

Privacy and Civil Liberties are in Palantir's DNA

Palantir is a mission-focused company. Our leadership team and founders, composed of California technologists and our allies in DC and beyond, are dedicated to working for the common good and doing what's right — in addition to being deeply passionate about building great software and a successful company.

Palantir was developed by scores of engineers over several years in the wake of the September 11, 2001 terrorist attacks to address the most complex information analysis and security challenges faced by the intelligence, military, and law enforcement communities. Since then, we have realized that our software platform can be applied to virtually any data set requiring complex information analysis, collaboration, and security mandates, including in the fields of cyber defense, regulation and oversight, and healthcare.

Being the best is our passion, and Palantir is quickly developing a reputation as a game changing technology in each of our domains. Yet as our adoption grows, our responsibility to the common good becomes even greater. At Palantir, this means creating technology that reflects our commitment to protecting privacy and civil liberties. That deeply felt commitment has been clear since the company's inception and is evident in the company's roster of advisors, leaders, engineers, and technology experts.

Prioritizing the protection of privacy and civil liberties was a key factor in forming Palantir's Advisory Board. One of the first members of our Advisory Board was Bryan Cunningham, a member of the Markle Foundation Task Force on National Security in the Information Age, a founding Vice Chair of the American Bar Association Cybersecurity and Privacy Task Force, and a published cybersecurity author and media contributor on these issues. Our Advisory Board also includes Michael Hurley, a senior staff member on the 9/11 Commission. Career government officers, Cunningham and Hurley have each served Democratic and Republican Administrations, both while in and out of government, to protect privacy and civil liberties while enhancing information sharing.

Based on guidance from its Advisory Board, Palantir has consistently invested its own funds to ensure that the Palantir platform includes the privacy and civil liberties protections mandated by legal requirements such as those in the 9/11 Commission Implementation Act and recommended by nonpartisan experts such as the Markle Foundation. We believe Palantir is one of the few platforms – if not the only one – that does this across the board.

Putting our values to work, Palantir voluntarily developed new technologies and a rigorous framework to: protect privacy and civil liberties; empower policymakers and administrators to enforce legal, regulatory, and policy requirements; and, equally important, ensure that the implementation of all requirements is audited. Our breakthrough technologies which protect privacy and civil liberties include:

Granular Data Accessibility

The ability of any technology to effectively – and verifiably – ensure that individual users have access to all of, but only, the data that they are authorized to access and use depends upon the degree of granularity at which the technology can tag, track, and control access to the individual data elements. Particularly in the government context, different data often has different requirements in terms of levels of sensitivity, security clearance, and sharing rules and limitations. Application of the rules that govern data access and sharing must be tracked at the most granular data level, including by source and applicable restrictions. For example, Personally Identifiable Information (PII), especially about US Persons, often carries stricter access limitations than non-PII. Similarly, information about a person from one source might have stricter access rules than information about a person from another source. Palantir's ***Access Control Model*** enforces such limitations while enabling the right information to reach the right people at the right time. Additionally, users need the capability to roll back all past edits or deletions of their data to any previous state, which enables effective redress or pursuit of alternative analytic hypotheses. This feat requires a special type of database technology that Palantir developed and calls its ***Revisoning Database***. The Revisoning Database enables a secure and intuitive analysis environment where all edits, updates, and imports/exports are tracked in real-time along with their associated metadata. This is how Palantir satisfies legal requirements and policy recommendations for ***authentication*** and ***access control***.

Thorough and Flexible Core Auditing Capabilities

A thorough and flexible auditing engine, which enables ***real-time and immutable auditing***, must be built into the core of all new information sharing and analysis technologies, and not attached separately as an afterthought. During the analysis lifecycle, the data and user environments often change, new information sources come into play or are found to be inaccurate, and data is combined and disaggregated in myriad ways. Users constantly ask new types of questions, create persistent queries, and initiate other types of automatic studies. Throughout this dynamic lifecycle, a robust and privacy-protective analytic platform requires transparency regarding both who is allowed to access the data and who has in any way

modified, used, or deleted data. To effectively protect privacy and civil liberties while empowering mission performance and resource management, this auditing information should be available through a secure interface to properly authorized individuals only. Additionally, this auditing information should be formatted as easily understandable information and not just stored in cryptic log files that prohibit practical auditing. At the same time, however, at least one set of audit logs must be **immutable**, that is, incapable of being altered, even by system administrators. Real-time and immutable auditing capabilities have been built into Palantir's platform from the start.

