

Privacy Policy

Effective as of October 12, 2026

Synoptic Technologies, Inc. ("Synoptic," "we", "us" or "our") provides a platform for researchers and traders to exchange information, access data streams, and, where enabled, interact with third-party trading venues through a Trading Terminal (the "Synoptic Platform"). This Privacy Policy describes how Synoptic processes personal information that we collect through the Synoptic Platform as well as through our other digital or online properties or services that link to this Privacy Policy (including as applicable, our www.synoptic.com website and any other website that links to this Privacy Policy and social media pages) as well as our marketing activities, live events and other activities described in this Privacy Policy (collectively with the Synoptic Platform, the "Service"). Synoptic may provide additional or supplemental privacy policies to individuals for specific products or services that we offer at the time we collect personal information.

This Privacy Policy does not apply to information that we process on behalf of our business customers (such as businesses and other organizations) where such processing is subject to a separate agreement between Synoptic and such customer. In such cases, if you have concerns regarding your personal information that we process on behalf of a business customer, please direct your concerns to that business customer.

Index

- **Personal information we collect**
- **Tracking Technologies**
- **How we use your personal information**
- **How we share your personal information**
- **Your choices**
- **Other sites and services**
- **Security**
- **International data transfers**
- **Children**
- **Changes to this Privacy Policy**
- **How to contact us**
- **Supplemental Privacy Notice – Trading Terminal (Synoptic)**

Personal information we collect

Information you provide to us or that we generate about you. Personal information you may provide to us through the Service or otherwise includes:

- **Contact data**, such as your first and last name, salutation, email address, billing and mailing addresses, professional title and company name, and phone number.
- **Demographic data**, such as your city, state, country of residence, postal code, and age.
- **Profile data**, such as the username and password that you may set to establish an online account on the Service, date of birth, biographical details, photograph or picture, links to your profiles on social networks or cryptocurrency exchanges, reputation score, influence score, information about your participation in our tournaments, verification status(es), accounts you

follow, interests, preferences, promotions, or surveys, and any other information that you add to or is generated on your account profile.

- **Communications data** based on our exchanges with you, including when you contact us through the Service, communicate with us via email, social media, or otherwise.
- **Transactional data**, such as information relating to or needed to complete your transactions on or through the Service, including order numbers and transaction history.
- **Marketing data**, such as your preferences for receiving our marketing communications and details about your engagement with them.
- **Synoptic Platform user-generated data**, such as comments, questions, messages, posts, photos, videos, upvotes or downvotes, and other content or information that you generate, transmit, or otherwise make available on the Synoptic Platform, as well as associated metadata. Metadata includes information on how, when, where and by whom a piece of content was collected and how that content has been formatted or edited. Metadata also includes information that users can add or can have added to their content, such as keywords, geographical or location information, and other similar data.
- **Data Stream Provider data**, such as business verification documentation, stream configuration settings, provider performance metrics, compliance status, API credentials, integration settings, and account standing information.
- **Data Stream usage data**, such as API access patterns, stream consumption metrics, data retrieval logs, rate limiting status, integration configurations, webhook endpoints, and stream subscription details.
- **Synoptic Platform tournament data**, including information that you share when you choose to enter or participate in a Synoptic Platform tournament, such as your tournament submission post.
- **Other data** not specifically listed here, which we will use as described in this Privacy Policy or as otherwise disclosed at the time of collection.
- **Sensitive personal information.** Please do not provide sensitive personal information (e.g., social security numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background or trade union membership) unless specifically requested for a stated verification or compliance purpose. Account credentials and financial-account information processed for enabled features are described in this Policy and the Supplemental Privacy Notice. Do not include secret trading credentials or wallet recovery phrases in support messages or public content.

Third-party sources. We may combine personal information we receive from you with personal information falling within one of the categories identified above that we obtain from other sources, such as:

- **Public sources**, such as government agencies, public records, social media platforms, and other publicly available sources.
- **Data providers**, such as information services and data licensors.
- **Partners**, such as marketing partners and event co-sponsors.
- **Customers and other Synoptic Platform users**, including users who may submit information about you in connection with their use of the Synoptic Platform.
- **Service providers** that provide services on our behalf or help us operate the Service or our business.

