

June 20, 2006

Chris A. Vein
Executive Director and Chief Information Officer
Department of Telecommunications and Information Services
City & County of San Francisco
875 Stevenson Street, 5th Floor
San Francisco, California 94103-0948

Re: Privacy and the San Francisco municipal WiFi initiative

Dear Mr. Vein:

This letter is in response to your request for more information with regard to issues raised in the April 19, 2006 letter to you from the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF), and American Civil Liberties Union (ACLU). Google shares these organizations' commitment to online privacy, and to providing consumers with clear notice and choice about their privacy and security. We are happy to have the opportunity to explain further how we will meet these aims while providing free, reliable, and city-wide wireless Internet service to the city of San Francisco. In short, our proposed WiFi service will embody standards of privacy higher than those of major access networks in existence today.

The April 19 letter laid out five points regarding privacy practices for the WiFi service. We address each of these points in turn.

(1) Log-In.

The EPIC/EFF/ACLU letter urges the city to "ensure that individuals can use the free service without 'signing in.'" As described in our RFP with Earthlink, Google's plan for the free wireless service would require users to sign in to the network with a Google Account.

Minimal Registration. When a user creates a Google Account (if she does not already have one), Google asks for a username and password, which the user may then use to log in to Google WiFi for access to the free service. Users may provide any email address to create their Google Account username. Compared to existing Internet Service Providers (ISPs), which often require a user's name, address, telephone number, credit card information, or wireless service providers, which sometimes require credit checks, Google's proposed free service would require minimal information for account registration.

Information Collected. As described in the RFP, Google WiFi will not store the content of users' online communications or data transfers. As proposed, Google WiFi will collect information about account usage, such as when a particular username has signed in to Google WiFi and the frequency and size of its data transfers. Google also may use the locations of the nodes through which a customer connects to Google WiFi to provide information relevant to those locations.

When logged into Google WiFi, users will be able to visit any web page and use email, chat, or other services — Google's or any other providers' — of their choice. If users choose to use a Google service while logged into Google WiFi, the privacy notice of that service will describe how Google collects information with regard to that service, and provide users with choices about privacy specific to that

service. Google employees will not access the content of any communications users send or receive, except under the limited circumstances described in the Google Privacy Policy.

Temporary Storage. On a regular basis — every 180 days, if not more frequently — Google will delete the WiFi account usage information (described above) associated with a Google Account. Google WiFi may retain only aggregate, non-personally identifiable statistics about use of the network beyond that period. The significance of this policy is straight-forward but is worth emphasizing: with both privacy and operational considerations in mind, Google will keep the account session information described in the preceding paragraph only temporarily. As EPIC, the EFF, and the ACLU noted in their previous letter to you (October 19, 2005): “[R]educing the amount of time that the system stores user and transactional data will enhance privacy”

Abuse Prevention. The aim of Google’s sign-in requirement is to help prevent and correct abuses of a free, distributed network used by potentially hundreds of thousands of consumers. The log-in is designed to help reduce the kinds of abuses that cannot readily be kept in check without some form of authentication: the distribution of malware and viruses, for example. Authentication will also help further reduce the kinds of abuses that can be limited — though not completely — through technological means, such as the limiting of computer ports used to send spam.

Choice. Google WiFi users will enjoy a range of choices with respect to their Google WiFi account information. They may create and use different Google Accounts to access the network or separate Google services, such as Gmail. When logged into Google WiFi, users will be able to visit any web page and use email, chat, or other services — Google’s or any other providers’ — of their choice. If users choose to use a Google service while logged into Google WiFi, the privacy notice of that service will describe how Google collects information with regard to that service, and provide users with choices about privacy specific to that service. Users may choose to edit or cancel their Google Accounts at any time. Also, as described on page 153 of the RFP, Google will encourage users to use Virtual Private Networks (VPN) — whether offered by Google or any third-party — to help protect their security. Finally, users may, of course, choose to use a service other than Google WiFi to access the Internet.

(2) Information Sharing.

The EPIC/EFF/ACLU letter also urges the city of San Francisco to ensure that Google will “not share personal information without first obtaining voluntary, affirmative consent from the user.” The letter asserts that Google “reserve[s] the ability to sell user information to others based on an opt-out model” and that “under such a scheme, the company will be default sell information unless the user takes affirmative steps to prevent the sale.”

This statement does not reflect the intended practice of Google WiFi with respect to the sharing of personal information. In the event that our position on this point was unclear before, we should take the opportunity to restate a point made on page 147 of the Earthlnk/Google RFP and the Google Privacy Policy (<http://www.google.com/privacy.html>):

“Google shares personal information with other companies or individuals outside of Google in the following limited circumstances:

We have your [the user’s] consent. We require opt-in consent for the sharing of any sensitive personal information.

We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Policy and any other appropriate confidentiality and security measures.

We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law.”

Google will only share users' personal information with third parties under these narrow circumstances. It is our policy and practice to provide clear notice to our users and give them meaningful choices about the use of their personal information.

(3) Legal requests for information

The EPIC/EFF/ACLU letter urges the city of San Francisco to ensure that Google “agrees to fair procedures for addressing legal requests for personal information. Such procedures would include notice to the individual before personal information is released to others.”

Google's position on this point can be stated succinctly. In civil matters, it is Google's policy to provide notice to users before personal information is released. The same is also true in criminal matters, unless law enforcement officials have represented that such notice would impede an investigation in progress.

(4) Routine erasure of non-essential data

The EPIC/EFF/ACLU letter urged the city of San Francisco to “ensure that Earthlink adopts a data retention schedule that routinely erases non-essential data.” Google cannot speak to Earthlink's policies on this point. With respect to the free Google WiFi portion of the service, as stated above and in the RFP, Google will on a regular basis (< 180 days) delete information associated with Google WiFi accounts and their use of the network.

(5) Law enforcement tools.

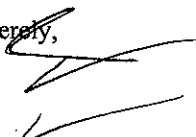
Finally, the EPIC/EFF/ACLU letter urges the city of San Francisco to “ensure that cameras and automated enforcement tools are used only for extremely narrowly-defined purposes, and that strict access and privacy policies are implemented and enforced.”

Google recognizes the difficulty of balancing individual privacy and legitimate law enforcement needs. That said, Google has no plans to offer camera or other surveillance tools for law enforcement in its WiFi network. In our view, any plans by the City to use a WiFi network for such purposes — whether a Google network or any other — would demand a rigorous privacy impact assessment.

Conclusion

We hope that these points alleviate the concerns and clarify any misunderstandings raised in the EPIC/EFF/ACLU letter of April 19 — or in the municipal WiFi process as a whole. We look forward to answering any further questions you may have about Google WiFi — and to providing all of San Francisco with this innovative service.

Sincerely,



Christopher Sacca
Head of Special Initiatives
Google Inc.