

[BY EMAIL (techconnect@sfgov.org)]

April 19, 2006

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

Re: TechConnect RFP 2005-19; Earthlink / Google and Privacy

Dear Mr. Vein,

The selection of Earthlink / Google as a provider for municipal broadband access in San Francisco raises privacy issues. Google proposes to subsidize public Internet access by serving targeted advertisements to users. Users have no ability to opt out of this targeting. They have to provide an email address to sign in, thus allowing Google to track individuals uniquely across sessions of Internet use. Google follows an opt-out model for disclosing individuals' information to third parties.

Earthlink discloses subscribers' personal information for marketing purposes, and engages in "enhancement," the purchasing of additional personal information on individuals without their knowledge or consent. Earthlink also partners with online profiling company Doubleclick.

In addition, the Earthlink / Google proposal seeks to create a surveillance infrastructure for San Francisco by allowing greater deployment of video cameras and automated enforcement tools, such as parking meters.

In this letter, we urge you to negotiate terms with Earthlink / Google in order to establish reasonable privacy rights for users of this network. Specifically, we urge you to:

- Ensure that individuals can use the free service without "signing in."
- Ensure that both companies do not share personal information without first obtaining voluntary, affirmative consent from the user.
- Ensure that Earthlink / 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.
- Ensure that Earthlink adopts a data retention schedule that routinely erases non-essential data.
- Ensure that cameras and automated enforcement tools are used only for extremely narrowly-defined purposes, and that strict use, access and privacy policies are implemented and enforced.

Background

On October 19, 2005, the ACLU of Northern California, Electronic Frontier Foundation (EFF), and Electronic Privacy Information Center (EPIC) submitted comments to TechConnect concerning privacy issues raised by municipal broadband access.¹ In that letter, we raised a series of privacy issues that sought to focus attention on whether users of the municipal broadband network will have secure and private access to the Internet. We applaud TechConnect for including the privacy issues we raised in RFP 2005-19.

On February 21, 2006, we stressed that the city should consider minimum standards for the privacy issues raised by the RFP. We argued that privacy notices are not enough and that minimum standards are necessary for each of the privacy questions posed to proposers in order to guarantee respect for users' rights. We proposed a series of standards for a privacy-friendly network.

On April 3, 2006, EPIC and EFF provided a privacy analysis of the six proposals to provide the city with municipal broadband. One provider was compliant with the standards proposed in the February 21 letter. None of the remaining five proposals satisfied even half of the standards.

On April 5, 2006, San Francisco TechConnect ranked the Earthlink / Google proposal as the most advantageous to the city. The Earthlink / Google proposal performed relatively poorly on privacy metrics specified in our February 21st letter.

We believe that the Earthlink / Google proposal can be improved so that its users are afforded reasonable privacy rights. We urge the city to negotiate for such heightened privacy protections.

Heightened Privacy Protections

Ensure that individuals can use the free service without "signing in."

Under the Earthlink / Google proposal, those who wish to use the advertising-supported service must register, and then sign in every time they wish to use the service. This sign-in requirement creates the opportunity for Google to track individuals uniquely across sessions. Profiles can be built, and access logs maintained that will invite law enforcement and others to request individuals' information.

There is no way to choose not to be profiled by Google under the company's proposal. Fundamentally, the Google profiling is non-consensual, because in order to use the service, one must sign in and be tracked by the company.

¹ Letter from Nicole A. Ozer, Technology and Civil Liberties Policy Director, ACLU of Northern California; Kurt Opsahl, Staff Attorney, EFF; & Chris Jay Hoofnagle, Senior Counsel, EPIC West Coast Office, to San Francisco TechConnect, Oct. 19, 2005, available at <http://epic.org/privacy/internet/sfws10.19.05.html> and attached as Appendix A.

Privacy is an inalienable right under the California State Constitution. As an inalienable right, a citizen's privacy is not to be bought, sold, or bargained away, not even for advertising-supported "broadband." We therefore urge the City to negotiate an agreement with Google that allows individuals to use the service without signing in. Those who find value in targeted advertisements could be free to sign in if they wished, and thus opt-in to the profiling. But those concerned about privacy and the ability to visit websites without being targeted for content-related advertising would be free to browse with anonymity.

