Palantir

100 Hamilton Avenue
Palo Alto, California 94301

PALANTIR & LAW ENFORCEMENT

Protecting Privacy and Civil Liberties

TABLE OF CONTENTS

Introduction **2**

Solution Overview **3**

Privacy Protective Technology **4**

Enforcing Access 4

Managing Data Retention 5

Overseeing Use and Ensuring Accountability 7

Privacy & Civil Liberties Engineering **8**

INTRODUCTION

As local, state, and federal level law enforcement agencies introduce cutting-edge investigative and analytical techniques to better serve and protect their communities, they must also employ equally innovative technologies to ensure that those techniques do not undermine fundamental privacy and civil liberties protections.

The Palantir Platform provides law enforcement customers with a data integration and analysis software platform that builds upon existing law enforcement data stores to enable comprehensive knowledge management, collaboration, search, and investigative capabilities. A core feature of the offering is the flexibility necessary to build a rigorous data management and oversight regime without sacrificing utility. Analytical effectiveness does not need to come at the expense of privacy protections.

This white paper describes key technical features of the Palantir Platform that can be configured to protect privacy and civil liberties and meet evolving regulatory standards. It also describes our approach to civil liberties engineering as a confluence of efforts working with customers, developers, advisors, and other relevant stakeholders to build and help implement solutions that effectively address the law enforcement challenges of today and tomorrow.

SOLUTION OVERVIEW

Palantir Technologies is a software company focused on helping our customers solve some of the world's hardest problems. Our flagship software, the Palantir Platform, features a full suite of analytical tools that enable organizations and their analysts to collaboratively generate actionable insights from large and disparate data sets. The Palantir Platform has been used to tackle data-driven problems in myriad contexts, from efficiently delivering aid to victims of a natural disaster to helping law enforcement agencies (LEAs) coordinate efforts to track a dangerous fugitive or rescue an abducted child.

Consistent with our core philosophy, the Palantir Platform supports both powerful analysis and protection of privacy and civil liberties through the following key architectural principles:

Precision data control	Our LEA customers own and control their data, and can regulate access, use, and sharing of that data with extreme granularity.
Intelligence augmentation, not artificial intelligence	We recognize that computers excel at certain tasks (e.g., repetitive computations), while humans are better at others (e.g., critical decision making, especially where the lives and liberties of individuals are concerned). Palantir is designed to put the analyst at the top of the analytical chain, while the machine handles the more tedious workflows, thereby freeing humans to focus on the types of data problems that cannot be solved purely algorithmically or that could affect individual liberties if mishandled.
Mission-driven data analytics	We understand that information is not an end in itself and that the goal of law enforcement analysis is not to indiscriminately amass or review large data sets, but rather to maximize useful and mission-focused insights that are gained from data. With this focus front-of-mind, Palantir can help customers limit the use (or misuse) and exposure of irrelevant data.

The following section details the specific ways in which the Palantir Platform's capabilities are used to protect privacy and civil liberties while maximizing mission effectiveness.

PRIVACY PROTECTIVE TECHNOLOGY

In addition to providing a powerful suite of analytical tools, the Palantir Platform is designed to be flexible and configurable to meet the legal and ethical requirements of various jurisdictions. This flexibility allows organizations to operate responsibly in nascent and ever-evolving legal regimes. This built-in flexibility allows law enforcement agencies to implement privacy- and civil liberties-protective policies in the context of data analytics, and to adapt their data analytics tools to new requirements as legislatures and courts react to the evolving technological landscape.

Enforcing Access

The Palantir Platform is designed with **robust and granular access controls** that allow LEAs to ensure users are exposed only to the information they need to do their job and are lawfully entitled to see. Access control frameworks can be configured on a data-point-by-data-point basis to precisely match the organizational and data management structure of any LEA.

Source-based access restrictions	Information from law enforcement data sources (e.g., Criminal History Records, Computer-Aided Dispatch Calls for Service, or Automated License Plate Reader data) can be controlled at the property or sub-property/metadata level. For example, general users may be permitted to see non-identifying features of an offense record (e.g., type of offense, date, time), while only supervisors are granted permission to see details identifying the individuals involved as suspects, victims, or witnesses in the recorded event.
Functional access restrictions	Multiple levels of access can be used to restrict the mode of interaction with any given data element. Palantir users can be assigned:
Owner permissions	Allows users to read, edit, and grant access to others
Write permissions	Allows users to read and edit
Read permissions	Allows users only to view or read

Discovery permissions	Allows users to search for matching results, but instead of seeing any actual details of the matching record they are only shown a message providing contact information for the appropriate data owner/controller to contact to request authorized access
No permissions	Does not allow users to search, discover, view or in any other way interact with or identify the existence of a piece of information
Role-based access restrictions	Role-based classifications allow administrators to define groups of users (or individual users) whose particular responsibilities permit them to access certain sets and levels of information. This capability enables LEAs to enforce applicable classification regimes for sensitive or restricted data types (e.g., records related to juveniles, sex offense victims, or other sensitive/vulnerable victims), individual roles and legal authorities, and changing access conditions over time (e.g., access can be terminated automatically at the close of a case, end of a grand jury term, etc.).
Predicate-based access restrictions	Access controls can be further configured to enforce predicate- or justification-based access restrictions for particularly sensitive information. For example, when Automatic License Plate Reader (ALPR) data is integrated in the Palantir Platform for search and analysis, Palantir users accessing this data can be required to provide mandatory, auditable search predicates such as investigation categories and/or a specific case number certifying the particular inquiry has a legitimate purpose. Additional restrictions can be further applied based on these purposes to, for example, limit the geospatial and temporal ranges of ALPR query results returned in accordance with the investigatory parameters.