Dynamic Access Framework

History teaches that privacy and civil liberties can face their greatest threats during times of crisis. Individuals and organizations faced with an emergency often feel they must immediately make information sharing less controlled. Hindered by legacy technologies, some organizations can see their only option as temporarily abandoning secure and privacy enhancing systems in favor of faster, but less secure and protective, means. Making matters worse, many legacy technologies force this result because they were deliberately engineered to require massive investments in time/money to change their underlying information-handling frameworks, thereby ensuring the companies that created them would have long-term modification and development revenue. Palantir takes the opposite approach. Our platform provides system administrators the ability themselves to continue the use of privacy and civil liberties protective technologies while, as consistent with applicable law and policy, modifying access and related rules in real-time. In a crisis, leaders using Palantir could instantly institute more expansive temporary sharing rules without losing the full framework of protections and auditing capabilities built into Palantir to protect privacy and civil liberties, and without incurring huge additional expense and delay. Palantir's unprecedented flexibility results from a suite of technologies that together enable a dynamic framework for interpreting and implementing access control and other information technology requirements. These technologies also enable seamless collaboration by incorporating ***differentiated access*** and ***selective revelation***. Differentiated access allows individuals to collaborate, but only see the individualized "cut" of the data permitted by the access controls discussed above. Selective revelation requires increasingly strict legal and policy predicates prior to the access or use of increasingly sensitive/intrusive personal information, particularly about Americans.

Palantir was built by technologists serious about protecting privacy and civil liberties. Members of our team have reached out to policymakers to make them aware of these capabilities, and to get their feedback on how we can ensure that these capabilities will be used to protect our citizens. For more information on privacy, civil liberties, and Palantir's systems please contact inquiries@palantirtech.com.

Selected Legal & Regulatory Requirements to Protect Privacy and Civil Liberties

To protect privacy and civil liberties in the context of government action, complex and overlapping legal and regulatory requirements exist to control information sharing. These requirements control information sharing within and between Federal, State, and local government organizations, as well as with the private sector and, importantly, the required technological capabilities for such sharing. Below is a list of some of the requirements that Palantir engineered its technology from the ground up to incorporate.

Selected Legal Requirements

U.S. Federal Statutes

- National Security Act of 1947 (as amended)
- Judiciary Act
- Homeland Security Act
- USA PATRIOT Act
- Intelligence Reform & Terrorism Prevention Act
- 9/11 Commission Implementation Act
- Privacy Act
- Electronic Communications Privacy Act
- Stored Communications Act
- Foreign Intelligence Surveillance Act
- Freedom of Information Act

Other Requirements

- Executive Order 12333 (as amended), and others on Intelligence Activities & Information Sharing
- Required Attorney General-approved intelligence activities implementation regulations
 - CIA: Headquarters Regulation 7-1 (classified)
 - DoD Directive 5240 and others
 - USSID 18
 - AG Guidelines for FBI
 - Other IC members have similar regulations
- Memoranda of Understanding
- Executive Order 12958 (as amended), and others on Classified Information and Freedom of Information
- DNI Privacy & Civil Liberties Guidelines and Implementation Guide
- Intelligence Community Directives (ICDs), including ICD 501

Looking in detail at one of the most important legal authorities in this area, the Intelligence Reform & Terrorism Prevention Act (IRTPA) Section 1016(b)(2) (as amended) requires that Information Sharing Environment (ISE) technology provide a decentralized, distributed, and coordinated environment that, among other requirements:

- (A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;
- (B) ensures direct and continuous online electronic access to information;
- (C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;
- (D) builds upon existing systems capabilities currently in use across the Government;
- (E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
- (F) facilitates the sharing of information at and across all levels of security;
- (G) provides directory services, or the functional equivalent, for locating people and information;
- (H) incorporates protections for individuals' privacy and civil liberties;
- (I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;
- (J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;
- (K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;
- (L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;
- (M) permits analysts to collaborate both independently and in a group (commonly known as 'collective and non-collective collaboration'), and across multiple levels of national security information and controlled unclassified information;
- (N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and
- (O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

Palantir Implements the Markle Foundation Task Force Recommendations

The Markle Foundation Task Force on National Security in the Information Age was formed after September 11, 2001 to determine how best to make information discoverable and accessible to the right officials at the right time to enable improved decision making with regard to major security threats against our nation. The Markle Task Force has been the primary advisory source for many of the technology requirements enacted into law as described above. In March 2009, the Markle Task Force issued a new report to the Obama Administration and Congress entitled “Nation At Risk: Policy Makers Need Better Information to Protect the Country.” Palantir has developed its technology from the ground up to address the types of privacy and civil liberties requirements outlined by the Markle Task Force. The following chart describes how Palantir meets the Markle Task Force technology recommendations.

