Lenovo
Smart Privacy

Personalizing your privacy for greater control.

Frequently Asked Questions (FAQs)

This document contains the most commonly asked questions from customers who are interested in Lenovo Smart Privacy Services.

1. What is Lenovo Smart Privacy Services?
Lenovo Smart Privacy Services is an intelligent software that empowers you to enhance your privacy protection while you surf, browse, and shop online. With features that interrupt common digital surveillance, Lenovo Smart Privacy Services helps you own, control, and personalize your privacy, all in one place.

2. Where does my data go when I use Lenovo Smart Privacy Services?
Lenovo Smart Privacy Services was built to help protect your personal information. Personalizing your online privacy settings is our highest priority and each feature uses different protection protocols:

- To monitor your information against known organizational data breaches, the Privacy Scan feature uses your email address and phone number imported from your PC to find matches between your information and the information within certain breached databases. These data points are not stored and the results of your privacy scan are only stored locally on your PC.

- To monitor your information against account takeovers and identity theft, the Monitor feature requests you to create a user profile by entering your email address, name, physical address, DOB, and phone number. This information is stored via security enhanced storage protocols & encrypted with AES256.

- To help secure the privacy of your Lenovo Smart Privacy Services account, your private key is stored in an encrypted data base and is inaccessible to anyone except yourself. Lenovo does not have access to this information.

3. Where does my data go when I run a Privacy Scan?
Lenovo Smart Privacy Services uses your data (such as your email address) to perform a privacy scan that matches your information against our database of breached data. Lenovo Smart Privacy Services does not save any of your scanned data on our servers and the results reside only on your PC locally.

4. Why is Lenovo Smart Privacy Services better than what comes with my browser?
While your browser's privacy settings are designed to protect your digital privacy, its protection capabilities are often limited in scope to the management of your browsing history, cookie storage, flagging dangerous websites, and content sharing permissions.

Lenovo Smart Privacy Services not only works to make your browsing experience more private by blocking 3rd party web trackers[2] but also helps to secure your online accounts, encrypts your WiFi connection, monitors your information for exposure in organizational data breaches, and removes your profiled data from select sites found on the internet[1].

Lenovo

5. I can download a free anti-tracker, why should I use Lenovo Smart Privacy Services?

Lenovo Smart Privacy Services is not just an anti-tracker, it is a comprehensive set of privacy features that monitors your information for leaks caused by organizational data breaches, removes your information from select data brokerages/marketing lists[1], creates a more secure connection between your device and the internet through a personal VPN[3], and more safely stores and auto-fills your credentials in the browser as needed.

Free anti-trackers present a privacy dilemma to today's end users because the use of the software often hinges on the company getting access to your information. This could also mean that they are collecting or selling your information to data brokers. Further, free anti-tracking extensions often require you to be subjected to paid advertisements.

6. I already have a password manager, do I need to use Lenovo Smart Privacy Services?

Lenovo Smart Privacy Services' Vault feature and browser extension is more than a password manager. Apart from storing your logins, passwords, and credit card details in a vault with a synced browser extension[4] that conveniently auto-fills your credentials in the browser, it also creates unique passwords allowing you to use a different password for each of your accounts without having to remember anything.

It also helps you generate digital aliases that mask your email address on digital accounts. As a result, organizations that store your information cannot see your real email address, thus making your information less vulnerable to being shared with 3rd parties or misused after an organizational data breach[3].

7. Can I import my data from another password manager?

Yes. The information stored on a different password manager can be imported into Lenovo Smart Privacy Services through Edge, Chrome, and Firefox web browsers.

8. Who is a data broker?

Data brokers are entities who collect and sell consumer information (or analytic scores or classifications made based on consumer data) to other data brokers, companies, and individuals. Data brokers do not have a direct relationship with the people they collect data from, and the impacted individuals are often unaware that their information is being collected.

9. Which data brokers, people search sites, junk mailers, credit card solicitors, and telemarketers does Lenovo Smart Privacy Services monitor?

As of June 2021, Lenovo Smart Privacy Services monitors the following:

Donotcall.gov (Telemarketing), DirectMail (Junk Mailers), Lexis Nexis / Know X (Data Broker), Valpak (Junk Mailers), Spokeo (People Search Sites), AddressSearch.com (People Search Sites), DMAChoice (Junk Mailers), BeenVerified (People Search Sites), PeekYou (People Search Sites), ID True (People Search Sites), TruePeopleSearch (People Search Sites), Infogroup (Junk Mailers), RedPlum (Junk Mailers), InstantData (Data Broker), Radaris (People Search Sites), Oracle Data Cloud (Data Broker), Infotracer (People Search Sites), ThatsThem (People Search Sites), PeopleFinders (People Search Sites).

Features of Lenovo Smart Privacy Services

Privacy Scan - Identify At-Risk Digital Accounts
Helps uncover which digital accounts and personal information could be leaving you vulnerable for account takeover and identity theft.

Dashboard - Understand & Personalize Privacy
Get access to a privacy dashboard & understand your privacy risks review privacy alerts, take steps to reduce risks, manage private information, personalize digital account choices, and control your overall privacy risk profile.

Monitor - Detect & Act On Private Data Leaks
Get notified when it has been detected that your digital accounts & personal information have been leaked in organizational data breach or found on select search sites / aggregated marketing lists and take action to reduce the risk of account takeovers, identity theft, phishing scams, and spam mail[1].

Control - Enable Anti-tracking & Personal VPN
Prevent advertisers from reaching you by blocking 3rd party web trackers from knowing your online activity[2] and mask your device's IP address with a personal VPN for a safe and private browsing experience[3].

Vault - Store & Auto-fill Credentials & Credit Cards
Store your digital logins, passwords, and credit card details in a protected space with a synced browser extension[4] that conveniently auto-fills your credentials in the browser as needed.

Lenovo