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

Nate Cardozo, Kurt Opsahl, Rainey Reitman

May 5, 2016
Table of Contents

Executive Summary ................................................................................................................. 4
   How Well Does the Gig Economy Protect the Privacy of Users?................................. 4
   Initial Trends Across Sharing Economy Policies ........................................................... 6

Chart of Results ......................................................................................................................... 8

Our Criteria ................................................................................................................................. 9
   1. Require a warrant for content of communications............................................. 9
   2. Require a warrant for prospective location data.............................................. 9
   3. Publish transparency reports ........................................................................ 10
   4. Publish law enforcement guidelines ............................................................... 10
   5. Notify users about government data requests ............................................... 10
   6. Fight for user privacy in Congress as a member of the Digital Due Process Coalition ............................................................................................................ 11

Company Results ....................................................................................................................... 12
   Airbnb ................................................................................................................................. 12
   FlipKey .............................................................................................................................. 14
   Getaround ............................................................................................................................ 16
   Instacart ............................................................................................................................... 18
   Lyft .................................................................................................................................... 19
   Postmates ............................................................................................................................. 21
   TaskRabbit ......................................................................................................................... 22
   Turo ................................................................................................................................... 23
   Uber ................................................................................................................................... 24
   VRBO ................................................................................................................................ 26

Links and Additional Resources .............................................................................................. 27

Results From Previous Reports ............................................................................................... 28
   2015 ................................................................................................................................. 28
   2014 ................................................................................................................................. 29
   2013 ................................................................................................................................. 30
   2012 ................................................................................................................................. 31
   2011 ................................................................................................................................. 32

Authors: Nate Cardozo, Kurt Opsahl, Rainey Reitman
Editors: Parker Higgins, Dave Maass
Formatting: Parker Higgins


Who Has Your Back 2016 is released under a Creative Commons Attribution 3.0 License.
Executive Summary

How Well Does the Gig Economy Protect the Privacy of Users?

The last several years have seen a boom in what many call the “sharing” or “gig” economy.¹

These companies connect users offering services to other users interested in purchasing those services. Uber and Lyft help passengers find folks with a car to drive them around, creating a distributed taxi-like service. TaskRabbit helps users find a helpful stranger to do anything from yard work to standing in line. Airbnb, FlipKey, and VRBO let users rent out their homes. All of these companies and many more act as virtual middlemen, connecting sellers of services to buyers.

These companies also collect sensitive information about the habits of millions of people across the United States. Details about what consumers buy, where they sleep, and where they travel are really just scratching the surface of this data trove. These apps may also obtain detailed records of where your cell phone is at a given time, when you are logged on or active in an app, and with whom you communicate.

It’s not just the purchasers in the gig economy who have to trust their data to the startups developing these apps. Individuals offering services are users just like the buyers, and also leave behind a digital trail as (or more) detailed than that of the purchasers. From Lyft drivers to Airbnb hosts to Instacart shoppers, people providing services are entrusting enormous amounts of data to these apps. The sharing economy companies collect the contents of communications, geolocation information, and may also have identifying information like one’s phone number, home address, and associated Facebook profile.

As with any rich trove of data, law enforcement is increasingly turning to the distributed workforce as part of their investigations. That’s not necessarily a bad thing, but we need to know how and when these companies actually stand up for user privacy, and when do they simply act as vehicles for government access?

Over the last six years, the Electronic Frontier Foundation has published Who Has Your Back, an annual overview of the public policies and practices of major technology and communications companies in response to law enforcement requests. We’ve followed social networking sites, email providers, ISPs, cloud storage providers, and other companies. The report has been an unqualified success: whereas no company achieved

¹ There are a wide range of terms for this market force, including the sharing economy, the gig economy, the 1099 economy, the collaborative economy, the on-demand economy, the matching economy, and collaborative consumption. We don’t have a position on what the most appropriate term is and may use these words interchangeably. Learn more about terms and stats related to the gig economy: https://newsletters.briefs.bloomberg.com/document/4yz1acbgrfxz8uwan9/the-workers-demographics
credit in every category the first year we launched, more than half of the companies achieved credit in 4 or more of our 5 categories by last year, and 23 of 24 followed industry best practices. Transparency reports, law enforcement guidelines, a policy of providing notice to users about law enforcement requests, and requiring a warrant for content were rare in 2011, and have all become industry standard practices. Thanks to these efforts, the digital world is more secure against government overreach.

