Why Data Transparency is Not Enough to Protect Your Business

Published At: January 18, 2022
Last Updated: January 29, 2025
7 Min Read

Lusha
7 Min Read

Lusha
Chief Knowledge Officer

Give me the TL;DR ↓

Data transparency is on the tips of everyone's tongues lately, and you may be asking why.

Flashback to April 10th, 2018, Mark Zuckerberg, the founder and CEO of Facebook is in big trouble with the U.S. Congress.

What happened?

It was found that Cambridge Analytica, a British political advertising consulting firm, was collecting data on 87 million Facebook users without their knowledge or consent. In return, this data was misused to influence the 2016 presidential campaigns and other political events in Britain and Russia.

Ever since the scandal broke, data privacy has been the talk of the town, with investigative journalism exposing that other top tech companies have also had massive data breaches we didn't know about. Since then, there have been more online communities dedicated to discussing data transparency and privacy; one Reddit forum has over 1.2 million members!

This has forced B2B companies to take a second look at the third-party vendors they use to run their business, especially big data companies. But with billion-dollar companies experiencing breaches, how can you ever be sure your important information is safe? Well, you can't.

Data transparency is not enough to keep your data safe. However, there are many ways to hold big data companies accountable and put the power back into your hands as a business owner or leader. If you want to know what they are, continue reading this blog post to learn what data transparency is, why it won't protect your company, and how to be proactive in guarding your information and reputation.

What is data transparency?

Data transparency is where companies who collect the personal and business data and data insights of their prospects, clients, and customers (or outside their organization) are open and honest when they do so.

They provide a "privacy policy," which is a legal document on their website that outlines what data they collect (name, contact and financial information, etc.), how they collect data (through tracking your IP address or another method), how they manage and protect data (the quality of the website security) who they share data with (third parties, solicitors, etc.), and they also ensure that there is data accuracy in their reports.

A company is held legally responsible for the statements they write in their privacy policy. That means if they share or sell data without the knowledge or consent of their prospects, clients, or customers, they could face legal repercussions.

Why is data transparency on everyone's mind?

Data transparency is the subject of many discussions after the most significant data breaches of the 21st century have happened just within the last ten years. A data breach is when confidential or sensitive information is stolen, tampered with, or shared without permission by hackers, business competitors, or even big data companies.

For example:

- 2012: LinkedIn had 700 million users' data taken and sold on the deep web.
- 2013: Adobe has hackers steal 3 million users' credit card data.
- 2017: Advocate Medical Group has 4 million patient records tampered with.
- 2019: Alibaba had 1.1 billion pieces of user data breached.
- 2020: 500px, the photo-sharing platform had 14 million records compromised.

Even worse, many of these companies didn't catch or reveal the data breaches until years later to the public, their customers, or users after they were forced by law to be data transparent. As a result, users of websites are starting to realize if big billion-dollar tech companies can't keep our information safe, why should we trust or use them?

Without data transparency, your business can sink

B2B companies not only need to command data transparency from big data companies, but they also need to be open and honest with their employees and customers about how they collect, store and use data. Seriously! A data breach can have a massive impact on

your business, revenue, reputation, and customer segments.

- **You could face lawsuits:** Affected customers could choose to sue your business, costing thousands or millions in legal fees and restitution. You could also face penalties from your local government for not being data transparent or enforcing suitable security measures.

- **You could be held for ransom:** Businesses could experience ransomware and have data held hostage, either by your competitors or by hackers who want to extort you for money or proprietary information about your product or service.

- **Your reputation could be destroyed:** Customers want to trust the companies they purchase from; a data breach can damage your reputation and public image. It communicates that you don't have the security to protect your information.

- **Your business operations may be halted:** Data breaches require an internal investigation by cyber security specialists to find the source of the attack, understand the extent of the breach, develop strategies to contain it, and eliminate the main threat. Operations may be greatly reduced before any more attacks happen.

Don't rely on big data companies, to tell the truth

Data transparency is great, but unfortunately, B2B businesses owners should understand that just because a company says it will collect, handle, and store your personal and business data with care, it doesn't mean they actually will.

If a company experiences a data breach, they have a very good reason to lie or omit the truth from their customers and clients.

We all try to downplay or hide our mistakes when we mess up. For example, you might undercut a friend by going after a job they wanted and keeping it hush, to not lose that friendship. The same goes for data companies who experience security issues, sure it may not be their fault, but the fallout from customers and the public learning about it is the reason why they may avoid being data transparent. In 2021, Zoom had to pay an $85 million class-action lawsuit because they lied about giving data to Facebook and Google.

As business owners, you can never put the trust of something like your sales data or other company intel in someone else's hands.

A checklist to take control of your data and future

The power is always in your hands. We don't have control over what third-party vendors choose to do with our data, but we can limit threats to our privacy in several ways. Below is a checklist to ensure the companies you're using are data transparent.

- **Protect your website with antivirus software** and a secure sockets layer (SSL). This encryption method ensures any data your customers enter through forms on your website will be encrypted and useless to hackers.

- **Get data breach and cyber security training for leaders** of your company to stay on top of the latest software and strategies to protect data and know-how to train and prepare their staff.

- **Train your employees on safety procedures**, including not sharing files, passwords, or sensitive information outside the company.

- **Thoroughly read any third parties' privacy policy** (i.e., tech subscription services, financial services), research the company, and ask if they have had any data breaches before you decide to work with them.

- **Hire cybersecurity specialists to provide yearly checkups** across your website, databases, software, and servers to find any weaknesses hackers may find to steal your data.

Main takeaways

- **What is data transparency?** It is when a company outlines how they collect, store, manage, use, and protect the personal and business data of their customers, clients, and users. Also, companies should reveal if they will share or sell your data to third parties.

- **Why data transparency won't protect your business:** Many big data companies still lie to their customers, users, and the public when massive amounts of data are stolen, sold or tampered with in fear of lawsuits and bad publicity.

- **How can you protect your company data:** Get antivirus protection, train leaders and staff on the latest safety measures, and most importantly research if your third-party vendors have had a data breach and read through their privacy policy thoroughly.

Lusha
Chief Knowledge Officer

Our fearless leader and Chief Data Officer, Lusha is the B2B data's most-loved personal assistant. She's always there when you always need her, whether it's on Linkedin or B2B sites, helping you to find personal contact details for your prospect. Catch her on the blog, Lusha.com, or on her social media handles.

Keep on reading

SALES

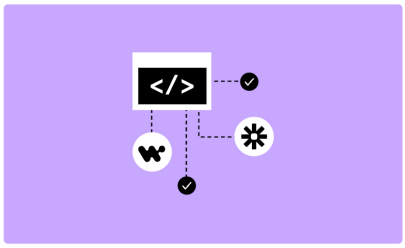
Introducing Lusha Playlists: Your Prospecting on Autoplay

April 14, 2025 | 4 min read

SALES

Introducing AI Recommendations: Your Personal Prospecting Assistant

February 13, 2025 | 3 min read



MARKETING

Seamless Automations with Lusha API Using Zapier & Workato

December 17, 2024 | 6 min read