- **Third-party services, such as social media, wallet and authentication providers, that you use in connection with the Service.** This may include usernames, profile information, wallet identifiers and authentication or connection records, depending on your settings and the integration.

Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as:

- **Device data**, such as your computer or mobile device's operating system type and version, manufacturer and model, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique identifiers (including identifiers used for advertising purposes), language settings, mobile device carrier, radio/network information (e.g., Wi-Fi, LTE, 3G), and general location information such as city, state or geographic area.
- **Online activity data**, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them.
- **Communication interaction data** such as your interactions with our email, text or other communications (e.g., whether you open and/or forward emails) – we may do this through use of pixel tags (which are also known as clear GIFs), which may be embedded invisibly in our emails.

For more information concerning our automatic collection of data, please see the Tracking technologies section below.

Data about others. We may offer features that help users invite their friends or contacts to use the Service, and we may collect contact details about these invitees so we can deliver their invitations. Please do not refer someone to us or share their contact details with us unless you have their permission to do so.

Tracking Technologies

Cookies and other technologies. Some of the automatic collection described above is facilitated by the following technologies:

- **Cookies**, which are small text files that websites store on user devices and that allow web servers to record users' web browsing activities and remember their submissions, preferences, and login status as they navigate a site. Cookies used on our sites include both "session cookies" that are deleted when a session ends, "persistent cookies" that remain longer, "first party" cookies that we place and "third party" cookies that our third-party business partners and service providers place.
- **Local storage technologies**, such as HTML5 local storage, that can store data locally on your device and provide functionality similar to cookies.
- **Web beacons**, also known as pixel tags or clear GIFs, which are used to demonstrate that a webpage or email was accessed or opened, or that certain content was viewed or clicked.
- **Session-replay technologies**, such as those provided by HotJar that employ software code to record users' interactions with the Services in a manner that allows us to watch video replays of those user sessions. The replays include users' clicks, mobile app touches, mouse movements, scrolls and keystrokes/key touches during those sessions. These replays help us diagnose usability problems and identify areas for improvement. You can learn more about HotJar at <https://www.hotjar.com/legal/policies/privacy/>.

For information concerning your choices with respect to the use of tracking technologies, see the Your choices section, below.

How we use your personal information

We may use your personal information for the following purposes or as otherwise described at the time of collection:

Service delivery and operations. We may use your personal information to:

- provide the Service;
- enable security features of the Service;
- establish and maintain your user profile on the Service;
- facilitate your invitations to friends who you want to invite to join the Service;
- facilitate social features of the Service, such as by identifying and suggesting connections with other users of the Service and providing chat or messaging functionality;
- communicate with you about the Service, including by sending Service-related announcements, updates, security alerts, and support and administrative messages;
- communicate with you about events or contests in which you participate; and
- provide support for the Service, and respond to your requests, questions and feedback;
- operate and maintain Data Streams, including processing stream data, managing provider accounts, handling stream subscriptions, and monitoring stream performance;
- facilitate Data Stream Provider onboarding, including verification and compliance checks;
- process and manage Data Stream subscriptions and access;
- monitor and maintain Data Stream performance, availability, and quality;
- provide technical support for Data Stream integration and usage.

Service personalization, which may include using your personal information to:

- understand your needs and interests;
- personalize your experience with the Service and our Service-related communications; and
- remember your selections and preferences as you navigate webpages.

Service improvement and analytics. We may analyze use of the Service and our communications to understand activity and engagement, including page visits, navigation and email interactions; improve the Service and our business; and develop new products and services. For Data Streams, this includes analyzing usage patterns and trends, optimizing delivery, monitoring and improving API performance and reliability, and developing features and improving data quality and reliability. For example, we use Mixpanel for this purpose.

Marketing. We, our service providers and our third-party partners may collect and use your personal information for marketing purposes. For example, we may send you direct marketing communications and may personalize these messages based on your needs and interests. You may opt-out of our marketing communications as described in the Opt-out of communications provision below.