Given that most of the companies we’ve been tracking over the years have improved their practices to meet our standards, we recognize that this report has successfully incentivized the change we were looking for. That’s why this year we are dropping all of our traditional companies from the report and bringing in a new slate of tech companies.

This year, the focus of our report is sharing economy companies. These relatively young companies have quickly infiltrated our daily lives, impacting how Americans shop, drive, and travel. But even as these companies are increasing in popularity, questions remain as to whether this developing industry is keeping pace with the rest of the technology sector on user privacy concerns. When the government comes knocking, will these companies stand for transparency and privacy?

Findings: Sharing Economy Companies Lag in Adopting Best Practices for Safeguarding User Privacy

Many sharing economy companies have not yet stepped up to meet accepted tech industry best practices related to privacy and transparency, according to our analysis of their published policies. This analysis is specific to government access requests for user data, and within that context we see ample room for improvement by this budding industry. Users are the core of these companies, as both the providers and consumers of the companies’ business. Yet, when the government comes knocking, most gig economy companies—whether home rental services, car sharing, or on-demand labor—aren’t promising to stand by their users.

There are, however, some gig economy companies leading the field on this issue.

We analyzed 10 companies as part of this report. Of them, both Uber and Lyft earned credit in all of the categories we examined. We commend these two companies for their transparency around government access requests, commitments to protecting Fourth Amendment rights in relation to user communications and location data, advocacy on the federal level for user privacy, and commitment to providing users with notice about law enforcement requests. These two companies are setting a strong example for other distributed workforce companies. It’s clear that Lyft and Uber are competing on privacy and transparency. In contrast, another ride-sharing company, Getaround, received no stars in this year’s report.

Other sharing economy companies have taken steps to stand up for user privacy. In particular, FlipKey (owned by TripAdvisor) has adopted several policies related to

---

2 A thorough explanation of our criteria is available directly following the chart.
government access of user data. FlipKey requires a warrant for user content or location data and promises to inform users of law enforcement access requests. It is also a member of the Digital Due Process Coalition, fighting for reform to outdated communications privacy law. Of the home sharing companies we reviewed, FlipKey does the most to stand up for user privacy against government demands.

Only two other companies from our research set earned credit in any categories: Airbnb and Instacart, each earning credit in three categories. Both of these companies require a warrant for content, publish law enforcement guidelines, and are members of the Digital Due Process Coalition. We were encouraged by their efforts to adopt policies safeguarding user data, and we look forward to improvement over the next year.

Fully half of the companies we reviewed—Getaround, Postmates, TaskRabbit, Turo, and VRBO—received no credit in any of our categories. This finding is disappointing, but we’re optimistic that these companies will take our report as a wake-up call and step up to stand behind their users.

**Initial Trends Across Sharing Economy Policies**

Industry-wide, we can see some initial trends. First, it is clear that while some sharing economy companies have prioritized standing up for user privacy in the face of government demands, many have not. On the whole, the gig economy just hasn’t caught up with the rest of the tech industry in safeguarding user data against unwarranted government access demands.

Of the categories we evaluated, more companies earned credit for membership in the Digital Due Process Coalition than for any other category. This may indicate a strong interest from these younger tech companies in joining with a broad set of tech companies and non-profit organizations to update the laws that impact email privacy, cloud data storage, and geolocation data. This policy position is in alignment with what we see now in Congress: the House of Representatives unanimously passed the Email Privacy Act in April, seeking to update the law to better protect email privacy.