Ensure that both companies do not share personal information without first obtaining voluntary, affirmative consent from the user.

Both Earthlink and Google reserve the ability to sell user information to others based on an opt-out model. Under such a scheme, the company will by default sell information unless the user takes affirmative steps to prevent the sale.

Opt-out is not an acceptable model for information selling. Because it is in the financial interest of companies to sell users' information, they tend to adopt opt-out policies that are hard to employ. It is simple for a company to erect barriers to opting out--they can require excess authentication to express the choice or they can hide the opt-out mechanism from the user.

We believe that opt-in should be the standard for information sharing. Opt-in places the burden on the provider to convince individuals that sharing their information is in their interest. It allows the provider to make the case for information sharing, and to make privacy interfaces more user-friendly and less opaque.

We therefore urge the City to negotiate an agreement with Earthlink / Google to only use opt-in policies for the sharing, rental, or sale of personal information.

Ensure that Earthlink / 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.

As we noted in our October 2005 letter, service providers face legal pressures from other network users, industries, and governments to disclose personal information. There should be a process that fairly resolves these requests for information. We believe that the provider should follow the standard set by the Cable Communications Policy Act of 1984 (47 USC § 551). That act, which also applies to satellite television providers, specifies a procedure where individuals are notified before their information is revealed to others pursuant to legal process. It was passed to protect individuals' television viewing habits from disclosure, information that is at least as sensitive as e-mail and web browsing records. It has been in effect since 1984, and accordingly many companies have processes to comply with its standards.

We therefore urge the City to negotiate an agreement with the providers specifying that they will comply with the Cable Communications Policy Act procedures. Except in circumstances where law enforcement presents a court order binding the service provider to secrecy, the service provider should inform the user of the request as soon as possible, and, in any event, the service provider should be prepared to litigate to avoid disclosing data if the request is legally insufficient.

Ensure that Earthlink adopts a data retention schedule that routinely erases non-essential data.

As mentioned above, service providers can be the focus of extraordinary requests for users' data. As an intermediary, a service provider finds itself in a position to collect and store detailed information about its users and their online activities that may be of great interest to third parties. Reducing the amount of time that the system stores user and transactional data will enhance privacy and reduce the costs and burdens of responding to requests for user data.

In its proposal, Google specified that it will limit its data retention to no longer than 180 days, but Earthlink did not make a similar commitment. We urge the City to negotiate an agreement with Earthlink to create a data retention schedule that maintains data only for so long as necessary for operation of the network.

Furthermore, we urge the City to ensure that both providers adopt procedures along the lines of EFF's "Best Practices for Online Service Providers," which describes legal policies and technical procedures for protecting privacy.² Clear policies will conserve resources, help safeguard private data, and preserve freedom of expression online.

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.

The Google / Earthlink proposal declares itself capable of supporting public video surveillance on the wireless network. Use of the wireless network for the transmission of public surveillance data poses extraordinary risks for both the people of San Francisco and for the City. The City should not link public video surveillance cameras to the wireless network.

The security of the entire wireless network is extremely important. However, the security of video surveillance transmissions requires an even higher standard of care. It is being relied upon by law enforcement, and innocent individuals who are simply walking down the street in San Francisco are not choosing for their images and information to be transmitted in this manner.

² These guidelines were developed by technical and legal experts for service providers that wish to handle user data ethically. They are available at <http://www.eff.org/osp/>.

An insecure video surveillance system is dangerous on many levels. Bad actors could intercept the information and store or manipulate the data to modify the camera image, or use the data to target women and children, people of color, and members of the lesbian and gay community. Stolen camera data could also be used to blackmail individuals, or for identity theft. Significant questions about liability would be raised if someone were harmed in one of these ways due to a breach of the security of the City's wireless system.

The City is currently lacking any legally enforceable standards for its current video surveillance program, including how the cameras are used, how long the surveillance footage is retained, and who can access the information. The City should not consider an even broader and much less secure public surveillance system without properly addressing the privacy and security concerns.

Conclusion

Below, we have attached the Earthlink / Google section of our privacy analysis. As you can see, the Earthlink / Google proposal fell short of privacy-enhancing standards that we proposed. These privacy-enhancing standards are reasonable and one of the six potential providers satisfied all of them.