Compliance and protection. We may use your personal information to:

- comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas, investigations or requests from government authorities;

- protect our, your or others' rights, privacy, safety or property (including by making and defending legal claims);
- audit our internal processes for compliance with legal and contractual requirements or our internal policies;
- enforce the terms and conditions that govern the Service; and
- prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks and identity theft.

Research and commercial uses. We may use and share information collected or generated through the Service, including personal information, usage and activity data and derived analytics, for lawful business purposes, including research, product development and commercial offerings.

Further uses. In some cases, we may use your personal information for further uses, in which case we will ask for your consent to use of your personal information for those further purposes if they are not compatible with the initial purpose for which information was collected.

How we share your personal information

We may share your personal information with the following parties and as otherwise described in this Privacy Policy, in other applicable notices, or at the time of collection.

Affiliates. Our corporate parent, subsidiaries, and affiliates.

Service providers. Third parties that provide services on our behalf or help us operate the Service or our business (such as hosting, information technology, customer support, email delivery, marketing, consumer research and website analytics).

Payment processors. Any payment card information you use to make a purchase on the Service is collected and processed directly by our payment processors, such as Stripe. For Data Stream Providers, we use Stripe Connect to facilitate marketplace payments. Stripe may use your payment data in accordance with its privacy policy, <https://stripe.com/privacy>. Data Stream Providers may be required to provide additional information to Stripe for identity verification and compliance purposes.

Third parties designated by you. We may share your personal information with third parties where you have instructed us or provided your consent to do so.

Partners and business customers. Third parties with whom we partner, including parties with whom we co-sponsor events or promotions, with whom we jointly offer products or services, or whose products or services may be of interest to you, and customers or licensees of our data products and services.

Data Stream Providers. If you subscribe to or access a Data Stream, we share certain information with the relevant Data Stream Provider, such as:

- Subscription status and usage analytics
- Aggregated performance metrics
- Technical integration details necessary for service delivery
- Payment processing status (excluding detailed financial information)

Data Stream Infrastructure Providers. We work with specialized service providers to deliver, monitor, and maintain Data Streams, including:

- API infrastructure and management services
- Stream monitoring and alerting services

- Data quality and verification services
- Performance analytics providers

Linked third-party services. If you verify through, log into, or otherwise link a social media or other third-party service to your Service account, we may share your personal information with that third-party service. The third party's use of the shared information will be governed by its privacy policy and the settings associated with your account with the third-party service. For example, we allow users to link their accounts to their X (formerly known as Twitter) accounts. You can learn more about how X uses your personal information by visiting its privacy policy at <https://x.com/en/privacy>.

Professional advisors. Professional advisors, such as lawyers, auditors, bankers and insurers, where necessary in the course of the professional services that they render to us.

Authorities and others. Law enforcement, government authorities, and private parties, as we believe in good faith to be necessary or appropriate for the Compliance and protection purposes described above.

Business transferees. We may disclose personal information in the context of actual or prospective business transactions (e.g., investments in Synoptic, financing of Synoptic, public stock offerings, or the sale, transfer or merger of all or part of our business, assets or shares), for example, we may need to share certain personal information with prospective counterparties and their advisers. We may also disclose your personal information to an acquirer, successor, or assignee of Synoptic as part of any merger, acquisition, sale of assets, or similar transaction, and/or in the event of an insolvency, bankruptcy, or receivership in which personal information is transferred to one or more third parties as one of our business assets.

Other Synoptic Platform users and the public. Your profile and other Synoptic Platform user-generated content may be visible to other users of the Service and the public. For example, other users of the Service or the public may have access to your information if you chose to make your profile or other personal information available to them through the Service, such as when you provide comments, reviews, survey responses, or share other content. This information can be seen, collected and used by others, including being cached, copied, screen captured or stored elsewhere by others (e.g., search engines), and we are not responsible for any such use of this information.

Your choices

In this section, we describe available choices and, where applicable, additional rights under privacy law.

Access or update your information. If you have registered for an account with us through the Service, you may review and update certain account information by logging into the account.