On the other side of the spectrum, most of the companies we analyzed were not yet publishing transparency reports. Only two companies in the field—Lyft and Uber—have published reports outlining how many law enforcement access requests they’ve received. As a result, the general public has little insight into how often the government is pressuring gig economy companies for access to user data. This concerns us, as one way to make surveillance without due process worse is to allow it to happen entirely in secret. Publicizing reports of law enforcement access requests can help illuminate patterns of overzealous policing, shine a light on efforts by companies to resist overbroad requests, and perhaps give pause to law enforcement officials who might otherwise seek to grab more user data than they need for an investigation. We sincerely hope that next year’s Who Has Your Back report shows a general movement in the gig economy toward publishing transparency reports.
We recognize that shifts in industry momentum can take time. It took several years before we saw changes in the policies of tech giants in response to our annual Who Has Your Back report. We hope that next year’s report will find more of these companies adopting these best practices and standing by their users.

In the meantime, we commend companies like Lyft, Uber, and FlipKey for leading the sharing economy on privacy and transparency, and appreciate Airbnb and Instacart for taking steps to stand with their users.
# Chart of Results

<table>
<thead>
<tr>
<th></th>
<th>Requires warrant for user content</th>
<th>Requires warrant for prospective location</th>
<th>Issues a public transparency report</th>
<th>Issues public law enforcement guidelines</th>
<th>Tells users about government data demands</th>
<th>Stand up for user privacy in Congress</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Airbnb logo]</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>![Carrot logo]</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>✔</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>![Lyft logo]</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>![Turo logo]</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>![VRBO logo]</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
</tbody>
</table>

[Links to the Electronic Frontier Foundation (EFF)](https://www.eff.org)
Our Criteria

Consumers should be able to understand their privacy rights by reading the policies of the companies that hold their data. As such, this report only takes into account evidence of company practices that are official and publicly viewable online. A company can only earn credit for our warrant for content, warrant for location data, and user notification categories by making commitments in a privacy policy, terms of service, law enforcement guidelines, or a similarly public, official document. Promises or assurances from companies made directly to EFF or in any private context are not a factor in whether a company receives stars in this report, nor are news articles published by third parties or unofficial remarks over social media. In order to earn credit for defending user privacy in Congress, the company must be listed on its own behalf as a coalition member on the Digital Due Process website.3

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 law enforcement to obtain a search warrant before they will hand over the content of user communications to law enforcement. Because in U.S. law a search warrant must be issued by a neutral magistrate and supported by probable cause, this policy ensures that private messages stored by online services are treated consistently with the protections of the Fourth Amendment to the U.S. Constitution. In 2010, the Sixth Circuit Court of Appeals held in United States v. Warshak4 that the Fourth Amendment 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.5 However, companies in any circuit can uphold Fourth Amendment rights for their users by requiring a warrant before disclosing the content of user communications.

2. Require a warrant for prospective location data

In this category, companies earn recognition if they require law enforcement to obtain a warrant before they provide prospective location data to the government. When a company provides prospective location data to the government, it agrees to inform the government about GPS or similar location data it will collect on a user or users going

3  https://digitaldueprocess.org
4  Read more about this case: https://www.eff.org/cases/warshak-v-united-sta
5  On April 27, 2016, the House of Representatives passed the Email Privacy Act, which would codify Warshak for all jurisdictions. https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform
forward. For example, law enforcement may ask for the company to reveal whenever a user’s app detects GPS coordinates. Given the sensitivity of location information and recent court rulings\(^6\) that support warrants for certain types of location data, many companies are requiring a warrant for prospective location data to ensure location information is treated consistently with the Fourth Amendment.

3. **Publish transparency reports**

We award companies a star in this category if they publish useful data about how many times the government sought user data and how often the companies provide user data to the government. Until recently, companies were not allowed to include national security requests in transparency reports at all. National security transparency reporting is still strictly limited by statute, but the government has recently allowed companies to provide limited transparency about those types of requests. It is a best practice for companies to include all demands that can be disclosed under the law, including data about national security requests.

4. **Publish law enforcement guidelines**

Companies earn credit in this category if they publish policies or guidelines explaining how they respond to data demands from law enforcement. Through these guidelines, a company can explain what types of data it will provide under which legal process. Guidelines help the users understand what information is available to law enforcement and its protections, while also helping law enforcement keep requests narrow and targeted.

