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
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/.
