Google's Privacy Policy: What Would be the Real Impact of APEC?

November 2007

On September 14, Peter Fleischer, Google's Global Privacy Counsel, called for the creation of international standards for internet privacy that would "meet the expectations and demands of consumers, businesses, and governments," and endorsed the Asian Pacific Economic Cooperation (APEC) framework.

After taking recent hits in the press about its desired merger with online marketing company, DoubleClick, and being ranked by Privacy International as the worst major Internet company in terms of consumer privacy, the positive news coverage about Google resulting from the APEC endorsement announcement was likely a pleasant change of pace for the company.

According to Google, it has endorsed APEC's framework because it balances the need to facilitate e-commerce with definable and workable privacy protections for the individual. However, it is important to dig deeper and analyze the APEC standards to determine whether this framework contains adequate safeguards for privacy and is ultimately a good roadmap for international privacy standards.

APEC defines personal information and centers on nine principles:

1) preventing harm;
2) notice;
3) collection limitations;
4) uses of personal information;
5) choice;
6) integrity of personal information;
7) security safeguards;
8) access and correction;
9) accountability.

The following is an analysis of the APEC standards and the impact that these standards might play in alleviating the privacy concerns posed by some Google services.

Definition of Personal Information

APEC broadly defines personal information as information that can be used to identify an individual, as well as "information…when put together with other information would identify an individual."(APEC at 5). However, it explicitly states that its framework does not apply to personal information that a user stores for "personal, family or household purposes."(APEC at 6). Specifically, address books, phone lists or family newsletters are not included as protected information under APEC.

However, addresses, phone numbers and other personal information are precisely the kinds of data that current Google users often store in Google programs. For example, contact lists stored in Gmail, entries in Google Calendar, and addresses in Google Checkout may fall outside of APEC's framework. As a result, APEC fails to adequately encompass and protect the typical Google user's personal information.

Principle I: Preventing Harm

In its first principle, preventing harm, APEC states that privacy protection "should be designed to prevent the misuse of information." Unlike policy frameworks such as Canadian privacy law, which stipulate that unauthorized collection, use or disclosure is a per se violation and do not require evidence of harm to establish a privacy violation, APEC allocates the burden on consumers to show that they have been harmed by a company's privacy policy.

The first principle also sets out a vague standard for remedial measures if a consumer is able to surmount its burden and show that harm has occurred. APEC states that "remedial measures should be proportionate to the likelihood and severity of the harm" of misuse. (APEC at 11). However, APEC offers no real world examples of how proportionality would be formulated.

Principle II: Notice

According to its notice principle, APEC requires data controllers, like Google, to inform users of clear policies on "what information is collected about them and for what purpose it is to be used." (APEC at 12). Since Google currently does not provide its user's with a comprehensive privacy policy, this principle may help to inform users of Google's practices.

Through its broad range of services, Google retains an unprecedented array of personal information from users who take advantage of features like Google Maps, Gmail, Google Video, Google Talk, Google Reader, Google Calendar, Google Checkout, Blogger, and Orkut. Generally, when an account holder uses these programs, Google is

able to retain personal information about the user and their search requests, including information on the user's finances, sexual orientation, political affiliations and health.

Users are not informed that Google retains their personal data for an indefinite period of time, without limitations on disclosure or subsequent use of the information. Further, users do not have the ability to delete or withdraw personal information upon termination of services. In other words, what you do on these programs and what you say will be retained and perhaps used in a variety of ways and you have absolutely no notice or choice in the matter.

For example, Google's social networking program, Orkut, retains records of users' employment, address, phone number, hobbies and user profile, long after the user has terminated their account. Additionally, when users enter searches through Google Toolbar, Google collects all search results and identifies all Google Toolbar users with a unique cookie that enables Google to track the user's subsequent movement on the web.

Unfortunately, APEC's notice requirement would accomplish only trivial changes in Google's current practices, since it stipulates that notice is effective if it is given either before or at the time that personal information is collected. (APEC at 12). "At the time" notice is ineffective since it does not allow users to object before data is collected. As a result, "at the time" notice cannot possibly constitute a meaningful form of consent. This is especially true when contrasted against the requirement of knowing consent imposed by OECD guidelines.

In response to criticism of its lack of privacy safeguards, Google recently proposed to delete records of search strings ("cookies") within 18 months. Soon after, other search engines, like Microsoft, Yahoo and AOL, resolved to do the same. In fact, Ask.com has even proposed an option that would allow users to prevent it from recording search terms and IP addresses. However, Google still has yet to provide its users with the ability to opt out of data retention or to expunge cookies. Furthermore, if a Google user returns to a site within 18 months of their last visit, the cookie automatically renews.