5. **Notify users about government data requests**

To earn a star in this category, companies must promise to tell users when the government seeks their data unless prohibited by law, in very narrow and defined emergency situations\(^7\), or unless doing so would be futile or ineffective.\(^8\) 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 also recognize that prior notice is not always possible, for instance in emergency situations.

---

\(^6\) For an overview of some of the court decisions and ongoing battles related to location data, visit [https://www.eff.org/deeplinks/2015/06/california-new-york-cell-phone-location-records-are-private](https://www.eff.org/deeplinks/2015/06/california-new-york-cell-phone-location-records-are-private)

\(^7\) The exceptions should not be broader than the emergency exceptions provided in the Electronic Communications Privacy Act, 18 U.S.C. § 2702 (b)(8).

\(^8\) An example of a futile scenario would be if a user’s account has been compromised or hijacked (or their mobile device stolen) and informing the “user” would concurrently—or only—inform the attacker.
6. Fight for user privacy in Congress as a member of the Digital Due Process Coalition

Every year, we look for companies to earn credit in this category by taking a specific pro-user public policy position or joining a coalition in support of privacy-protective policies.

This year, we are recognizing companies that are members of the Digital Due Process Coalition. The Digital Due Process Coalition advocates for stronger privacy protections for communications and associated data in response to changes in technology, primarily through reform of the Electronic Communications Privacy Act. DDP stands for four principles:

1. Requiring a warrant for user content;
2. Requiring a warrant for mobile device location information;
3. Requiring a warrant for prospective communications metadata that shows who’s calling whom or who’s messaging whom; and
4. Requiring that subpoenas for information are only used to gather information on specific accounts or individuals, not in bulk.
Company Results

Airbnb

Internet-based peer-to-peer home sharing service.

Airbnb earns three stars in this year’s *Who Has Your Back* report. While there is room for improvement, we commend Airbnb for taking initial steps to facilitate transparency and user privacy. In particular, Airbnb earns credit for requiring a warrant for content, publishing law enforcement guidelines, and being a member of the Digital Due Process Coalition. Going forward, we encourage Airbnb to require a warrant for prospective location data, publish transparency reports, and provide users notice when their data is sought by law enforcement.

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

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

**Warrant for prospective location data.** Airbnb does not state that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** Airbnb does not have a published transparency report.

**Law enforcement guidelines.** Airbnb publishes guidelines explaining its standards for providing user information to law enforcement, available here:


**Inform users about law enforcement data requests.** Airbnb does not promise to provide users with notice about law enforcement requests. It states in its law enforcement guidelines that it will generally do so, but provides an overly broad exception for any instance which would “create or increase risk of fraud upon Airbnb’s property, its Members, the Platform, Applications, or Services.” From its privacy policy:

> We will use commercially reasonable efforts to notify users about law enforcement requests for their data unless:
providing notice is prohibited by the legal process itself, by court order we receive, or by applicable law; or we believe that providing notice would (a) be futile, (b) be ineffective, or (c) would create a risk of injury or bodily harm to an individual or group, or (d) create or increase a risk of fraud upon Airbnb’s property, its Members, the Platform, Application, or Services (collectively, “Risk Scenarios”).

In instances where Airbnb complies with legal requests for user data without notice to the user for the reasons described above, Airbnb will use commercially reasonable efforts to notify that user about the request after the fact if we determine in good faith that we are no longer legally prohibited from doing so and that no Risk Scenarios apply.

**Digital Due Process Member.** Airbnb stands up for user privacy in Congress as a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company and briefed them on our findings prior to publication.
FlipKey

Internet-based peer-to-peer vacation rental service.

FlipKey earns four stars in this year’s *Who Has Your Back* report. While there is room for improvement, we commend FlipKey for taking many steps to facilitate transparency and user privacy. In particular, FlipKey earns credit for requiring a warrant for content and location data, notifying users when their data is sought by law enforcement, and being a member of the Digital Due Process Coalition. Going forward, we encourage FlipKey to publish transparency reports and a law enforcement guide.