These access control elements can combine to enable privacy protective compartmentalization of information of different types, while providing a single point of access across many types of users, roles, and responsibilities within a LEA.

Managing Data Retention

LEAs are inundated with data, and they need to be able to quickly identify what is immediately useful, what needs further consideration, and what can be discarded as

irrelevant to an authorized investigation. Furthermore, law enforcement information that is collected and analyzed may not always be permitted to be—or, as a matter of best practices, should not be—held indefinitely.

For example, some federal statutes and regulations (e.g., 28 CFR Part 23, pertaining to multijurisdictional agencies' handling of Criminal Intelligence records) establish rules for the handling and preservation of certain classes of records. Other records types (e.g., ALPR "hits" or Tips and Leads reports) may be governed by state, local, or institutional policies addressing whether and how long information can be retained in data systems.

The Palantir Platform enables LEAs to effectively implement **differential records retention** and **purging standards** for such records. Palantir can be configured to notify data owners when retention deadlines are approaching so that records may be reviewed and asks data owners to confirm deletion actions or (where appropriate) assert justification for continuing to retain the data. Palantir also provides flexibility by supporting different records removal measures, including:

- **Archiving** (i.e., securely locked-down and/or restricted storage of older or more sensitive information);
- **Anonymization and de-identification** of personally identifying records;
- **Soft deletion** (i.e., records deletion in such a way that records retrieval is effectively impossible through front-end user access, but still possible through back-end administrator access if properly authorized and needed, e.g., for redress purposes or investigation of allegations of mishandling); and
- **Hard deletion** (i.e., records deletion of data such that records retrieval is no longer possible via either front-end or back-end methods under any circumstances).

Palantir provides a **consolidated platform for records access using a pointer system** to establish a single authoritative version of each record (as opposed to paper records regimes or other digital records management systems that may replicate records for different user interactions). As a result, all changes, updates, corrections, and other definitive actions are automatically propagated system-wide to all users. Maintaining a single authoritative version of each record ensures that critical records purging is efficiently propagated throughout the enterprise to mitigate the risk of digital records "copies."

Overseeing Use and Ensuring Accountability

LEAs using the Palantir Platform can rely on detailed records of system usage to provide quick and easy, empirically-backed analyses that show exactly how a system is used.

Our technology is engineered to make audit analytics efficient and powerful. The Palantir Platform provides tamper-evident and effectively immutable audit logs that can be configured with extreme specificity to give authorized parties a full view of users' interactions with the system and use of information to which they have access.

But beyond simply generating and storing audit trails, we have worked with our law enforcement customers to provide the analytical tools and capabilities needed to make audit records truly usable. As a result, auditors or other oversight officials with the means to identify and investigate potential misuse or abuse of sensitive law enforcement information to mitigate privacy and civil liberties risks can do so easily and independently of primary users or IT Department assistance.

PRIVACY & CIVIL LIBERTIES ENGINEERING

The continued protection of privacy and civil liberties in the context of new technologies, particularly those that facilitate data analytics on a broad scale, is one of the most important challenges of our time. This challenge raises questions of law, policy, and our shared community values, but also difficult questions about the role that technology can play in increasing accountability and buttressing sound policy.

As a software company focused on solving hard engineering problems and committed to the importance of privacy and civil liberties values, we believe that we are uniquely situated to address these crucial technical questions. We have built a unique **Privacy and Civil Liberties Team** that works with customers to implement the above capabilities and even configure new technologies to meet specific needs.

Beyond our work with our developer and field engineering teams, support customer and community engagement to truly make the above technologies actionable. For example, we work with our customers to provide technical assistance with the drafting of Privacy Impact Assessments of Palantir systems components. We also have extensive experience engaging with our customers, their legal counsel, policy experts, and privacy officers to adapt and refine policies to better align business rules and operating procedures with the realities of current and emerging technologies and to provide firmer grounding for the adoption, configuration, and implementation of the privacy protective technologies provided by Palantir—especially in cases where existing regulations expressed in "paper file" terms do not cleanly translate to the architectures of modern information systems.

To support these initiatives, we draw on the expertise of a formal team of what we call Civil Liberties Engineers (a multi-disciplinary group with backgrounds spanning law, computer science, and philosophy who share a common passion for privacy and civil liberties issues), a prominent advisory board of academic and privacy experts (the Palantir Council of Advisors on Privacy and Civil Liberties), external privacy counsel, and others. We also have a history of actively and constructively engaging with independent review organizations (e.g., the Institute for Intergovernmental Research), policymakers, advocacy groups, and privacy academics to continuously reevaluate and refine our technologies and to identify and build new privacy protective technologies.

We are committed to building, deploying, and maintaining exceptional privacy protective technologies to help our law enforcement customers responsibly serve and protect.