prevented from publicly disclosing this fact.

We are especially pleased to recognize the first company to ever receive a full gold star in each of the categories measured by the privacy and transparency report: Sonic.net, an ISP based in Santa Rosa, California.

While we've been extremely impressed by the strides some of these companies have made since last year, there's plenty of room for improvement. We're hopeful that next year we'll see more protections for users from location services providers like Loopt and Foursquare, since location information is so sensitive and increasingly sought by the government. In addition, Amazon is entrusted with huge quantities of information as part of its cloud computing services and retail operations, yet does not produce annual transparency reports, publish a law enforcement guide, or promise to inform users when their data is sought by the government. We were pleased that Comcast and Yahoo! stood up for user privacy in courts, but neither company has hit any of the other criteria for earning recognition in our other categories. AT&T, Microsoft, and Apple 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 last, Verizon and MySpace earned no stars in our report. The overall poor showing of AT&T, Verizon and Comcast, who provide Internet connectivity to so many people, is especially troubling.

2012 Results

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

New Companies in the 2012 Report

Companies included in last year's report: Amazon, Apple, AT&T, Comcast, Dropbox, Facebook, Google, Microsoft, MySpace, Skype, Twitter, Verizon, Yahoo!

New companies added to this year's report: Spider Oak, Sonic.net, Loopt, Foursquare, LinkedIn

Last year, our report covered the largest US social networks, ISPs, and email providers. We also included Skype and Apple, as these companies have great quantities of sensitive user data that could prove ripe for government access requests. We also allowed the Internet at large to vote on a company worth including in our chart, and based on that feedback we added Dropbox.

This year, we wanted to highlight issues arising from government access to location data and the companies that collect that information. Especially as web-enabled smartphones and tablets become more prevalent, location data reveals an [incredibly intimate portrait](#) of users' every move and that information can be gathered and kept for a very long time. This concern prompted us to add location-based service providers Loopt and Foursquare to our report this year. We were disappointed to learn their practices don't stack up — Loopt received only one star (as a member of the Digital Due Process Coalition) and Foursquare received no stars at all.

We hope that next year Loopt and Foursquare will take steps to improve their practices, given the sensitivity of location information. We have seen myriad examples of the government seeking access to sensitive user location data without proper judicial oversight. Location information [appeared](#) to be the target of the government's demand that Twitter turn over user data in the Wikileaks investigation. And location data may be the motivating factor behind a [government subpoena](#) for the Twitter account information of Occupy Wall Street protester Malcolm Harris (a subpoena we are happy to see Twitter is [resisting](#)).

EFF has long championed location privacy in the courts. In 2011 we submitted an amicus brief in [US v Jones](#), a case in which the US Supreme Court unanimously confirmed that Americans have constitutional protections against warrantless GPS surveillance by law enforcement. While this set a strong legal precedent for protecting individual privacy against GPS tracking, third party service providers like Loopt and Foursquare might prove to be a [weak link](#) the government can pressure for access to user location information. There is no question that law enforcement is eagerly accessing location information from third-party providers for a wide range of investigations. It's vital these providers commit to being transparent about government access requests and fighting those requests when they are overbroad.

In addition to location-based services, we added cloud storage provider SpiderOak to the report this year to join Dropbox and companies like Amazon that provide cloud storage as part of a suite of services.

We also added 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.

Sonic.net and SpiderOak specifically asked to be included in our report. We encourage other service providers who have a commitment to stand up for their users to let us know if they would like us to consider them for future reports. We also encourage service providers to suggest other, publicly verifiable criteria we could add.

In Depth: Specific Criteria and the Changes for 2012

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 2012.

Promising to Inform Users About Law Enforcement 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 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, she 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, 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. In our 2011 report, Twitter received a full star for making this promise in its law enforcement guidelines. We gave half a star to Google since its commitment was made only in a blog post and a difficult-to-find FAQ.

2012

Dropbox, LinkedIn, Sonic.net and SpiderOak have now joined Twitter in promising to notify their users when possible about government attempts to seek information about them. Google continues to get its half star because it hasn't made this commitment in a formal policy. This brings the total to over five companies that have committed to giving

you the opportunity to defend yourself against government attempts to get access to your information when they can. That's very good news.

For example, LinkedIn's [FAQ](#) for users says:

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 5/22/12 from [http://help.linkedin.com/ci/fattach/get/1568450/0/filename/LinkedIn Law Enforcement Data Request Guidelines.pdf](http://help.linkedin.com/ci/fattach/get/1568450/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf)

SpiderOak has a similarly short and strong [policy](#):

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)].