**Warrant for content.** FlipKey does require a warrant before giving content to law enforcement. According to their terms of service:

> Typically, we require 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 to compel our disclosure of certain communications between people using FlipKey or precise location information. We make exceptions to these requirements for emergency and exigent requests, where a user has provided consent, or - for requests that do not require a warrant - where other legal or regulatory standards apply.

**Warrant for prospective location data.** FlipKey states that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** FlipKey does not have a published transparency report.

**Law enforcement guidelines.** FlipKey does not publish guidelines explaining its standards for providing user information to law enforcement.

**Inform users about law enforcement data requests.** FlipKey promises to provide users with notice about law enforcement requests. According to its terms of service:

> If we are required by law to disclose personal information submitted by a user, we will attempt to provide such user with notice (unless we are prohibited or it would be futile) that a request for information has been made in order to give the user an opportunity to object to the disclosure. We will attempt to provide this notice by email, an email address was given, or by postal mail if we have a postal address. If you do not challenge the disclosure request, we may be legally required to turn over your information.
Digital Due Process Member. FlipKey stands up for user privacy in Congress by being a member of the Digital Due Process Coalition.

Interactions with company. We contacted the company and briefed them on our findings prior to publication.
Getaround

Peer-to-peer car sharing and local car rental.

Getaround earns zero stars in this year’s *Who Has Your Back* report. In particular, Getaround does not require a warrant for content or prospective location data, does not publish a transparency report, does not publish law enforcement guidelines, does not provide notice to users when their data is sought by law enforcement, and is not a member of the Digital Due Process Coalition.

**Warrant for content.** Getaround does not require a warrant before giving content to law enforcement, stating in its privacy policy:

> Except as otherwise described in this Privacy Policy, Getaround will not disclose personal information to any third party unless required to do so by law or subpoena or if we believe that such action is necessary to (a) conform to the law, comply with legal process served on us or our affiliates, or investigate, prevent, or take action regarding suspected or actual illegal activities; (b) to enforce our Terms of Service, take precautions against liability, to investigate and defend ourselves against any third-party claims or allegations, to assist government enforcement agencies, or to protect the security or integrity of our site; and (c) to exercise or protect the rights, property, or personal safety of Getaround, our Users or others.

**Warrant for prospective location data.** Getaround does not state that it requires a warrant before providing prospective location data to law enforcement. Its privacy policy states:

> We monitor all cars to prevent theft, and to allow us to locate you in case of accident, emergency, lock-out, etc. Your location information will only be used in direct relation to Getaround business, and may be released to insurance companies, the police, or similar parties in the due course of investigating and processing accident claims, and providing you with help in the case of an emergency or lock-out.

**Transparency report.** Getaround does not have a published transparency report.
Law enforcement guidelines. Get around does not publish guidelines explaining its standards for providing user information to law enforcement.

Inform users about law enforcement data requests. Getaround does not promise to provide users with notice about law enforcement requests.

Digital Due Process Member. Getaround does not stand up for user privacy in Congress by being a member of the Digital Due Process Coalition.

Interactions with company. We contacted the company and briefed them on our findings prior to publication.
Instacart

An Internet-based grocery delivery service.

Instacart earns three stars in this year’s *Who Has Your Back* report. While there is room for improvement, we commend Instacart for taking initial steps to facilitate transparency and user privacy. In particular, Instacart earns credit for requiring a warrant for content, publishing law enforcement guidelines, and being a member of the Digital Due Process Coalition. Going forward, we encourage Instacart to require a warrant for prospective location data, publish transparency reports, and provide users notice when their data is sought by law enforcement.

**Warrant for content.** Instacart requires a warrant before giving content to law enforcement, stating in its law enforcement guides:

[W]e require a valid search warrant based on probable cause to produce the contents of user communications.

**Warrant for prospective location data.** Instacart does not state that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** Instacart does not have a published transparency report.

