
# Google Apps Security For Lawyers: Premier Edition Only

***July 15, 2010***

I must confess I never much researched Google Apps' security provisions. I just assumed that, as a product designed for the general public's ease of use, they were minimal at best and that any data passing through gmail or google docs was unsecured. In other words, I never used them for professional purposes.

Turns out, I was only half right. The good news: Google employs significant security provisions for its apps suite, but only for their **Premier edition**, i.e., the one that costs money. So for lawyers using Google apps for communication, collaboration and document storage, beware: if you're using the standard edition, your data is unprotected.

Google Premier Apps consists of:

- **Gmail** includes email, IM, voice and video chat, and syncs with Outlook and Blackberry.

- The **calendar** is integrated with your gmail system, can be shared through the groups function and syncs with Blackberry.

- **Documents** includes spreadsheets, drawings and presentations and are easily shared for collaboration.

- Google **Sites** is an easy way to create secure web pages for intranets and team projects. No coding or HTML is required.

- Google **Groups** can be used as mailing lists and to share calendars, docs, sites, and videos easily with co-workers.

- Google hosts your **videos**, creating an channel for your business that can be used either through your intranet or shared on the web.

- Last, **wave** enables groups to discuss issues or projects in written format, where each participant's written contribution shows up in real time.

- Here are the highlights of Google's security policies:

- Google adheres to the United States Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce's Safe Harbor Program.

- Google has obtained a SAS 70 Type II attestation and will continue to seek similar attestation for the Google Apps messaging and collaboration products as well as for our security and compliance products, powered by Postini. A SAS 70 audit is an independent assessment by an outside audit firm that validates the subject company's adherence to its defined controls and confirms that these controls are operating e!ectively. When complete, the audit firm provides a report that details the company's compliance with these controls.

- Google will not share data with others except as noted in the Google Privacy Policy.

- Google provides capabilities for customers to take data with them if they choose to use external services in conjunction with Google Apps or stop using Google services altogether.

- Some user data, such as email messages and documents, are scanned and indexed so users within a customer's domain can search for information in their own Google Apps accounts.

- Email is scanned so Google can perform spam filtering and virus detection.

- Email is scanned so Google can display contextually relevant advertising in some circumstances.

- Except when users choose to publish information publicly, Google Apps data is not part of the general google.com index.

- Google offers these additional customized security controls:

- Single Sign-On (SSO) service to customers with Premier, Education, and Partner Editions. Google Apps has a SAML-based SSO API that administrators can integrate into their LDAP, or other SSO system. This feature allows administrators to utilize the authentication mechanism of their choice, such as certificates, hardware tokens, biometrics, and other options.

- Administrators can set password length requirements for their domain users and view password strength indicators that help identify passwords that meet the length requirement but may still not be strong enough.

- Administrators can reset a user's sign-in cookies to help prevent unauthorized access to their account. This will log out that user from all current web browser sessions and require new authentication the next time that user tries to access Google Apps. Combined with the existing ability for administrators to reset user passwords, this feature to reset users' sign-in cookies improves security in the cloud in case of device theft or loss.

- Google Apps Premier and Education Editions offer domain administrators the ability to force all users in their domain to use Hypertext Transfer Protocol Secure (HTTPS) for services such as Gmail, Docs, Calendar, Sites, etc. Information sent via HTTPS is encrypted from the time it leaves Google until it is received by the recipients' computer.

- With policy-enforced Transfer Layer Security (TLS) for Simple Mail Transfer Protocol (SMTP), administrators can set up policies designed for securely sending and receiving mail between specific domains. For example, an administrator could specify that all external mail sent by their accounting team members to their bank must be secured with TLS — or deferred if TLS is not possible. Similarly, an administrator could mandate a secure TLS connection between their domain and their outside legal counsel, auditors, or any other partners with whom employees may trade sensitive communications.

While the security measures offered by Google are significant, there are still two issues of concern that remain. First, Google operates on a multi-tenant cloud platform, which means that your data resides on shared server space with any other Google cloud users. While this is a fairly common practice among cloud vendors, it is not the configuration of choice for lawyers trying to control their data, even if off-premises. It is better to choose a vendor who stores each customer's data on a single server.

More importantly, Google will not reveal (to you and presumably anyone else) the geographic location of your data, and it can be transferred from one server to another at any time. This gives rise to jurisdictional issues, since the site where data is located when a cause of action arises may be difficult to determine. It also renders your data subject to the laws and regulations of the geographic location of your data, which vary Since Google has servers around the world, this could be problematic should a breach ever occur.

If you're a Google Apps user, be sure to subscribe to their Premier Edition to be certain you are meeting your ethical obligations regarding confidentiality and privacy. Better choice: find an Saas vendor whose products are designed for attorney communication and document storage to avoid the multi-tenant and jurisdictional issues. In any case, be sure to do your due diligence regarding any vendor's security and privacy policies.