ELECTRONIC PRIVACY INFORMATION CENTER

A Privacy Analysis of the Six Proposals for San Francisco Municipal Broadband

Six companies have proposed plans to bring municipal broadband to San Francisco. They range from approaches where users will pay monthly fees, to advertising-supported services and free services.

Whatever the City's approach, we think it is important that the accepted proposal respect Californian's fundamental right to privacy. San Franciscans have the right to a network that respects privacy and autonomy, one that allows users to explore what the Internet has to offer, including information about medical conditions and the use of online banking, without fear of government or commercial surveillance and intrusion. In the summary below, we compare the six proposals against a model standard of privacy rights. This comparison only judges the proposals on privacy rights; other important interests, such as bridging the digital divide, reliability in service, and quality of service, are not considered.

Again, we applaud City officials for their efforts to bring municipal broadband to San Francisco. This effort is an important experiment in public policy, one that we fully support. Our efforts are intended not to slow down or frustrate this important process, but rather to ensure that the network respects privacy rights.

Background

On October 19, 2005, the ACLU of Northern California, Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC) submitted comments to TechConnect concerning the privacy implications of municipal broadband access. In that letter, the groups 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 (see Appendix A). In issuing the Request for Proposals, the City did seek privacy information from proposers, but did not set minimum standards for protecting privacy.

In a follow up letter dated February 21, 2006, the groups stressed that the city should consider minimum standards for the privacy issues raised by the RFP. The groups 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. Model minimum standards were proposed (see Appendix B).

Below, EPIC and EFF compare the privacy implications of the six proposals made to provide San Francisco with broadband service against the model minimum standards. These standards promote privacy by limiting collection, use, and retention of personal information. The fundamental approach endorsed is that where information needs to be collected, it should only be used for operational purposes and deleted after it is no longer needed. Practically speaking, the minimum standards specified are best served by a system that:

- Allows access without "signing in." Signing in can require personal information that enables tracking. Even if signing in is done pseudonymously, it may enables session to session tracking and eventual identification of users.
- Provides a level of access that is free. Fees, unless there are reasonable avenues for cash payment, can allow the network operator to identify users through credit card or check account information.
- If advertising is present, it is not targeted based on users' identity, location, or web surfing behavior.

In light of these considerations and the Gold Standard set forth by ACLU, EFF, and EPIC, one proposal is clearly more protective of privacy than the others. The SF Metro Connect proposal is for a free service that does not require a sign in. Unlike other proposals, it doesn't attempt to commercialize users' data by monitoring them. Overall, the SF Metro Connect proposal is the most privacy-protective approach, and it satisfies nearly all the factors contained in the Gold Standard.

Short Summaries of Proposers' Bids

Communications Bridge Global (CBG)

Communications Bridge Global is not included in this analysis or in the privacy comparison chart, because the company failed to meaningfully respond to the city's request to provide information on privacy.

Earthlink/Google

Earthlink and Google have jointly proposed a plan where Earthlink would provide a premium, paid service delivering 1 Mbps connection speed, and Google would provide an advertising-supported 300 Kbps connection. Both services require the user to sign on, thus creating the opportunity for persistent tracking across sessions. The Google advertising supported service would target advertisements to individuals based on their Internet usage and other information.

MetroFi

MetroFi proposes an advertising-supported service with a 1 Mbps connection, or the same connection without advertisements for $20 a month.

As with many companies operating under self-regulatory privacy norms, MetroFi's privacy statement is contradictory. It claims only to gather anonymous information for the free service, but later on the same page, the company states that its free service collects email addresses and demographic information through surfing behavior and questionnaires. Email addresses are identifiable, personal information. Furthermore, aggregate surfing behavior and questionnaire information can be used to identify individuals.

NextWLAN

NextWLAN proposes to use transmitters to provide connectivity through consumer-grade DSL access. In the company's "Micronode network," users would be connected to DSL lines through subscribers' access points and repeaters. Basic services (384 Kbps symmetric connection) are advertising supported. Upon signing in, users would be located to their very street address, and

advertising would be targeted to them. For-fee premium services could accommodate 1.5 or 3 Mbps connections.

