Palantir

A CORE COMMITMENT

PROTECTING PRIVACY & CIVIL LIBERTIES

Prepared by:

Palantir Technologies Inc.
http://www.palantir.com
+1.650.815.0200

INTRODUCTION

Palantir Technologies is a mission-driven company, and a core component of that mission is protecting fundamental rights to privacy and civil liberties. Since its inception, Palantir has invested its intellectual and financial capital in engineering technology that can be used to solve the world's hardest problems while simultaneously protecting individual liberty. We believe an information system becomes a liability when it lacks robust, built-in measures to promote responsible data use. This is why we have made data protection among our highest priorities at every point in the development of the Palantir Platform, and it is why organizations in sectors ranging from national security to global finance to health care trust the Palantir Platform to safeguard their most important data and analysis assets. This document describes the ways in which Palantir is working to meet the demands of the 21st-century data-handling environment while protecting privacy and civil liberties.

The Palantir Platform comprises a number of powerful technologies that can form the basis of a rigorous governance policy designed to ensure the protection of privacy and civil liberties. At a time when the creation of electronic information is expanding exponentially, and both government and private-sector electronic information handling is under increasing scrutiny, robust privacy and civil liberties protections are crucial to building public confidence in the management of potentially sensitive information. Precision data access and use controls, secure information sharing, multiple means of checking data accuracy, real-time and immutable audit functions, and federated database systems as described below are uniquely facilitated by the Palantir Platform. In the Palantir Platform, these protections are based on the same technology that makes Palantir so analytically powerful. Consequently, these protections are seamlessly integrated into the platform's functionality without degrading its analytic effectiveness or ease of use. In fact, they can actually promote mission success, making analysts' jobs easier and improving work products.

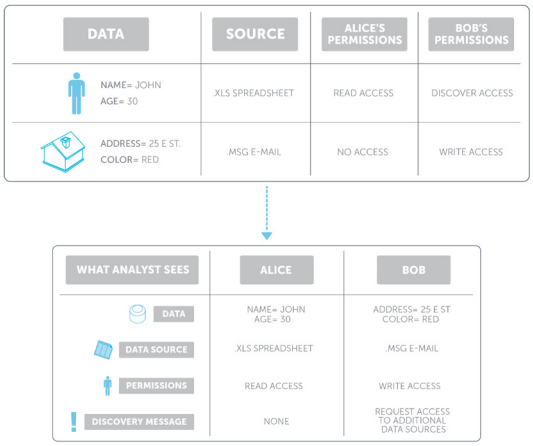
In addition to these technical capabilities, Palantir also deploys a team of privacy and civil liberties engineers whose mission is to constantly improve these privacy-enhancing technologies and promote their adoption by our customers and more broadly. They keep close track of global developments in law and policy that could require changes in data-handling practices and they collaborate with customers to help them comply with new requirements. Palantir's engineers work to ensure that our technology sets the standard for enabling compliance with existing laws and regulations, improving existing privacy protections, and anticipating and addressing future privacy and civil liberties issues likely to arise in a constantly evolving technical and legal landscape.

PRECISION DATA PROTECTION

The Palantir Platform includes precision data handling and multi-level security capabilities that support a number of vital privacy protections. The platform enables users with multiple and varying access permissions to interact appropriately with data with multiple and varying access restrictions, seeing only data they are authorized to see and using it only in ways for which they have authority. Palantir secures information on a data-point-by-data-point basis, including the metadata associated with each point. (In database terms, this is referred to as "sub-cell level security.") This is in stark contrast to many data management systems currently in use today that, at best, offer all-or-nothing access at the network or data system level, a limitation that often leads to information under- or over-sharing.

This multi-level security model allows Palantir customers to implement a number of fundamental Fair Information Practice Principles that underpin information-handling law and policy around the world.[1] Palantir gives administrators the flexibility they need to design and implement a precision data protection regime. Each Palantir user can be assigned a series of access permissions that will enable the selective revelation of information based upon the user's particular role, mission, or authority, as well as his or her security clearance (where applicable). Data owners and individuals who provide data to the system can thus be more certain that data use will be limited to the purposes for which the data was originally collected.

Palantir's access controls are also dynamic, allowing authorized personnel to adjust access to specific data points, data sources, analyses, or other information. These access adjustments can be permanent or temporary, based on the changing needs of the user and the security and regulatory requirements of the particular enterprise. Access control adjustments take effect within seconds, instantly barring any newly unauthorized user from any further interaction with the newly restricted data. As with most user actions in Palantir, such information access changes are recorded in immutable audit logs, ensuring individual accountability for any changes and enabling appropriate management or oversight officials to recognize inadvertent misuse or failures in training or management with regard to data handling and protection.



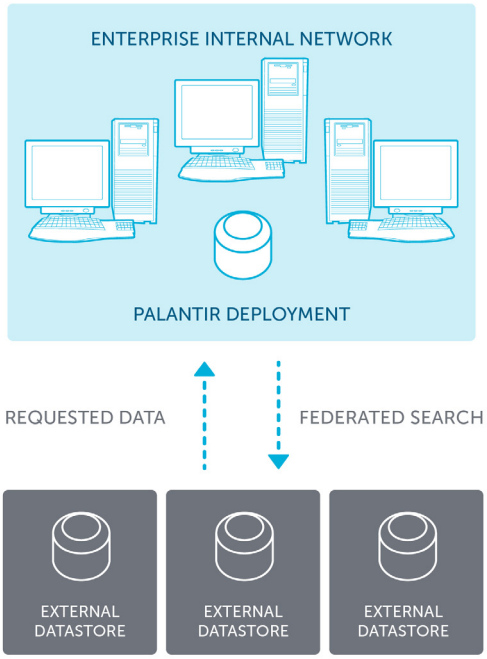
MULTI-LEVEL SECURITY. In Palantir, users with multiple and varying access permissions can interact appropriately with data with multiple and varying access restrictions.

