Coalition Letter on San Francisco Municipal Broadband

[BY EMAIL (techconnect@sfgov.org)]

February 21, 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 / Privacy and Municipal Broadband

Dear Mr. Vein,

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 uses 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.

At section 2.11 of the RFP, TechConnect requested proposers to provide a copy of their privacy policy, to certify that it complies with applicable law, and to explain how it will communicated to users. TechConnect also requested proposers to explain how they will address a series of privacy issues raised in our October letter.

In this letter, we stress that the city should consider minimum standards for the privacy issues raised by the RFP. Privacy notices are not enough. The short history of E-commerce has shown that companies often issue privacy policies that are substantively weak and extend to users few legal rights to redress privacy violations. Minimum standards are necessary for each of the privacy questions posed to proposers in order to guarantee respect for users' rights.

To assist TechConnect in this process, we suggest model minimum standards to each of the questions included in the RFP. We also urge TechConnect to consider the safeguards recommended in EFF's "Best Practices for Online Service Providers," which describes legal policies and technical procedures for protecting privacy. [2]

• What personal information is collected about users?

Providers should take all reasonable steps to enable use of the network without the collection of personal information. Data collection should accommodate the individual's right to

communicate anonymously and pseudonymously through the service.

"Operation of the network" refers to actions necessary to technically run the network. This includes actions necessary for guaranteeing service availability, billing, network testing, and reasonable security measures.

• How is this information used?

Providers should use information for purposes necessary to operation of the network.

• How long is this information stored?

Providers should specify a data retention schedule for all information collected. Providers should store information only for so long as needed to operate the network. In no event should data be kept for more than a few weeks. Information that needs to be kept to provide enhanced services should be the minimum necessary to provide the service, be deleted as soon as operationally possible, and providers should employ technical measures to shield this information including obfuscation or aggregation.[3]

• With whom is this information shared?

Providers should only share information for purposes necessary to operate the network. Entities that receive personal information should be held to the same privacy standards as the provider.

• Is this information commercialized in any way?

Providers should not commercialize personal information collected in the course of operating the network unless the user opts in to such uses of data.

"Opt in" refers to affirmative consent, a situation where the user can employ the network for basic services, and affirmatively choose to enroll in additional services. That is, a user does not "opt in" to the service by simply using the network. Providers should obtain affirmative consent again where there is a material change to information collection or use policies. Furthermore, an expression of affirmative consent should only be effective for one year.

• 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.

• 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.

• 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.

• 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 affirmative consent before enumerating users across sessions.

• Are policies in place to respond to legal demands for users' personal information in accordance with applicable laws?

Providers should comply with legal demands for users' personal information only after verifying the legal sufficiency of the request, and notify the subject of the request as quickly as possible before providing information to the requestor. A good model is set forth by the Cable Communications Policy Act (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.

• 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.

• Are users provided with a mechanism to review this information and to correct inaccuracies or delete information?

Providers should extend reasonable opportunities for users to correct or delete personal information collected and maintained by the provider and its affiliates or partners.

Thank you for considering our comments. If we can be of further help, please feel free to contact us.

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

[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.

[2] Attached as Appendix B. 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/.

[3] See Appendix B.