Of all the proposals, NextWLAN is probably the most frank in how it plans to force-feed users advertising. It also seems to contradict its privacy guarantees. For instance, in the privacy section, the company claims that "NO User profiling mechanisms shall be incorporated into the" network. However, elsewhere the company specifies that users will be immutably directed to location-aware portals:

> On the revenue side, the WGR Gateway also uniquely incorporates the defining, enabling element of a Free-to-the-User, No-Cost-to-the-City municipal WiFi network: an e-commerce monetized, fully captive location aware Internet portal. Upon logging in to SFWiFi a User will be immediately and immutably redirected to a portal-proxy server hosted webpage cognizant of the User's to-the-street-address location and supporting state of the art e-advertising functions (automatically generated maps pointing to local merchants and other businesses of interest to the User can yield the Network Operator up to $0.25 per mouse click in local search advertising revenue) and other key User Services.

San Francisco has broad, laudable goals in providing municipal broadband to its citizens and visitors. It should not make them "fully captive" to a system that knows their location and can "immutably redirect[]" them to advertisers.

NextWLAN claims that is collects name, address, and phone number and that this information is never disclosed. But the company does not specify how it addresses legal demands for subscriber information, which obviously has to be disclosed to law enforcement and others in certain circumstances.

It is important to note that NextWLAN's proposal is simply the most frank about using location and other data to target advertising. Other proposals that promote advertising-supported services are not substantively different, but these other companies may have better public relations messaging to mask how privacy invasive these practices are.

Razortooth (Redtap)

Razortooth (Redtap) has proposed a cooperatively-owned network combined with the creation of community access centers and initiatives to promote digital literacy. The company proposes a free basic service that would cover government property, and a $5 a month co-op membership fee for other areas. As with the other proposals dependent on payment, the membership fee creates an opportunity to identify and then track users across sessions. However, the low price of the co-op service, combined with the community access centers does make it possible for Razortooth to sell access packages for cash to those who wish to use the service without identifying themselves. Razortooth promises "No ad-ware or spy-ware will be used. Users will be free to access the Internet unhampered by ad-driven business models or pop-up-ads."

The company claims that it "will not share ANY private user information or anonymous demographic information with ANY outside vendor not affiliated with RedTAP." This is an important promise; it could be strengthened by removing the qualifier "private" before "user information" and by adding a policy that requires routine deletion of user data after it is no longer operationally necessary to maintain. It is also important to ensure that the co-op members who run the proposed system do not snoop on other users by means of their ability to service the access points. Razortooth is included in the privacy comparison chart below because the company provided us with their privacy policy after we requested it.

SF Metro Connect (Seakay/Cisco Systems/IBM)

This proposal seeks to combine Seakay's experience, Cisco's hardware, and IBM's software to create a non-profit operated 1Mbps network called SF Metro Connect. It would operate on a public-radio-like model, where equipment was donated, underwriting solicited from corporations, and donations sought from community members and foundations. SF Metro Connect would provide a free 1Mbps symmetric connection, and charge for those needing more bandwidth. The company claims that: "Our self sustaining economic model presents a viable financial alternative to what in our opinion is a model of collecting information and charging users for premium service." From the proposal, it appears that the only information SF Metro Connect would collect is the MAC addresses of users.

Overall, from the information available, SF Metro Connect's proposal appears to be the most privacy friendly. In a FAQ posted on the Seakay site, the company claims, "SF Metro Connect will not collect, disseminate, sell or use any personally identifiable data about any individual network users for any purpose, unless required by law. We support a user's right to privacy."

However, it should be noted that there is significant controversy surrounding the corporate citizenship of Seakay's partners, Cisco Systems and IBM. Cisco is alleged to have provided the Chinese government with technology enabling state censorship. IBM has helped the US government develop intrusive data mining systems and has been a strong opponent of information privacy laws.

Respectfully submitted,

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

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

Proposal Comparison Chart[1]

San Francisco Request for Proposals	Coalition Gold Standard[2]	Earthlink (premium) / Google (free)	MetroFI	NextWLAN	Razortooth (Redtap)	SF Metro Connect (SeaKay, Cisco, IBM)
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.	Email address for free service, billing information for premium service.	Name, address, and phone.	Registration requests name, email address, birth date, gender, zip code, primary language, secondary language, occupation, industry, and personal interests.	"…will not collect user information." FAQ states: "… will not collect, disseminate, sell or use any personally identifiable data about any individual network users for any purpose, unless required by law."
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.	Free service will use info for targeting advertisements.	Service targets marketing based on user's street address.	For "record keeping, marketing to you the customer, and for billing purposes."	Operation of network.