[1] For more information, see "Palantir and the Fair Information Practice Principles," available on the Palantir website.

FEDERATED DATA SOURCE ARCHITECTURE

A federated database system allows data from multiple autonomous, and independently located databases to be searched and analyzed while avoiding the privacy- and cost-related risks associated with the creation of a single, centralized database. For example, the aggregation of multiple data sources into a single master database can lead to confusion about, or even inadvertent weakening of, the data-handling rules that apply to a particular piece of data. Enterprises can more easily adhere to these rules by maintaining separate, autonomous data repositories. This strategy also reduces the amount of data potentially exposed at the site of a security breach. Finally, a federated database system can allow data owners to share information without surrendering either control over data use or the responsibility of maintaining information accuracy.

The Palantir Platform includes technologies that enable enterprises to implement federated approaches to data integration.[2] With the Palantir Platform, multiple entities can maintain their own, autonomous databases, using legacy hardware and software, while Palantir connects to and indexes these databases without copying them in their entirety into a central database. This enables analysts to search external autonomous databases from within Palantir. Records returned by a particular query—and only those records— are imported into the Palantir Platform for structuring and analysis. Federated data that has been imported into Palantir remains tethered to its original source, ensuring that edits or deletions performed by the owners of the original data source are reflected in Palantir. Palantir's Horizon technology goes a step further by enabling users to perform certain types of analysis on federated structured data without transferring the source documents into the Palantir base realm.



FEDERATED SEARCH ARCHITECTURE. Users query an index of external data sources from within the Palantir workspace. Only data matching that query is imported into the internal data store for further use.

[2] Palantir's federated search appliance—the Palantir Raptor service—"wraps" Palantir's search capabilities around databases without importing their data wholesale into a centralized database.

ACCURACY & REDRESS

Action taken on the basis of inaccurate information risks undermining mission success, and may also result in costly mistakes, improper government surveillance or arrest, or other significant curtailments of civil liberties. Palantir provides users with effective means to detect and correct errors in their enterprise data, thereby improving the quality of the analytic product and reducing the risk of intentional or inadvertent privacy violations.

Tethered sourcing connects data points in Palantir to source records supporting that data. Users can independently review the provenance and pedigree of data and determine for themselves whether the information is accurate. Subject to sufficient access permissions, users can also review a complete history of the data, where they can track additions, modifications, and deletions, thus avoiding making the same errors repeatedly. The ability to share data securely within the Palantir Platform also encourages greater collaboration, allowing analysts to review each other's data and conclusions while mitigating security risks and minimizing occasions for unauthorized file or document dissemination.

In spite of all of these protections, inaccuracies in any data set are inevitable. When such inaccuracies are identified, they must be quickly corrected to ensure the minimum amount of disruption for those affected, protect against misidentification, enable redress, and enhance mission success. Palantir maintains a single, canonical version of data, rather than propagating multiple copies of information across an enterprise, each of which must then be located to be updated or deleted. Consequently when mistakes in the data are discovered, corrections are quickly pushed to all users, greatly simplifying the redress process and reducing the likelihood of repeated errors.

ANONYMIZATION

Anonymization or deidentification of data (i.e., the removal or masking of Personally Identifiable Information (PII) from records) has long been regarded as a means of sharing information while protecting the identity of the individuals to whom that information pertains. While recent studies have suggested that it may increasingly be easier to "reidentify" supposedly anonymized data, most experts still agree that, in many situations, anonymization still provides significant privacy and civil liberties benefits.[3]

The Palantir Platform includes technologies that promote effective data anonymization and combat reidentification. For a given data record, Palantir's granular access controls can be used to apply protections to PII while allowing the rest of the data to be shared for analysis. This effectively anonymizes data, allowing greater information sharing without compromising individual privacy. Furthermore, Palantir's ability to granularly secure data promotes a compartmentalized approach to data access, which decreases the likelihood of unwarranted reidentification of data that has been deliberately anonymized to protect identities.

CONCLUSION

The Palantir Platform powers a host of different capabilities necessary to provide robust privacy and civil liberties protections and enforce compliance with applicable laws, policies, and procedures. These unique protective capabilities include: precision data protection and dynamic access control, mechanisms to ensure data accuracy, federated search and analysis, effective anonymization of personal data, and real-time and immutable auditing of data use. On the Palantir Platform, enterprises can build a privacy and civil liberties regime that offers strong protections without sacrificing analytic power. A Palantir deployment can be readily configured to answer the complex privacy and civil liberties-led demands of 21st century data handling.

3 See, e.g., Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010).

Palantir Technologies, Inc.
100 Hamilton Ave.
Suite 300
Palo Alto, CA 94301

Inquiries: www.palantir.com/contact

www.palantir.com