**Law enforcement guidelines.** Instacart publishes guidelines explaining its standards for providing user information to law enforcement, available here:

[https://www.instacart.com/help/section/200758544#209928353](https://www.instacart.com/help/section/200758544#209928353)

**Inform users about law enforcement data requests.** Instacart does not promise to provide users with notice about law enforcement requests. It states in its law enforcement guidelines that it may do so, but does not make an affirmative promise to users:

We reserve the ability to notify individuals about law enforcement requests for data related to them or their transactions at our discretion unless we are prohibited from doing so by an appropriate court order or other legal mechanism.

**Digital Due Process Member.** Instacart stands up for user privacy in Congress as a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company and briefed them on our findings prior to publication.
**App-based peer-to-peer taxi service.**

Lyft earns six stars in this year’s *Who Has Your Back* report. We commend Lyft for taking steps to facilitate transparency and user privacy, receiving credit in every one of our categories for their exemplary policies.

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

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

> We may produce information in the absence of a subpoena or warrant where there is an emergency that involves protecting a User or third party or stopping illegal activity that poses an immediate threat of death or serious bodily harm, as discussed in the emergency request section below. In these events, we require that valid and sufficient legal process be produced within three days of production of the information.

**Warrant for prospective location data.** Lyft states that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** Lyft has a published transparency report, available at:


**Law enforcement guidelines.** Lyft publishes guidelines explaining its standards for providing user information to law enforcement, available here:


**Inform users about law enforcement data requests.** Lyft promises to provide users with notice about law enforcement requests:

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

**Digital Due Process Member.** Lyft stands up for user privacy in Congress as a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company and briefed them on our findings prior to publication.
Postmates

Internet-based delivery service.

Postmates earns zero stars in this year’s *Who Has Your Back* report. In particular, Postmates does not require a warrant for content or prospective location data, does not publish a transparency report, does not publish law enforcement guidelines, does not provide notice to users when their data is sought by law enforcement, and is not a member of the Digital Due Process Coalition.

**Warrant for content.** Postmates does not require a warrant before giving content to law enforcement.

**Warrant for prospective location data.** Postmates does not state that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** Postmates does not have a published transparency report.

**Law enforcement guidelines.** Postmates does not publish guidelines explaining its standards for providing user information to law enforcement.

**Inform users about law enforcement data requests.** Postmates does not promise to provide users with notice about law enforcement requests.

**Digital Due Process Member.** Postmates does not stand up for user privacy in Congress by being a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company and briefed them on our findings prior to publication.
TaskRabbit

Internet-based on-demand labor and services.
TaskRabbit earns zero stars in this year’s *Who Has Your Back* report. In particular, TaskRabbit does not require a warrant for content or prospective location data, does not publish a transparency report, does not publish law enforcement guidelines, does not provide notice to users when their data is sought by law enforcement, and is not a member of the Digital Due Process Coalition.

**Warrant for content.** TaskRabbit does not require a warrant before giving content to law enforcement, stating in its privacy policy:

> TaskRabbit reserves the right to disclose Personal Information from both private and public areas of this website at our discretion, if required by law or if we are given reason to believe, in our sole discretion, that someone is causing injury to or interference with the rights of Users, the general public, or TaskRabbit, to comply with a judicial proceeding, court order or legal process.

**Warrant for prospective location data.** TaskRabbit does not state that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** TaskRabbit does not have a published transparency report.

**Law enforcement guidelines.** TaskRabbit does not publish guidelines explaining its standards for providing user information to law enforcement.

**Inform users about law enforcement data requests.** TaskRabbit does not promise to provide users with notice about law enforcement requests.

**Digital Due Process Member.** TaskRabbit does not stand up for user privacy in Congress by being a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company through two or more mediums to notify them of our results prior to publication, but did not receive a response.
Turo

Internet-based services for peer-to-peer car sharing.

Turo earns zero stars in this year’s *Who Has Your Back* report. In particular, Turo does not require a warrant for content or prospective location data, does not publish a transparency report, does not publish law enforcement guidelines, does not provide notice to users when their data is sought by law enforcement, and is not a member of the Digital Due Process Coalition.

