

Info Gathering In The Google Age: Notes On The SCA

Law360, New York (February 10, 2012, 4:43 PM ET) -- With much fanfare, and with more than a little criticism from privacy advocates, Google Inc. recently announced the update of its privacy policies and terms of service. Specifically, Google announced that users who sign in to their Google accounts for email and other services should expect that Google will “combine” the information being gathered by all of its various services.

For example, under Google’s new policies, users with Google accounts have been advised that their Internet searches will henceforth be informed by the specific terms and content of their prior searches. Likewise, advertisements will be tailored to suit individual users based on their prior searches and other user information.

Critics of these new policies have emphasized the privacy concerns inherent in Google’s stated willingness to link search information, embedded terms and other data across platforms to particular users — a capacity that may have existed previously but was not fully realized. Proponents have emphasized that the features will only enhance the appeal of systems that Google’s users have come to rely upon, and that in any event these changes will only apply to those users who are willing to log in to established accounts in the first place.

This debate is likely to continue. Regardless of its outcome, however, the focus on Google and the ever-increasing mosaic of data being gathered by search engines and electronic service providers highlights the increasing relevance of a vestige of the pre-Internet Age that most computer users have never heard of: the Stored Communications Act, 18 U.S.C. §§ 2701-12.

Enacted in 1986 as part of the Electronic Communications Privacy Act, the SCA originally was intended to create additional protections for owners of electronic data given the increasing use of third-party vendors for data storage and electronic communications services. In practice, it is easier for law enforcement to obtain most private communications and other electronic content under the SCA than to obtain a warrant for more traditional correspondence or papers.

Under the SCA, strict restrictions (and penalties) are imposed on private parties’ disclosure of electronic information, subject to a few narrow exceptions. Notably, under the SCA, civil litigants cannot obtain electronic mail or other “content” information from electronic communications services or remote computing services, even pursuant to civil subpoenas (which Google routinely challenges). By contrast, the SCA does not impose an absolute bar on civil litigants’ ability to obtain basic subscriber and noncontent information pursuant to subpoena.

However, similar strictures do not apply in a law enforcement context — where the SCA actually makes it easier for prosecutors to seize user communications and data. Here, the SCA creates a sliding scale of restrictions that varies depending on the type of information being requested. At the more restrictive end of the spectrum, the SCA requires the government to obtain a search warrant to obtain unopened electronic communications that have been held in storage for less than 180 days.

However, unopened emails that have been held in storage for more than 180 days, or (according to some courts) retrieved communications, may be accessed without a warrant, provided that the government first issues a subpoena with notice or obtains a court order under Section 2703(d) (sometimes referred to as a “d” order) based on a showing that there are “reasonable grounds to believe” that the information being sought is material to an ongoing investigation — a lesser showing than would be required under the Fourth Amendment.

Other information requires even less of a showing. Indeed, while searches using Google or other services arguably encompass protected “content” under the SCA, the government has taken the position in prior litigation that logs kept by search engines are not protected at all under the SCA.

In practice, because browsing the Internet as we now know it was not really possible in 1986, the SCA reads like a crazy quilt of rules and confusing standards that do not perfectly align with the reality of today’s computer user. For example, emails are treated differently depending on whether they reside on a user’s home computer, a corporate server or a server hosted by Google.

The SCA also makes a distinction between new and older emails that makes little sense today. Surely, the typical computer user’s expectation of privacy in his or her emails does not decrease simply because the email has been read or is more than 180 days old. Indeed, it seems counterintuitive to grant greater protection to new, unopened email spam than to purposefully archived emails.

More fundamentally, an important 2010 ruling by the Sixth Circuit in *U.S. v. Warshak* called into question the SCA’s allowance of government access to electronic information without a warrant, given that the privacy interests at issue here are the same wherever a communication is located, and whether an email is old, new or unopened. However, it is too early to tell whether that ruling signals the beginning of a larger trend toward greater privacy protections.

All of which brings us back to Google. Linking different categories of information — searches, websites logged, email and other content — back to the individual end user obviously holds great appeal to Google as a mechanism for tailoring future services and advertisements to customer preferences. It also offers real value to users. But those same attractions likewise make this information an even more appealing resource for law enforcement or others under the SCA. There already has been a fair amount of litigation concerning the discoverability of email. It is reasonable to expect further fights specific to the other types of content that Google is now compiling for its users.

--By Stephen M. Juris, Morvillo Abramowitz Grand Iason Anello & Bohrer PC

Stephen Juris is a partner in Morvillo Abramowitz's New York office, where he focuses principally on white collar defense and governmental investigations, regulatory enforcement matters, and complex commercial litigation.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.