AUDIT LOGGING

Palantir's immutable and real-time audit logging technologies help ensure compliance with applicable policies designed to protect privacy and civil liberties. Palantir's audit logs can be configured to capture the information a particular customer requires in order to identify behavior that might indicate misuse of data. Audit logs can record everything from login attempts to specific user search queries to user views of individual records.

A typical view of audit logs – reams of impenetrable data.

All audit logs are only as effective in protecting privacy and civil liberties as the frequency and level of review of them by appropriately authorized officials. However, such review is often complicated by the fact that audit logs consist of row-upon-row of information that can be difficult to analyze, discouraging busy managers from reviewing them regularly.

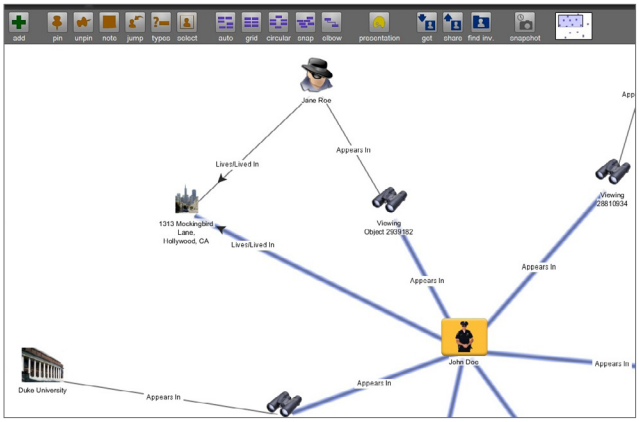
The Palantir Platform solves this problem. Audit log information can be imported into the Palantir Platform where it can then be reviewed using Palantir's various analytic tools. Palantir's unrivaled analytic capabilities then can quickly turn these rows of impenetrable data into actionable intelligence that can identify intentional or inadvertent violations of privacy and civil liberties protective policies.

A view of audit log data in the Palantir Platform, here showing the temporal progression of certain user activities

For example, using the Timeline Helper, a manager can review the daily rhythm of use and quickly identify unusual activity that might indicate misuse of data, whether deliberate or not.

Drilling down into this particular user's activity, the manager can then do a search on the Graph to discover what records this user was viewing during this unusual activity.

In cases where the manager not only is working with the audit log information but also has been given access by administrators to the underlying data set, the manager can search for common links between the records viewed and the user. In this case, we see that one of the individuals at one time shared a common address with the user. This may be an indication that the user is inappropriately monitoring the activity of a significant other.



An analysis on the Graph of the audited activities of a particular user, connecting one particular record subject to the same address as a user.

Using Palantir, an investigator is able to quickly sift through large amounts of auditing data, identify suspicious activity, and drill down into that activity to determine whether there may have been a violation of law or policy.