**Warrant for content.** Turo does not require a warrant before giving content to law enforcement, stating in its privacy policy:

> We may disclose your Personal Information to other members of the Turo corporate family or to third parties, including our insurance and claims providers, as we believe to be necessary or appropriate: under applicable law, including laws outside your country of residence to provide insurance and claims services; to comply with legal process; to respond to requests from public and government authorities including public and government authorities outside your country of residence; to enforce our Terms of Service and related Policies; to protect our operations or those of any of our affiliates or users; to protect our rights, privacy, safety, or property, and/or that of our affiliates, you, or others; and to allow us to pursue available remedies or limit the damages that we or our users may sustain.

**Warrant for prospective location data.** Turo does not state that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** Turo does not have a published transparency report.

**Law enforcement guidelines.** Turo does not publish guidelines explaining its standards for providing user information to law enforcement.

**Inform users about law enforcement data requests.** Turo does not promise to provide users with notice about law enforcement requests.

**Digital Due Process Member.** Turo does not stand up for user privacy in Congress by being a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company through two or more mediums to notify them of our results prior to publication, but did not receive a response.
Uber

App-based peer-to-peer taxi service.

Uber earns six stars in this year's *Who Has Your Back* report. We commend Uber for taking steps to facilitate transparency and user privacy, receiving credit in every one of our categories for their exemplary policies.

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

Typically, we require 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 to compel our disclosure of certain communications between people using Uber or GPS location information. We make exceptions to these requirements for emergency and exigent requests, where a user has provided consent, or - for requests that do not require a warrant - where other legal or regulatory standards apply.

**Warrant for prospective location data.** Uber states that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** Uber has a published transparency report, available here:

https://transparencyreport.uber.com/

**Law enforcement guidelines.** Uber publishes guidelines explaining its standards for providing user information to law enforcement, available here:

https://www.uber.com/legal/other/guidelines-for-law-enforcement/

**Inform users about law enforcement data requests.** Uber promises to provide users with notice about law enforcement requests. It states in its law enforcement guidelines that it may do so, but does not make an affirmative promise to users:

It is our policy to notify riders and driver-partners of law enforcement requests for their information before disclosure, with exceptions for emergencies, exigent requests, when we have a good faith belief that notice would be counterproductive or would create a risk to safety, or when we are prohibited from doing so by law (i.e., statutory prohibition, court order, delayed notice). Law enforcement officials seeking non-disclosure of legal process should provide the details of their investigation to us so that we may determine whether a request falls into one of these exceptions. In all other circumstances, law enforcement
officials who do not want their request disclosed should obtain an appropriate court order establishing that notice is prohibited before serving legal process on Uber.

**Digital Due Process Member.** Uber stands up for user privacy in Congress as a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company and briefed them on our findings prior to publication.
VRBO

Internet-based market for peer-to-peer vacation rentals.

Note: VRBO is part of the same corporate entity as HomeAway (which is in turn owned by Expedia), which offers a similar service. They are governed by the same privacy policy, so this analysis applies to both of them as well as other companies within the HomeAway family operating under this policy.

VRBO earns zero stars in this year’s *Who Has Your Back* report. In particular, VRBO does not require a warrant for content or prospective location data, does not publish a transparency report, does not publish law enforcement guidelines, does not provide notice to users when their data is sought by law enforcement, and is not a member of the Digital Due Process Coalition.

**Warrant for content.** VRBO does not require a warrant before giving content to law enforcement. Its privacy policy states:

> We may disclose your personal data to enforce our policies, or where we are permitted to do so by applicable law, such as in response to a request by a law enforcement or governmental authority, or in connection with actual or proposed litigation, or to protect our property, people and other rights or interests.

**Warrant for prospective location data.** VRBO does not state that it requires a warrant before providing prospective location data to law enforcement.

**Transparency report.** VRBO does not have a published transparency report.

**Law enforcement guidelines.** VRBO does not publish guidelines explaining its standards for providing user information to law enforcement.

**Inform users about law enforcement data requests.** VRBO does not promise to provide users with notice about law enforcement requests.

**Digital Due Process Member.** VRBO does not stand up for user privacy in Congress by being a member of the Digital Due Process Coalition.