Privacy requests. Depending on your location and applicable law, you may request access to or a copy of your personal information, correction or deletion, withdrawal of consent, restriction of certain processing, or an opt-out of any sale, sharing or targeted advertising as defined by that law. These rights are subject to applicable conditions and exceptions; withdrawal does not affect prior lawful processing or processing lawfully undertaken on grounds other than consent.

To make a request, contact info@synoptic.com and describe the information or right involved. Where permitted or required, we may ask for information reasonably necessary to verify your identity or an authorized agent's authority. We will respond within applicable legal deadlines and explain any refusal as required. Where you have a right to appeal, contact the same address identifying your request and the basis for your appeal. You may also complain to your applicable privacy regulator. We will not unlawfully discriminate against you for exercising your rights.

Opt-out of communications. You may opt-out of marketing-related emails by following the opt-out or unsubscribe instructions at the bottom of the email, or by contacting us. Please note that if you choose to opt-out of marketing-related emails, you may continue to receive service-related and other non-marketing emails.

Cookies and other technologies. Most browsers let you remove or reject cookies. To do this, follow the instructions in your browser settings. Many browsers accept cookies by default until you change your settings. Please note that if you set your browser to disable cookies, the Service may not work properly. For more information about cookies, including how to see what cookies have been set on your browser and how to manage and delete them, visit www.allaboutcookies.org. You can also configure your device to prevent images from loading to prevent web beacons from functioning.

Privacy settings. We make available certain privacy settings on the Service, including options to control the visibility of your email address, X/Twitter handle, and phone number.

Advertising choices. You may be able to limit use of your information for interest-based advertising through the following settings/options/tools:

- **Browser settings.** Changing your internet web browser settings to block third-party cookies.
- **Privacy browsers/plugin-ins.** Using privacy browsers and/or ad-blocking browser plug-ins that let you block tracking technologies.
- **Platform settings.** Certain platforms offer opt-out features that let you opt-out of use of your information for interest-based advertising. For example, you may be able to exercise that option for Google and Facebook, respectively, at the following websites:
 - o Google: <https://adssettings.google.com/>
 - o Facebook: <https://www.facebook.com/about/ads>
- **Ad industry tools.** Opting out of interest-based ads from companies that participate in the following industry opt-out programs:
 - o Network Advertising Initiative: http://www.networkadvertising.org/managing/opt_out.asp
 - o Digital Advertising Alliance: optout.aboutads.info.

You will need to apply these opt-out settings on each device and browser from which you wish to limit the use of your information for interest-based advertising purposes.

Do Not Track. Some Internet browsers may be configured to send “Do Not Track” signals to the online services that you visit. We currently do not respond to “Do Not Track” signals. This is distinct from legally recognized opt-out preference signals, which we honor where required by applicable law. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>.

Declining to provide information. We need to collect personal information to provide certain services. If you do not provide the information we identify as required or mandatory, we may not be able to provide those services.

Linked third-party platforms. If you choose to connect to the Service through or to your social media account or other third-party platform, such as X, you may be able to use your settings in your account with that platform to limit the information we receive from it. If you revoke our ability to access information from a third-party platform, that choice will not apply to information that we have already received from that third party.

Data Stream Settings. Data Stream Providers can control Stream visibility and description through their provider dashboard.

Other sites and services

The Service may contain links to websites, mobile applications, and other online services operated by third parties. In addition, our content may be integrated into web pages or other online services that are not associated with us. These links and integrations are not an endorsement of, or representation that we are affiliated with, any third party. We do not control websites, mobile applications or online services operated by third parties, and we are not responsible for their actions. We encourage you to read the privacy policies of the other websites, mobile applications and online services you use.

Security

We employ technical, organizational and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies and we cannot guarantee the security of your personal information.

For Data Streams, we implement additional security measures including:

- API authentication and access controls
- Rate limiting and abuse prevention
- Stream data encryption in transit and at rest
- Continuous security monitoring of stream access and usage
- Regular security assessments of stream infrastructure

International data transfers

We are headquartered in the United States and may use service providers that operate in other countries. Your personal information may be transferred to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country.

Children

The Service is not intended for use by anyone under 18 years of age. If you are a parent or guardian of a child from whom you believe we have collected personal information in a manner prohibited by law, please contact us. If we learn that we have collected personal information through the Service from a child without the consent of the child's parent or guardian as required by law, we will comply with applicable legal requirements to delete the information.