[1] CBG is not included because the proposal contained no privacy information; Razortooth is included because while the company did not answer RFP questions, it did provide EPIC with its privacy policy.
[2] The full text of the Coalition Gold Standard is available as Appendix B.

San Francisco Request for Proposals	Coalition Gold Standard[2]	Earthlink (premium) / Google (free)	MetroFI	NextWLAN	Razortooth (Redtap)	SF Metro Connect (SeaKay, Cisco, IBM)
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.	Information retained as long as subscription is active.	Not specified.	Not specified.	N/A, because user information is not collected.
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.	No one.	Only to business partners to deliver specific services.	Only with third parties providing services requested by the customer.	N/A, because user information is not collected.
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).	Free services use user information for advertising.	Used to target advertising.	Used for Razortooth marketing.	N/A, because user information is not collected.

San Francisco Request for Proposals	Coalition Gold Standard[2]	Earthlink (premium) / Google (free)	MetroFI	NextWLAN	Razortooth (Redtap)	SF Metro Connect (SeaKay, Cisco, IBM)
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.	No.	Yes. Users are captive to location-based advertising portal.	"Once you register with RedTAP and sign in… will have presence information for you at all times you are logged into our services."	N/A, because user information is not collected.
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.	Users can avoid information collection for advertsing purposes only by paying for premium service.	No.	Not clear, but "The customer has the right to opt in/out of mailing lists and marketing related communication."	N/A, because user information is not collected.
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.	No persistent location tracking, but targeting of ads based on location in the free service.	No, location tracking is basis of service.	Not specified.	N/A, because user information not collected.

San Francisco Request for Proposals	Coalition Gold Standard[2]	Earthlink (premium) / Google (free)	MetroFI	NextWLAN	Razortooth (Redtap)	SF Metro Connect (SeaKay, Cisco, IBM)
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.	Yes.	Yes.	"Once you register with RedTAP and sign in to our services, we…will have presence information for you at all times you are logged into our services."	No.
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 given.	No legal access policy specified.	No legal access policy specified.	Yes, but policy does not specify whether notice will be given. Also, company reserves ability to disclose "in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of RedTAP's terms of use, or as otherwise required by law."	N/A, because user information is not collected.

San Francisco Request for Proposals	Coalition Gold Standard[2]	Earthlink (premium) / Google (free)	MetroFI	NextWLAN	Razortooth (Redtap)	SF Metro Connect (SeaKay, Cisco, IBM)
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.	Proposal says no, but MetroFi's privacy policy states that the company offers access and correction rights.	No user access policy specified.	Can access account information, unclear whether other data can be accessed.	N/A, because user information is not collected.
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.	Proposal says no, but MetroFi's privacy policy states that the company offers access and correction rights.	Correction and deletion rights unspecified.	Can edit and delete profile.	N/A, because user information is not collected.

ELECTRONIC PRIVACY INFORMATION CENTER

Joint Letter on San Francisco Wireless Internet Access

[BY MAIL AND EMAIL (techconnect@sfgov.org)]

October 19, 2005

TechConnect RFI/C 2005-07
Dept. of Telecommunications and Information Services
City and County of San Francisco
875 Stevenson St., 5th Floor
San Francisco, CA 94103

Re: Privacy Issues Associated with Municipal Wireless Internet Access

The American Civil Liberties Union of Northern California (ACLU), Electronic Frontier Foundation (EFF), and Electronic Privacy Information Center West Coast Office (EPIC West) submit these comments on TechConnect RFI/C 2005-07 in response to information received by the City concerning municipal wireless Internet access.

The ACLU is a nonprofit, nonpartisan organization dedicated to the defense and promotion of the civil liberties and civil rights secured by the state and federal constitutions and related statutes. The ACLU of Northern California, based in San Francisco, is the largest ACLU affiliate in the nation, with 50,000 members spanning communities from Crescent City to Fresno.

EFF is a nonprofit donor-supported membership organization working to protect fundamental rights regardless of technology; to educate the press, policymakers, and the general public about civil liberties issues related to technology; and to act as a defender of those liberties. Among its various activities, EFF opposes misguided legislation, initiates and defends court cases preserving individuals' rights, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, engages the press regularly, and publishes a comprehensive archive of digital civil liberties information on the most linked-to web sites in the world at www.eff.org.

