B27 Google™ Dual-Factor Authentication (2-Step Verification) and Its Impact on Cloud Data Collections

Jason M. Paroff, JD, 90 Park Avenue, 8th Fl, New York, NY 10016; and Jonathan Kessler*, 91 Hanrahan Avenue, Farmingville, NY 11738*

After attending this presentation, attendees will understand the recent move toward dual-factor authentication by online service providers such as Google™ to offer increased data/information security to its users, and the impact this can have on forensic data collections carried out in connection with litigation (which are often done by 3rd parties such as law enforcement officers or private practitioners hired to accomplish the same). Attendees will learn, as an example, how Google™ implements this technology, and what they will need to do in order to accomplish forensic data collections from Google™ when necessary for either civil or criminal litigation.

This presentation will impact the forensic science community by introducing this new and lesser-known technology, explaining various aspects of its implementation, and providing methods to properly address it so that forensic data collections can take place more quickly and smoothly than would otherwise be the case.

Recent security changes implemented by online data service providers such as Google™ have resulted in some changes to the way information must be accessed, collected and verified from Gmail accounts, and mail accounts hosted through Google™ Apps (http://www.google.com/enterprise/apps/business/). In order to avoid collection delays and frustrations, law enforcement officers and companies should prepare themselves ahead of time for dealing with these issues during a collection.

There are two relatively new security measures implemented by Google™, and accompanying best practices, that are important to be familiar with. The first is the use of Verification Codes.

In order to increase security, Google™ sometimes requests a verification code when a user attempts to access a Gmail account from a browser or machine that has not previously accessed an account. Without the verification code, the account cannot be accessed. Verification codes can only be obtained by the account holder in certain ways (e.g., a text message sent by Google™ to a pre-configured cell phone; via an application called "Google™ Authenticator," etc.).

Part of the collection process typically involves logging into the email account through a browser to verify message counts and other information, which may prompt a Google™ request for a verification code. To speed collection times, it is important to: (1) be aware of any users with mobile devices linked to such cloud accounts for the purpose of retrieving or generating verification codes; (2) provide the collections team with access to these users and their mobile devices as necessary; and, (3) alert these users that a collection will be occurring, and ask them to be ready to provide verification codes during the collection. Valid verification codes change every 30 seconds, so collection teams must work with these users in real time.

The second relatively new security measure implemented by Google is the use of 2-step verification. If a user or organization has chosen to enable 2-step verification for their Gmail or Google Apps accounts, collection teams will both need to obtain a verification code as noted above, and obtain an "application specific password" for any tool (e.g., Microsoft® Outlook) used to access the account that does not do so through the use of a browser. The application specific password can only be generated by the custodian or the account administrator. To speed collections when two-step verification is enabled, it is important to: (1) allay privacy concerns with custodians before the collection begins; and, (2) prepare custodians or account administrators for the process that generating the application specific passwords will take.

Collecting data from the cloud isn't as easy as it may seem to many attorneys, judges and others involved in litigation who may make such requests. Enhanced security features like those implemented by Google have the potential to delay forensic collections. With a little preparation however, law enforcement officers, legal and IT teams can ease administrative headaches and overcome obstacles to a successful collection.

Google™, Authentication, Data Collection

 ** Presenting Author*