Changes to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make material changes to this Privacy Policy, we will notify you by updating the date of this Privacy Policy and posting it on the Service or other appropriate means. Any modifications to this Privacy Policy will be effective upon our posting the modified version (or as otherwise indicated at the time of posting). In all cases, your use of the Service after the effective date of any modified Privacy Policy indicates your acknowledging that the modified Privacy Policy applies to your interactions with the Service and our business.

How to contact us

- **Email:** info@synoptic.com

Supplemental Privacy Notice – Trading Terminal (Synoptic)

This Supplemental Privacy Notice applies to personal information processed in connection with Synoptic's Trading Terminal. This notice supplements Synoptic's Privacy Policy and is intended to provide additional details specific to Trading Terminal functionality. If the notices conflict, this notice controls only for the Trading Terminal. Capitalized terms not defined here have the meanings given in the Trading Terminal Terms.

1. What the Trading Terminal does

The Trading Terminal is a web-based interface that allows individuals to connect eligible accounts and/or wallets at supported Trading Venues, which may include Polymarket, Kalshi and Hyperliquid, and submit Trading Instructions (e.g., viewing balances, placing/canceling orders, viewing fills/PnL, using charts, alerts/automation and, where enabled, swaps, transfers and approvals through supported on-chain protocols). Available integrations and permissions vary as described in the Trading Terminal.

2. Personal information we collect for the Trading Terminal

Depending on how you use the Trading Terminal, we may collect or generate the following categories of information:

1. Account and wallet connection data. Synoptic account identifiers, Trading Venue selected, wallet and signer addresses, Privy user/wallet identifiers, subaccount identifiers, connection status, permissions and authorization records (including scope, expiry and revocation status where available), and related configuration.

2. Trading and portfolio data. Portfolio/balances, open orders, order history, cancellations, positions, fills, PnL, transaction identifiers, fees, funding and related trading activity shown through the Trading Terminal. We maintain order records linking your Synoptic user ID, trading-wallet address and order details.

3. Terminal usage and interaction data. Interactions with the Trading Terminal, including content, feeds, markets and instruments viewed or selected; searches, watchlists, chart activity, preferences, alerts and automation settings; order-entry activity, whether or not an order is submitted or completed; and the timing and sequence of these interactions.

4. Device and usage data. IP address, approximate location derived from it, device/browser identifiers, pages/screens viewed, timestamps, navigation paths, clicks, and session activity.

5. Diagnostics and security data. Error logs, performance data, rate limiting events, and other telemetry used to maintain reliability and prevent abuse.

6. Credential and authentication information, including API credentials and signing-related information as described in Section 3.

7. Eligibility and verification data, where requested or generated: information and documents concerning identity, account authority, location, sanctions status, source of funds or other eligibility requirements, and related review results.

3. Credentials (API keys and wallet signing)

1. API credentials. For Polymarket, Synoptic's backend receives and holds your API key, secret and passphrase in server memory for authenticated operations, including order cancellation. Where configured, the credentials also persist in an encrypted browser cookie that Synoptic's server can decrypt. These credentials are distinct from the private key used to sign a new order.

2. Wallet infrastructure. We use Privy for wallet authentication, embedded wallets and signing for Polymarket and Hyperliquid. In the current on-device configuration, encrypted key material is distributed between your device and Privy infrastructure and the complete key is reconstructed

temporarily within Privy's isolated browser component for signing. Supported import or legacy flows may process a private key in your browser. We do not ask for your seed phrase or recovery phrase. Privy's Privacy Policy describes its own processing.

3. Authorization and connection records. We process wallet addresses, public keys, signatures, permission records and connection metadata, including Synoptic and Privy identifiers. Account-reset flows may also involve Privy access tokens and related authentication records. The current trading implementation obtains new wallet signatures through the frontend; Hyperliquid instructions reach our backend as signed commands.

4. Proxying. Trading Venue and transaction-infrastructure requests and responses may pass through Synoptic servers to provide the Trading Terminal, including to relay instructions, perform authorized API operations, and apply reliability, rate-limiting and security controls.