EPIC is a not-for-profit research center founded in Washington, DC in 1994 to focus public attention on privacy and open government. EPIC's West Coast office is based in San Francisco, and concentrates on consumer privacy issues.

Municipal wireless offers our society an opportunity to address digital divide issues, to give more individuals access to more information, to keep San Francisco competitive with other cities offering free or low-cost wireless, and many other valuable social ends.

We are heartened that the City has already recognized the profound importance of proper privacy protections for the municipal wireless system by stating in the RFI that:

The City anticipates a Network that protects the privacy of users, respects consumer choice, and fosters diversity of information and ideas.

Additionally, by asking vendors to specify the privacy policies and security standards that will be put in place "to protect the privacy of--and information transmitted by--users," the City has wisely made privacy a key policy standard for municipal wireless Internet access.

We have surveyed the privacy and free speech issues raised by the proposals and have provided some

concrete questions to assist the City in addressing these issues in a meaningful manner.

The Importance of Privacy

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.[1] Proposition 11, which added the privacy right to the State Constitution recognized that both the government and the private sector pose risks to information privacy:

The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.[2]

As the ballot proposition recognized, privacy is important because it gives individuals a zone of autonomy in which they can explore intellectual interests, personal relationships, and other socially valuable ends without fear of intrusion and oversight.[3] The "ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."[4]

San Franciscans have the right to a network that respects privacy and autonomy, allowing users to explore what the Internet has to offer, including information about medical conditions and the use of online banking, without fear of surveillance or intrusion.

We note that these principles cannot be viewed as mere aspirations. In general, when a government entity establishes and assumes responsibility for a system that provides public electronic communications services, that constitutes "state action" for constitutional purposes and requires the City to comply with the dictates of the state and U.S. Constitutions, including the First and Fourth Amendments.

Comment on Question 8

Question 8 from the RFI solicits comment on how to implement both privacy and freedom of expression on the network:

What privacy policies and security standards will you put in place to protect the privacy of--and information transmitted by--users?

We wish to emphasize that this question raises two important issues: first, how will the network protect the privacy of users. Second, how will the network protect information transmitted by users? These two questions, while they sound similar, are different. Many of the commercial responses to the RFI focus exclusively on the second question, emphasizing how their approach will protect against malicious users of the system. Such protection is critical to operation of the network. But both must be addressed to fully serve the City's policy standard of developing a network that protects the privacy of users and fosters diversity of information and ideas.

Protecting the Privacy of Users

A dialogue on how to protect users' information must encompass the following issues:

· Will users be enumerated, that is, assigned a unique number that can be used to track an individual from session to session?

Computers accessing the Internet must be identified in order to route content to the appropriate user. Computers must also be identified when they "host" or provide resources to other users. However, in most situations, there is no requirement that a unique identifier be employed to keep track of what an Internet user

does in a previous session. Linking session activity and creating a log of activities creates a profile of a user's activity. It is well settled that the First Amendment protects privacy of association, such as the sanctity of group membership lists, as well as the right to speak anonymously. Accordingly, it must be permissible for system users to use technical measures that shield their identities.

Special attention must be paid to whether users will be tracked by identifiers that are unchangeable, such as the "MAC" identifier embedded in network cards or by "usernames" assigned by the service. Such vendor plans can lead to a significant reduction in privacy.

- **Will the service attempt to commercialize data?**

A main goal of municipal wireless is to bridge the digital divide. Much of the population affected by the divide cannot exercise choice in the marketplace and choose a privacy-sensitive service provider. We therefore think it especially important that the city not bargain away privacy by choosing a service provider that commercializes users' data. In addition, we have specific privacy concerns with several of the proposals that include commercialization of the data.

For example, we are skeptical of claims that systems that use transactional logs to target advertising are truly anonymous. Any system that scans users' Internet usage for content can be tweaked to serve other purposes, or altered to track specific individuals. Furthermore, such targeting could lead to harm where, for instance, a family computer is used to research a sensitive and very private issue such as health concerns or political activity, and a later user of the same computer is presented with advertising pertaining to that earlier user's browsing.

We are similarly skeptical of bids where the service provider seeks to commercialize user or transactional data through affiliate or non-affiliate sharing agreements. If such a provider is chosen, the standard should be opt-in. Affirmative consent should be obtained before data is used for marketing by affiliates or non-affiliates.

