branch

Are Your Third-Party Tools Putting Your Data at Risk?

3 Pitfalls to Avoid

The Power of Data

Data powers and improves every aspect of our lives. A modern car generates 25 GB of data per hour working to monitor health and keeping drivers safe. A modern airplane generates up to 1 TB of data every flight to keep us safe and improve the experience. Data has the potential to provide significant value. Take this example from Branch CEO, Alex Austin, who previously worked as a statistician and mathematical modeling engineer: Using billions of data points to drive experimentation, his team was able to create a new technology for a solar panel, setting the world record for solar panel efficiency. Data was the key to innovation that could have changed the world. From this experience came a unique perspective on the usage of data as Alex got involved in the mobile ecosystem around 8 years ago. He was confident Branch could leverage the scale of data to build better user experiences in mobile.

But everyone who operates in the digital economy is now aware, data can be as much a liability as an asset. In recent years, there have been many stories in the news around data privacy: data breaches, companies who've mismanaged user data, and companies who do "creepy" things with customer data. These data missteps are met with wide consumer criticism, brand boycotts, and even government legislation. But simply complying with new data privacy legislation is no longer enough. Companies who manage customer data have a moral and ethical responsibility to use it wisely and not test the boundaries of user privacy.

The onus is ultimately on the industry to take a more educated and productive approach to assessing how data is used. Every industry in the world relies heavily on third party companies that operate behind the scenes. For example, we trust our lives with airlines that buy airplanes from a select number of manufacturers such as Boeing or Airbus. These airplane manufacturers then buy parts from *thousands* of companies that you've never heard of, all of which are crucial for airplane safety and reliability. You don't care about these third party companies, because ultimately you trust the manufacturer to have properly vetted these third parties before using the components.

The same exact system exists in the digital economy. As a company operating a digital service (website, app, etc), you rely heavily on third parties to provide a great experience to your users and operate your business. Rather than physical reliability and safety as experienced in the airline industry, you have to make choices around data privacy and security when working with third party service providers. We must get to the point where you can give your users confidence in data security and safety of these third parties, in the same way that the transportation industry gives travellers this confidence.

This paper outlines the data privacy principles you should hold your own company accountable to as well as the third-party companies with which you share data. If companies abide by these principles and pledge to be Good Data Citizens, data can in fact be a force for good. Data can be used anonymously without violating a user's privacy, and help to deliver better, more seamless experiences to users.

The Cost of Data

In a 2019 survey conducted by Statista, 46% of U.S. smartphone users indicated they only buy products/services from brands/companies that they are confident will protect their privacy. If you don't handle user data properly and vet third parties to do the same, you run the risk of losing customers, money, and market value. According to 2019 industry data, a third-party data breach can cost your company almost $4.3 million USD.

Put simply:
You can't afford to do business with companies who aren't Good Data Citizens.

So how can you ensure the third-party companies you partner with won't put your (and your users') data at risk? Better yet, how can you evaluate the trustworthiness of third-party companies ***before*** you partner with them?

Branch example: Branch gives our customer companies and their users this confidence by following a set of principles that we believe all third parties should adhere to — and that companies should leverage in their evaluations of third-party companies. From a user perspective, if a company would respect these rules, they would be trustworthy and generally "not creepy". Moreover, if companies were to comply with these principles, they would be in a good position for compliance with GDPR or CCPA — or with the myriad of other privacy laws and regulations that are inevitably coming down the pike.

The Good Data Citizen Checklist

Principle 1: Third parties should not collect or store more information than is needed to perform the service

Third parties with direct access to user information can be tempted to collect the information "just in case" they want to use it for an initiative in the future. They should not do this. Confirm with third-parties that only the bare minimum information needed to provide the service is collected before you hand over access to your data.

Branch example: Branch does not collect data like end users' names or email addresses. We neither want nor need that data.

This same principle applies to storing the data as well. Data should not be stored for longer than it's needed, and if it is, it should be cleansed.

Branch example: After 7 days, Branch effectively renders unreadable its logs of end user data. This is because, even though it could be nice to have that data available "just in case," we've made the determination that the "just in case" doesn't outweigh the privacy and security benefits of limiting the scope of the data that we store.

Principle 2: Third parties should not sell / transfer ownership of data to other third parties

This is a more aggressive stance, given that many business models are still based on the premise of buying and selling data. However, this is a key root cause in the uproar around data usage, and the primary concern in the series of scandals we've observed over the last year. A user feels that they should own their data, and when ownership is not clear, it feels creepy and wrong. Third parties should address this directly, just as CCPA and GDPR are attempting to through legislation.

Any third party tool you work with should have a clear policy that the data is never rented or sold without the explicit permission of the user, so users can feel safe that they maintain ownership of their data. Moreover, Good Data Citizens should support direct deletion as well as standard opt outs to ensure users have control over their data. On the side of user-facing companies, you should make these controls available through an easily accessible portal.

Principle 3: Third parties should be implementing best practices in security and data protection protocols

Lastly, but definitely not least, even the most well-intentioned Good Data Citizen can still fail you if they fail to secure data. You can evaluate whether the third-party company you're considering is a Good Data Citizen by the measures they've taken to protect data. For example, companies should implement SOC2 protocols and employ a third-party bug bounty system, as well as have dedicated security professionals watching over the technology. Moreover, employees should be given regular trainings on how to avoid social engineering tactics like phishing. Only through investment can third-party companies ensure safekeeping of data — and ensure your peace of mind in partnering with them. If combined with data-deletion policies as described in Principle 1, you — and your users — can be confident that user data is safe and protected.

Insisting each third-party service provider you work with is a Good Data Citizen is essential in today's environment, and should be the top priority for any company expecting to operate in the future.

If companies hold themselves — all third-party providers — accountable to these three principles, then users can be confident that their data is secure, protected, and not used for anything other than giving them a great experience with the company with which they've chosen to interact.

Branch's entire product strategy, as well as privacy policy has been founded on these principles. It's served us extremely well in the past and will be crucial as the regulation over data continues to grow, through CCPA and beyond.

Interested in learning more about Branch? Let's chat.

About Branch

Branch provides the leading cross-platform linking and attribution platform, offering solutions that unify user experience and measurement across devices and channels. Branch powers mobile links and cross-platform measurement to more than 3 billion monthly users across the globe, and is a trusted cross-platform marketing, engagement, and measurement solution for over 50,000 apps — including Foursquare, BuzzFeed, Yelp, OfferUp, and many more.