4. Tracking technologies used in the Trading Terminal

The Trading Terminal uses tracking technologies and similar tools as described in the Privacy Policy, including local storage technologies and session-replay technologies where deployed.

We may also use analytics tools (e.g., Mixpanel) and logging/monitoring tools to understand usage and improve the Trading Terminal. Secret credential values, private signing keys and recovery phrases are not intended for collection through analytics or session-replay tools. Authentication and signing involve separate credential processing as described in Section 3.

5. How we use Trading Terminal information

We use Trading Terminal-related information to:

- **Provide the Trading Terminal** (authenticate access, connect accounts/wallets, display portfolio data, submit Trading Instructions, provide alerts/automation, reconcile activity, support account resets, and calculate or collect applicable fees);
- **Secure and maintain** the Service (fraud prevention, abuse detection, rate limiting, troubleshooting);
- Analyze usage and activity patterns, personalize and improve the Service, conduct research, and develop features, analytics and data products;
- **Comply with law and enforce terms** (including eligibility, location and sanctions checks where undertaken, and retaining appropriate review records).

We may also use and share Trading Terminal information for the research and commercial purposes described in the Privacy Policy.

6. How we share Trading Terminal information

In addition to sharing described in the Privacy Policy, we may share Trading Terminal information with:

- 1. Trading Venues and wallet, node or transaction-routing providers** involved in the integration you enable, to establish connections, process authentication or signing requests, carry out Trading Instructions and related authorizations, and process applicable fees.
- 2. Service providers** that help operate the Trading Terminal (e.g., cloud hosting providers, logging/monitoring tools, analytics providers, session replay providers, and verification providers where used), consistent with the Privacy Policy.
- 3. Authorities and others** when required for compliance and protection purposes, as described in the Privacy Policy.
- 4. Independent third parties.** Trading Venues, wallet providers and other integrated Third-Party Services may process information for their own purposes under their own terms and privacy notices. Those independent practices are not controlled by Synoptic; Synoptic's own processing remains governed by this Privacy Policy and notice.

Optional leaderboards (if enabled): If we offer leaderboards and you choose to participate, we may display certain trading performance or profile information to other users and/or the public based on your selection. Connecting an account or wallet does not by itself publish your non-public trading history or portfolio to a profile or leaderboard; those features follow your selections and do not limit other disclosures described in this Policy.

Public blockchain records. Wallet addresses, transactions and related activity may be recorded on public blockchains that Synoptic does not control. Depending on the network, transaction information may be visible before confirmation and may be linked to you using other information. Synoptic cannot remove or alter those records. Changing Synoptic settings or ending your use of the Trading Terminal does not change records held on a blockchain or independently by a venue. Applicable requests concerning information held by Synoptic are handled under this Privacy Policy.

7. Retention

- We may retain Trading Terminal-related information for lawful business purposes described in this Policy, including service operation, security, research, product development, commercial offerings, dispute resolution and legal protection, subject to applicable legal requirements. Retention depends on the information, purpose, and applicable obligations, rather than solely on whether you continue using the Trading Terminal. Credential access, authorization periods and retention of related account or activity records are distinct; expiry or revocation of a trading permission does not itself delete retained information.
- Deletion requests are subject to applicable exceptions. Some records, including security or dispute logs and backup copies, may be retained where permitted or required.

8. Your choices (Trading Terminal specific)

- **Remove local data and revoke permissions:** Clearing site data/browser storage can remove locally stored API credentials and wallet connection/session information. It does not by itself delete a Privy wallet, revoke API credentials, session/agent permissions or wallet/fee approvals, cancel orders, or delete information already received by Synoptic. Revocation and its effect on orders depend on the applicable venue or provider rules. Use the relevant controls for revocation and the privacy-request process for applicable deletion requests.
- **Cookies and tracking controls:** Your choices for cookies and similar technologies are described in the Privacy Policy.
- **Leaderboard participation (if offered):** You will be able to opt in/out if we offer it.

9. Security

We use safeguards designed to protect personal information, but security risk is inherent and we cannot guarantee security.