We believe that the City can reform many of the categories where the Earthlink / Google proposal received ratings "in the red." By allowing individuals to use the service without signing in, many privacy risks will be reduced. By shifting the Earthlink / Google information sharing practices to opt-in, individuals will have the choice as to whether their data will be sold. By adopting policies that give notice of legal requests for their information, individuals will be able to challenge such requests where appropriate. By establishing data retention schedules, there will be less risk that the network will become a honeypot for various interests seeking data on users. And finally, there should be limitations on the use of the network for surveillance and strict policies to ensure that these powerful tools are not abused.

Respectfully submitted,

Nicole A. Ozer
Technology and Civil Liberties Policy Director
ACLU of Northern California
nozer@aclunc.org
415-621-2493

Kurt Opsahl
Staff Attorney
Electronic Frontier Foundation (EFF)
kurt@eff.org
415-436-9333

Chris Hoofnagle
Senior Counsel and Director, West Coast Office
Electronic Privacy Information Center (EPIC)
hoofnagle@epic.org
415-981-6400

San Francisco Request for Proposals	Coalition Gold Standard	Earthlink (premium) / Google (free)
What personal information is collected about users?	None, if possible. Anonymous and pseudonymous access should be available.	Google: email address Earthlink: name, address, telephone number, billing information, computer info. Earthlink also enhances data by buying information from third parties.
How is this information used?	Only for purposes necessary to operation of the network.	Google: to authenticate and login users. Earthlink: for provision of service and marketing.
How long is this information stored?	A data retention schedule should specify that data are kept only for so long as needed to operate the network.	Google: account usage information deleted regularly; never stored more than 180 days. Earthlink: as long as needed for business purposes.
With whom is this information shared?	Only when necessary for operation of the network.	Google: with third parties (with opt out rights). Earthlink: With affiliates.
Is this information commercialized in any way?	Providers should not commercialize personal information without voluntary, opt-in consent.	Google: Yes, used for personalized content and advertising. Earthlink: to market services, and to third parties (with opt out).

San Francisco Request for Proposals	Coalition Gold Standard	Earthlink (premium) / Google (free)
Is this information correlated to a specific user, device or location?	Providers should correlate information to specific users, devices, or locations only to the extent necessary to operate the network.	Google: Yes, but it is regularly deleted. Earthlink: Yes.
Are mechanisms available to allow users to opt in or opt out of any service that collects, stores, or profiles information on the searches performed, websites visited, e-mails sent, or any other use of the Network?	Opt in should be the standard for services that exceed the basic function of providing individuals with Internet access.	Google: Opt-in for sensitive information; opt-out for other info. Does not explain how the service profiles and targets users based on surfing. Earthlink: Opt-out.
Are mechanisms available to allow users to opt in or opt out of any service that tracks information about the user's physical location?	Providers should take all reasonable steps to enable location-based services without creating a tracking or logging mechanism that will create records of individuals' location.	Google: non-responsive Earthlink: Opt-out, once node-level tracking is available.
Are users enumerated or assigned any unique number that can be used to track them from session to session?	Providers should take all reasonable steps to design the system to prevent enumeration from session to session. Providers should obtain a user's voluntary affirmative consent before enumerating users across sessions.	Google: Cookies are used, but it appears as though users can disable them. Earthlink: Cookies are used, as is Doubleclick.
Are policies in place to respond to legal demands for users' personal information in accordance with applicable laws?	Providers should follow Cable Policy Act standards by giving the user notice of the legal demand before complying.	Google: Yes, but policy does not specify whether notice to the user is given. Earthlink: may disclose at company's sole discretion, policy does not specify whether notice to the user is

San Francisco Request for Proposals	Coalition Gold Standard	Earthlink (premium) / Google (free)
		given.
Are users allowed access to all information collected about them?	Users should be able to access personal information collected and maintained by the provider and its affiliates or partners.	Google: Yes. Earthlink: may access registration information.
Are users provided with a mechanism to review this information and to correct inaccuracies or delete information?	Providers should extend reasonable means for users to correct or delete personal information collected by the provider and its affiliates or partners.	Google: Yes. Earthlink: offers access and modification to information, but no apparent deletion.