- **Will the service provider resist legal demands for users' personal information?**

Because service providers are the vital link between individuals and Internet resources, they face legal pressures from other network users, industries, and governments to disclose personal information. As courts have noted, users "who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identities."[5] Typically, when user information is sought, the service provider is the first entity informed of the request.

This issue is especially sensitive when the service provider is, as here, a state actor, and may therefore face additional pressures from government to provide information about individuals' Internet use. 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.

The City should discuss procedures and policies for protecting users' personal information in the hands of vendors. Specifically, to protect and preserve users' rights to speak freely, the City should:

(1) ensure that the service provider will provide notice, within no more than seven days of receipt of a subpoena, to each person whose personal information is sought;

(2) allow the user at least fourteen days from the time notice was received to file a motion to quash; and

(3) prohibit any disclosure pending the disposition of any motion to quash.

- **How long will server logs be maintained?**

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. As a result, any municipal wireless service provider must deal with requests from law enforcement and lawyers to hand over private user information and logs. Yet, compliance with these demands takes away from the City's goal of providing users with reliable, private and secure network services.

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. [6] Personal information about users should be kept only as long as it is operationally necessary, and in no event for more than a few weeks. Aside from reducing retention, privacy risks can be managed by eliminating or obscuring personally identifiable information or by tracking usage in the aggregate rather than by personal identifiers.

We urge the City to ensure that its municipal wireless vendor adopt procedures along the lines of EFF's "Best Practices for Online Service Providers," which describes legal policies and technical procedures for protecting privacy.[7] Clear policies will conserve resources, help safeguard private data, and preserve freedom of expression online.

Protecting Information Transmitted by Users

The question of how to protect information transmitted by users can be addressed in a number of ways, and this list is not comprehensive. A dialogue on these issues should include the following considerations:

- **Will data be protected from interception by others?**

There must be measures to protect information transmitted by users from interception by others. A municipal wireless network will not be usable for personal activities, such as medical and banking activities if data can be intercepted and understood by others.

- **Will data be authentic? Will it be protected from corruption by others?**

There must be measures to ensure that the data flowing between the user and service provider is authentic. That is, there must be measures to shield users from being sent data that appears to be legitimate, but is really sent by a malicious actor. A typical example of this is the "man-in-the-middle" attack, where a malicious actor inserts himself between the service provider and the user in order to defraud one or both of the parties.

- **Will there be balance in addressing unlawful users?**

Malicious hackers and other bad actors will attempt to use the system. The City should strive to address these issues without punishing all users through identification requirements, such as the enumeration methods mentioned above. A few bad apples should not limit the network's ease of use for everyone else.

Where possible, unlawful uses should be addressed though techniques that do not involve identification. The service provider should track MAC addresses or usernames only after it determines that a specific computer is being used for unlawful purposes.

- **Will users have access to true end-to-end encryption?**

True end-to-end encryption allows communication that is shielded by mathematical algorithms from the user's computer to an online resource. It is not clear whether commercial commentators are proposing to offer true end-to-end encryption, or simply user-to-client encryption. In user-to-client encryption, the information is decrypted and sent "in the clear" after it reaches the service provider. Where possible, the system should employ true end-to-end encryption in order to properly protect user privacy.

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

Nicole A. Ozer

Appendix A

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] California law restrains the alienability of privacy rights in many respects. *See e.g.* Cal. Civ. Code § 1798.84(a) (making waivers of a variety of California-specific privacy protections inalienable by contract); Consumer Credit Reporting Agencies Act, Cal. Civ. Code § 1785.36.

[2] Proposed Amendments to Constitution, California Office of the Secretary of State, Nov. 7, 1972, available at http://library.uchastings.edu/ballot_pdf/1972g.pdf.

[3] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373 (2000).

[4] *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

[5] *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. at 578.

[6] Because of Constitutional and statutory regulations limiting government access to user data, we assume that the City itself will not have access to personal data collected by the service provider absent appropriate legal process.

[7] 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/.

EPIC Privacy Page | EPIC Home Page

Last Updated: October 19, 2005
Page URL: http://www.epic.org/privacy/internet/sfws10.19.05.html

Appendix A

ELECTRONIC PRIVACY INFORMATION CENTER

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.

Appendix B

• 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.

Appendix B