

Zoho Ups the Ante on Data Privacy

By: Laurie McCabe

2/10/20



Most people are well aware that we are actually paying for the “free” applications we use with our data. From Facebook to Google to Pinterest, vendors monetize user data through advertising and by tracking and selling our data to third parties.

But many people are not aware of the increasing scope of these practices. In November, for instance, The Wall Street Journal reported that Google had covertly gathered “[tens of millions](#)” of [medical records](#)—patient names, lab results, diagnoses, hospitalization records, and prescriptions—from more than 2,600 hospitals as part of a machine-learning project code-named Nightingale—without notifying Ascension doctors and patients about the project. It’s not a one-off. For instance, [WebMD’s symptom checker shares information with Facebook](#) , and Google and Mastercard [cut a deal to track retail sales](#).

Even fewer people realize that many B2B companies are allowing surveillance companies to track their *paying* users on their sites. That’s right—even if you are spending a small fortune on business software, many of the big names in the industry are trading user data for products and services from companies such as Google, Twitter and LinkedIn.

For instance, in exchange for the free use of Google Analytics, a software vendor might embed Google code on its homepage. If the vendor invests in Google AdWords, the embedded code is a way for it to see whether its AdWords spend has resulted in new visitors to its site. The catch is that through the code, Google now has that visitor or business user's usage data—what they've clicked on, how they're building dashboards, and other general user actions. Google can then leverage that information to target ads to that user based on their usage data acquired through the embedded code.

Zoho's 20 Year Commitment to Privacy

At Zoho's 2020 Analyst Day, Raju Vegesna, Zoho's Chief Evangelist, underscored the company's 20-plus year commitment to protect user privacy—yet another example of [Zoho's convictions](#). Zoho has never sold customer data, or made a single dollar from advertising revenue—even in the free editions of its products. This allows Zoho to avoid the conflicts of interest inherent in these practices.

The company's [privacy policy](#) spells out in great detail what information Zoho gathers from customers and users, how Zoho will and won't use that information, and how it will not.

For instance, Zoho's policy clearly states that users own their service data, that Zoho protects and limits access to it, and only processes it according to user instructions. The policy also stipulates that Zoho will automatically delete user data from its active database within 6 months of termination, and from its backups within 3 months after that.

Zoho's Latest Privacy Pledge

Now, Zoho is taking this commitment a step further with a pre-emptive strike against what it calls “adjunct surveillance,” meaning the surreptitious act by B2B vendors of trading customer-usage data to Google or Twitter or Facebook in exchange for the free use of their services. Through this tactic, surveillance companies are gathering information about users’ data from adjunct properties without their permission.

According to Vegesna, while this practice is a legally acceptable business practice, it’s not morally acceptable because user data is very valuable. As a result, Zoho has decided to block adjunct surveillance on its properties to protect the privacy of its users.

The company has removed all third-party codes on its website. Users won’t see embedded ‘like’ or ‘share’ buttons, and removed trackers from all ad companies. However, users will still be able to share a page on social media either directly or by using a tool such as Zoho Social.

Since Zoho runs on its own cloud infrastructure—instead of on public clouds such as AWS or Google, that also have ad-based businesses—they can’t track Zoho user behavior either.

As a result, Zoho users can gain the peace of mind that their data—and their customers’ data—is where it belongs, and that it’s not being shared without their knowledge.

Perspective

Zoho's decision to remove third-party trackers from its sites isn't a one-off or gimmick, but an extension of its long-standing commitment to privacy.

But it doesn't come without a cost: The move means that Zoho will have access to less user data for its own marketing efforts than it would have if it kept these trackers in place. But over the long haul, the move should pay off in terms of helping Zoho build its brand as a trustworthy company.

By getting out in front of this issue, Zoho can also challenge others in the B2B software industry to follow suit. Since it owns the technology entire stack, from the data center on up, it may be easier for Zoho to execute on this than it would be for many of its competitors. But by raising the bar—and the issue—Zoho is helping to elevate awareness and reshape directions in this increasingly important area.

© SMB Group