**Interactions with company.** We contacted the company through two or more mediums to notify them of our results prior to publication, but did not receive a response.
Links and Additional Resources

Digital Due Process:

Airbnb:
https://www.airbnb.com/terms/privacy_policy
https://www.airbnb.com/terms

FlipKey:
https://secure2.flipkey.com/content/terms/ftl/#privacy

Getaround:
https://www.getaround.com/privacy
https://www.getaround.com/terms

Instacart:
https://www.instacart.com/help/section/200758544#209928353
https://www.instacart.com/terms
https://www.instacart.com/privacy

Lyft:
https://www.lyft.com/privacy
https://www.lyft.com/terms

Postmates:
https://postmates.com/privacy
https://postmates.com/terms

TaskRabbit:
https://www.taskrabbit.com/privacy
https://www.taskrabbit.com/terms
Turo:
https://turo.com/policies/privacy
https://turo.com/policies/terms

Uber:
https://www.uber.com/legal/terms/us/
https://www.uber.com/legal/other/guidelines-for-law-enforcement/

VRBO:
https://www.vrbo.com/info/privacy
https://www.vrbo.com/info/termsandconditions
### Results From Previous Reports
#### 2015

<table>
<thead>
<tr>
<th>Company</th>
<th>Follows industry-accepted best practices</th>
<th>Tells users about government data demands</th>
<th>Discloses policies on data retention</th>
<th>Discloses government content removal requests</th>
<th>Pros-user public policy opposes backdoors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>★★</td>
<td>★★</td>
<td>★★</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Amazon</td>
<td>★★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Apple</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Comcast</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Credo</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Dropbox</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Facebook</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Google</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Microsoft</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Pinterest</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Reddit</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Slack</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Snapchat</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Sonic.net</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Tumblr</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Twitter</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Verizon</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Wickr</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>WordPress</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>★★</td>
<td>★★</td>
<td>N/A</td>
<td>★★★</td>
<td>★★★★</td>
</tr>
</tbody>
</table>
### 2014

<table>
<thead>
<tr>
<th>Company</th>
<th>Requires a warrant for content</th>
<th>Tells users about government data requests</th>
<th>Publishes transparency reports</th>
<th>Publishes law enforcement guidelines</th>
<th>Fights for users' privacy rights in courts</th>
<th>Fights for users' privacy rights in Congress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Amazon.com</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Apple</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Comcast</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>CREDO</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Dropbox</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Facebook</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Facebook</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Google</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Lookout</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Microsoft</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Myspace</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Pinterest</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Reddit</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Sonic.net</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>SugarCRM</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Tumblr</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Twitter</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Verizon</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>WTCKR</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>WordPress</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
</tbody>
</table>
### 2013

<table>
<thead>
<tr>
<th></th>
<th>Requires a warrant for content</th>
<th>Tells users about government data requests</th>
<th>Publishes transparency reports</th>
<th>Publishes law enforcement guidelines</th>
<th>Fights for users' privacy rights in courts</th>
<th>Fights for users' privacy rights in Congress</th>
</tr>
</thead>
<tbody>
<tr>
<td>amazon</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Apple</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>at&amp;t</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>comcast</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Dropbox</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>facebook</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>foursquare</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Google</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Microsoft</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>myspace</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Soncinet</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>brilliant</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>@twitter</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>tumblr</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Verizon</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>WordPress</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Tell users about data demands</td>
<td>Be transparent about government requests</td>
<td>Fight for user privacy in the courts</td>
<td>Fight for user privacy in Congress</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>amazon</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>at&amp;t</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>comcast</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropbox</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>facebook</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>foursquare</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinkedIn</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>loopt</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>myspace</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sonic.net</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sprint</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verizon</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td>⭐️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Tell users about data demands</td>
<td>Be transparent about government requests</td>
<td>Fight for user privacy in the courts</td>
<td>Fight for user privacy in Congress</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------------------------------</td>
<td>----------------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comcast</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropbox</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Myspace</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verizon</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo!</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>