APEC's notice requirement also dodges the issues that cookies pose. In fact, APEC specifically provides that "there are circumstances in which it would not be practicable to give notice at or before the time of collection, such as in some cases where electronic technology automatically collects information when a prospective customer initiates contact, as is often the case with the use of cookies." (APEC at 12-13)

Principle III: Collection Limitation

Principle three only addresses limitations to collecting data by providing that personal information should be collected "where appropriate, with notice to or consent of, the individual concerned." (APEC at 15). This provision is not actually a limitation on how much data can be collected, but rather a provision that a consumer has to be notified. And with notification possibly occurring "at the time" it is not clear that consumers

would have notice. Therefore, APEC would have little impact on Google's current practices of collecting a large amount of information about consumers.

Principle IV: Uses of Personal Information

APEC provides that personal information may be used with consent of the individual, by authority of law or when necessary to provide a service or product requested by the individual. This principle is somewhat broader than the OECD guidelines, which require consent or authority of law.

This principle may have a very limited impact on stemming broad use of personal information because consumers often unwittingly consent through terms buried in click-wrap agreements or privacy policies included on the sites. Further, the additional provision in APEC that provides for the use of personal information "when necessary to provide a service or product requested by the individual" may also continue to allow Google and other companies to use personal information in a wide variety of circumstances. The APEC standards appear to leave it up to the company to decide when the use of personal information about that individual is "necessary" to provide that service or product. Therefore, whenever an individual requested a service or product, the company could contend that the use of personal information was "necessary" to provide that product or service.

Principle V: Choice

On user choice in collection of data, principle five requires that users be given clear and accessible "mechanisms to exercise choice." (APEC at 17). However, choice is only required "where appropriate." Further, it is unclear to who "appropriate" refers to—does the company determine when choice is appropriate or does the individual decide? While privacy groups have urged Google to provide users with the ability to opt out of data retention, principle five only vaguely addresses when choice could be exercised.

Principle VI: Integrity of Personal Information

Principle six provides that "personal information should be accurate, complete and up-to-date to the extent necessary for the purposes of use." (APEC at 20). This provision is important since individuals may be harmed by use of inaccurate personal information. For example, an individual may not be able to purchase goods online if their credit history is damaged by use of inaccurate personal information. However, this provision imposes an obligation to keep personal information accurate "to the extent necessary for the purposes of use." Like other APEC provisions, it fails to define or provide examples of when it would be "necessary" to maintain accurate information.

Principle VII: Security Safeguards

Principle seven requires that information controllers, like Google, establish reasonable security safeguards that are proportional to the likelihood and severity of

harm. (APEC at 21). However, APEC fails to give an example of how to achieve proportionality and it does not define what constitutes "reasonable" safeguards and thus, provides little structure for Google or other companies to improve their security safeguards.

Principle VIII: Access and Correction

Principle eight begins to address user access to personal information. Although it recognizes access as "a central aspect of privacy" it also states that access is not an absolute right. (APEC at 22) In addition, APEC does not require users to be given direct access to their personal information. In fact, it provides that in some circumstances direct access should be precluded. Under principle eight, Google would not be required to give users access to all of their personal information. Nor would users have the right to be informed of what uses have been made of their data and to whom it has been disclosed.

Principle IX: Accountability

Principle nine establishes accountability for the entity tasked with controlling the disclosure and sharing of personal information. Specifically, if the information controller transfers personal information to a third party, it should obtain consent from the individual "or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."

Because of its massive market share and range of services, Google has a unique ability to share extracted data between these services and know the minutiae of a user's life and personal choices. The potential merger with DoubleClick appears to only exacerbate these concerns since the merged company would amount an even larger pool of information with potentially fewer protections.

Conclusion

APEC may do little to alleviate the privacy concerns with Google practices, or those of similar companies. One of APEC's primary flaws is that it sets no limits on data retention. Generally, APEC fails to establish a basic rules requiring consent for collection, use or disclosure. Overall, APEC is far less comprehensive than EU and OECD policies. Greater accommodation to the aims of business and law enforcement to collect information may be precisely why Google favors this framework.

Google plans to continue campaigning its adoption of APEC standards in Washington and internationally. It will also launch a public debate on YouTube.