Markle Task Force Requirement	Palantir Satisfies By
<p>Systematic controls for “authorized use” standard Systematic controls for the implementation of an “authorized use” standard...[by using] technology [that] enables each data object down to the field level, to be tagged, synchronized, and tracked with attributes such as date of change, user’s name, and clearance level, and modifications...[and] source attribution as a data pedigree.</p>	<p>Access Control Model & Revisioning Database Palantir’s Access Control Model allows for securing and sharing of components based on the pedigree and lineage of each element of data. Palantir’s Revisioning Database automatically tracks data pedigree, including date of change, user, security information, and data source information, and enforces any legal, regulatory, or policy requirements for protecting privacy and civil liberties.</p>
<p>Data discoverability Discoverability of data...across national security classification levels, with controllable types of access, from “silent hits” to partial access to full access, and the ability to monitor decisions of a component <i>not to share</i> data.</p>	<p>Access Control Model Palantir’s Access Control Model supports not only “read” and “write” access, but also “discovery” modes. Alerts and “silent hit” capabilities at various levels are built into the software, where silent hits as well as “no sharing” decisions are fully auditable.</p>
<p>Selective revelation of data Access rules allowing individuals to see only data to which they are entitled based on their clearances, role, mission and agency authorities of the entity at which they work... allow[ing] both for different access rules based on individual legal authorities and authorized uses of multiple government entities, and for dynamic revisioning of such access rules.</p>	<p>Access Control Model & Revisioning Database Palantir’s Access Control Model and Revisioning Database allow for granular access based on selected factors, including clearance, role, mission, and agency or individually based privacy and civil liberties protection requirements, and allow for dynamic (real-time) revision of the accesses based on mission, legal, or other factors. Individualized access could be changed, for example, due to a change of threat condition or a temporary emergency.</p>
<p>Anonymization of data Anonymization technology, which permits disparate data holders to create data indices of anonymized data elements. Such forms of “discovery without disclosure” will be useful when the sharing entities are less likely to share otherwise (e.g., classified compartment to compartment, cross-agency, public-private, or even country-to-country).</p>	<p>Dynamic Ontology, Access Control Model & Open Platform Palantir’s Dynamic Ontology allows users to model data in ways that anonymize the underlying data for collaboration. Palantir’s Access Control Model makes it possible to access the sensitive information when (and only when) appropriate. Palantir’s Open Platform design also enables incorporation of any external “anonymization” or de-identification technology, regardless of manufacturer.</p>
<p>Immutable audit trails Immutable audit trails to enable accountability and...to gain certainty on how systems are used. This will ensure that such use complies with policy and law, and will enhance confidence that the audit trail has not been tampered with, even by the database administrator.</p>	<p>Revisioning Database & Audit Logs In addition to the online history enabled by the Revisioning Database, Palantir also creates Immutable Audit Logs. Palantir’s platform can track usage and issue alerts if/when audit logs are improperly accessed.</p>

Markle Task Force Requirement (cont'd)	Palantir Satisfies By (cont'd)
<p>Real-time tracking of analytical activities Real-time tracking of analytical activities to ensure users are engaging the system in a manner consistent with their mission authorities and responsibilities. This audit capability is important for many reasons, including privacy and civil liberties concerns, as well as to meet operational, counterintelligence, and security requirements.</p>	<p>Audit Logs & Usage Analytics In addition to the audit capabilities discussed above, Palantir's open/extensible Usage Analytics product allows management to see how analysts are using Palantir across the enterprise.</p>
<p>Real-time "data tethering" capabilities Real-time "data tethering" capabilities, across federated data sources, to ensure that any information transferred between systems, particularly about individuals, is constantly updated and subjected to correction and redress.</p>	<p>Distributed Search Server Palantir's Distributed Search Server technology tracks the pedigree and lineage of data between and across all department and agency data sources. Not only is all data tracked, but so is the access of information and use and effectiveness of controls. Palantir can accomplish this across all legacy and new hardware and software systems, and with structured and unstructured data.</p>
<p>Identity management and authentication Underpinning these capabilities [is] a robust, enforceable, and fully monitorable identity management and authentication capability, [which has been asserted in the past to be] the principal remaining constraint to full implementation of the Markle Task Force's key recommendations.</p>	<p>Authentication Web Service In addition to the Access Control and other capabilities discussed above, Palantir Authentication Web Service allows the integration of all enterprise authentication sources into one single interface. This capability can be leveraged for Palantir and for all other enterprise services.</p>
<p>Open platform [O]pen platform . . . [foundational technology], so that best-of-breed elements can be selected and integrated.</p>	<p>Open API Palantir follows the Silicon Valley model and builds only open platforms. As such, Palantir integrates with any other software product that provides an interface for data interchange. In addition, we allow customers to extend Palantir itself through our Data APIs, Application APIs and Computer/Cloud Computing APIs.</p>

All intelligence, homeland security, law enforcement, and defense technologies should be carefully evaluated prior to deployment to determine the degree to which they meet the IRTPA and Markle requirements.