Accessed on 5/22/12 from https://spideroak.com/privacy_policy

Sonic's [policy](#) is similarly strong and clear:

Customer Notification Policy

For civil legal process - It is Sonic.net's policy to notify customers upon receipt of a civil subpoena demand of their account information. There is a two week wait period before disclosure of information.

Sonic.net will advise the customer that the information will be disclosed unless Sonic.net is in receipt of a document seeking a court approved protective order prior to the date on which Sonic.net must legally comply with the demand.

[...]

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

Accessed on 5/22/12 from https://wiki.sonic.net/wiki/Legal_Process_Policy

Transparency: Publishing Statistics on Law Enforcement Requests and Law Enforcement Guidelines

We're asking companies to do two things in order to earn a gold star in the transparency

category: provide reports on how often they provide data to the government and publish their law enforcement guidelines. Users make decisions every day about which companies they will entrust with their data. It's vital that companies are forthcoming about how often and through what process they hand user data to the government.

First, EFF is measuring 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 several other service providers have done the same and earned a half-star. These are Sonic.net, SpiderOak, LinkedIn, and Dropbox.

Second, we are tracking which companies publish their guidelines for law enforcement requests for user data, giving a half-star for this. Twitter led the way in this category, receiving a half-star in 2011. Importantly, we must note that many companies do not have written law enforcement guidelines. While we are pleased that companies that do have them are publishing them, we want to be clear that the lack of a half-star for those who don't have them, specifically Google and SpiderOak, should not be interpreted as a lack of transparency on their part.

We are pleased to note that [Facebook](#), [Dropbox](#), [Sonic.net](#), and [LinkedIn](#) published their law enforcement guidelines for the first time in 2012. We thus have five major service providers making clear to their users what standards and rules law enforcement must follow when they seek access to sensitive user data. This is good progress.

Defending Privacy in Court

Companies can 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, and that others may be bound by the secrecy of gag orders in national security letters, 2703(d) orders or other processes, leaving them unable to disclose the efforts they have made for their users. 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 those companies who were faced with a need to defend user privacy in court, took action to defend that privacy, and then were legally allowed to publicly disclose their efforts.

With that caveat, we are pleased to award new stars this year to three companies:

Comcast, which informed us that it challenged an IRS subpoena¹ on behalf of its users in 2003; Twitter, which earned a full star this year for standing up for its users in the [Harris case](#); and Sonic.net, for its efforts to challenge a government demand last year in the [Wikileaks investigation](#). Google, which already had a star in this category last year, also deserves special credit for going to bat for a user whose information was sought in the Wikileaks investigation.

Last year we awarded Yahoo! and Amazon and Google stars in this category. Yahoo! earned its star for fighting the Justice Department's attempt to [seize a Yahoo! user's email](#) without probable cause, causing the government to [back down](#) and withdraw its demand. Google's star was in recognition of several cases, including [resisting a Justice Department subpoena for search logs](#) in 2006. 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.

Defending Privacy in Congress

While company policies are important, we shouldn't be dependent on just company policies 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 take steps like joining in the effort toward 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 member in 2011 (Amazon, Apple, AT&T, Dropbox, Facebook, Google, and Microsoft) as well as five new members in 2012 (LinkedIn, Sonic, Loopt, Twitter, and SpiderOak).

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

¹ 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.

ensure that government are held to high standards when it comes to accessing sensitive information about us. These high standards — which ensure our communications and private affairs are not subject to arbitrary government access — are the foundation of 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 graph. 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, at the improvements major online service providers over the last year. While there remains room for improvement in areas such as the policies of location service providers, certain practices — like publishing law enforcement guidelines and regular transparency reports — are becoming standard industry practice. 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.

Appendix

2011 Results

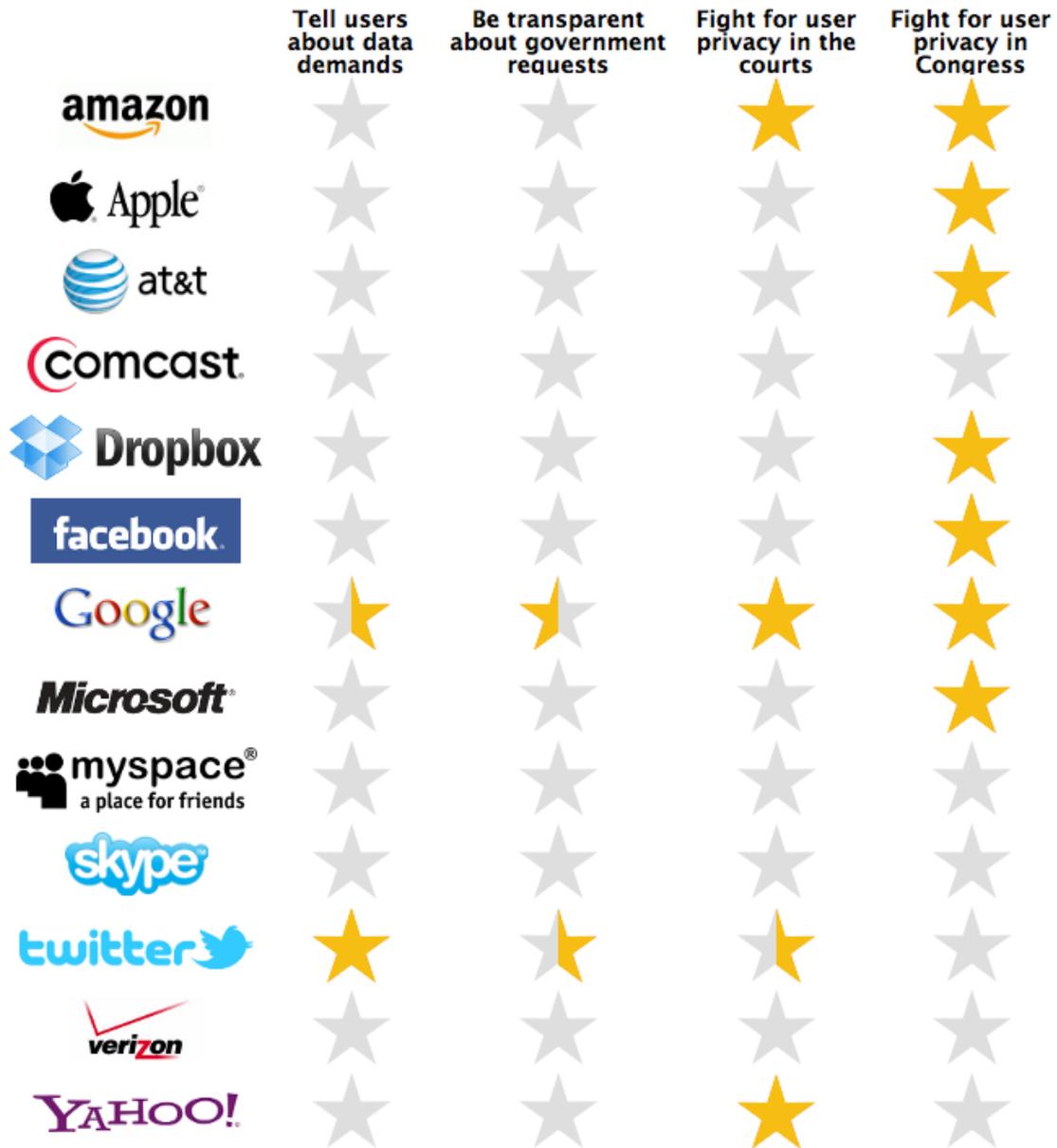


Chart available [here](#).

Relevant Links

Here are some of the links we used in making our assessments about a company's status. These links were accessed on May 22, 2012:

Amazon

http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496
<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://xfinity.comcast.net/privacy/2011-03/>
<http://comcast.com/corporate/legal/privacyStatement.html>
<http://www.comcast.com/Corporate/Customers/Policies/HighSpeedInternetAUP.html>

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/?page=211462112226850>
<https://www.facebook.com/safety/groups/law/guidelines/>

Foursquare

<https://foursquare.com/legal/privacy>
<https://foursquare.com/legal/terms>

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/>

LinkedIn <http://help.linkedin.com/ci/fattach/get/1568450/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf>

Loopt

<https://www.loopt.com/legal/PrivacyNotice>

Microsoft

<http://privacy.microsoft.com/en-us/fullnotice.msp#EHC>

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

MySpace

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

Skype

<http://www.skype.com/intl/en-us/legal/privacy/general/#3>

Sonic.net

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

<http://corp.sonic.net/ceo/wp-content/uploads/2012/04/Sonic.net-Legal-Process-Policy-2012.pdf>

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

SpiderOak

https://spideroak.com/privacy_policy

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

Twitter

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

<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>

Verizon

<http://www2.verizon.com/about/privacy/policy/>

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

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>