



Introduction

The ACLU of Northern California strongly supports the growth of wireless access and looks forward to a time when all of Silicon Valley will be able to utilize the wealth of information available on the Internet. However, none of us should be forced to pay for it with our privacy and free speech rights. Wireless Silicon Valley must ensure that any system it selects adequately protects these rights.

The ACLU of Northern California (ACLU-NC), along with the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC), submitted a letter on April 17, 2006, prior to the release of the request for proposal (RFP) that detailed the privacy and free speech concerns that must be taken into account when selecting a municipal wireless vendor. The organizations also requested that specific questions about privacy and free speech be included in the RFP to ensure that Wireless Silicon Valley and community members would have the necessary information to properly analyze the proposed systems and make an informed decision about which vendor should be selected for this important project.

Wireless Silicon Valley declined to include a specific question about privacy or free speech in the RFP, but rather decided to ask each vendor to submit its end user license agreement (EULA) – the agreement that a customer clicks on and agrees with prior to using the system. Wireless Silicon Valley also pledged at the RFP release event to take privacy and free speech into account in its decision. ACLU-NC expressed our concern at that time that without a specific question in the RFP, the vendors would not properly address privacy and free speech issues. As feared, the EULAs are extremely general and none of the three proposals selected by the task force—MetroFi, VeriLan, or Silicon Valley Metro Connect – even discusses privacy or free speech apart from merely stating that its EULA was attached to the proposal.

Importance of Privacy and Free Speech

Municipal wireless is meant to benefit the public, not businesses' pockets. As Wireless Silicon Valley considers the final proposals, privacy and free speech must be one of its highest priorities.

QUINN DELANEY, CHAIRPERSON | DONNA BRORBY, ROBERT CAPISTRANO, LISA HONIG, ROBERTA SPIECKERMAN, VICE CHAIRPERSONS | NANCY PEMBERTON, SECRETARY/TREASURER
DOROTHY M. EHRLICH, EXECUTIVE DIRECTOR | MAYA HARRIS, ASSOCIATE DIRECTOR | ALAN SCHLOSSER, LEGAL DIRECTOR
ANN BRICK, MARGARET C. CROSBY, TAMARA LANGE, JULIA HARUMI MASS, JORY STEELE, STAFF ATTORNEYS
CHERI BRYANT, DEVELOPMENT DIRECTOR | ERIKA CLARK, COMMUNICATIONS DIRECTOR
NATASHA MINSKER, NICOLE A. OZER, MARK SCHLOSBERG, POLICY DIRECTORS
STEPHEN V. BOMSE, GENERAL COUNSEL

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA
111 NORTH MARKET STREET, SUITE 940, SAN JOSE, CA 95113 | T/408.282.8970 | F/408.282.8975 | TTY/415.863.7832 | WWW.ACLUNC.ORG

Privacy is an inalienable right of all Californians under the California State Constitution. As an inalienable right, a citizen's privacy is not to be bought, sold, or bargained away.¹ A system's safeguards for privacy must play an important role in any municipal wireless selection process. Silicon Valley residents have the right to a wireless 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. Unless the wireless system possesses adequate protections for privacy and free speech, the very goal of the Wireless Initiative – to provide equal access to technology and information – will be undermined. The current proposals threaten to create a new digital divide: one in which wealthier people who can afford to pay for Internet access get to keep their privacy and free speech, while people who can't afford it are forced to pay for access with their rights.

Wireless Silicon Valley is building a new communications infrastructure for Silicon Valley and it must ensure that this system includes protections for fundamental civil rights. If Wireless Silicon Valley were to select one of the proposals as currently written, it would be akin to installing public telephone booths all around the community. However, in order to use them, you would have to agree that all of your conversations would be monitored and recorded, you would be forced to listen to advertisements for products based on what you are saying, and there would be no adequate safeguards that the content of your conversations would not be shared with other companies and the government. This is an unfair bargain for the people of Silicon Valley.

It is not too late for Wireless Silicon Valley to uphold its pledge to protect the fundamental rights of members of the Silicon Valley community. To assist Wireless Silicon Valley, we have reiterated the system safeguards that must be in place in any municipal wireless system to protect privacy and free speech and analyzed the three final proposals for these criteria.

Privacy and Free Speech Safeguards

1. Users should not be tracked from session to session.

There is no legitimate reason why a wireless service provider needs to keep track of what information a user views over the course of multiple log-in sessions. By creating a log of session activities and linking them to a unique identifier, the system creates a profile of a user's activity. While a municipal wireless company might desire to track users throughout sessions so that they can create detailed profiles to use for targeted advertising or to sell or trade to third parties, such profiling is unacceptable in a municipal wireless system. Such a log threatens both an individual's right to privacy, as well as his or her First Amendment right to speak and associate anonymously. A company using a targeted advertising model can simply target advertising for current sessions without maintaining logs that eviscerate an individual's right to privacy and free speech. Particularly in light of recent revelations about illegal and unconstitutional spying on

¹ 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.

Americans, it is important that there be safeguards to ensure that private information is properly protected. Accordingly, municipal wireless systems should not require static logins tied to identities or must include mechanisms to allow users to employ technical measures to shield their identities.

	<u>Privacy Compliant?</u>	<u>Does the Service Track Users from Session to Session?</u>
MetroFi	No	Requires a user login that can be used to track individual usage from session to session.
Silicon Valley Metro Connect	No	Requires a user login, tied to the user's address and credit card, which allows for what the proposal describes as "user tracking."
VeriLan	No	Requires a user login that can be used to track individual usage from session to session. May require credit card, address, phone number and other billing information. Tracks detailed user records including all inbound and outbound data.

2. The service should not attempt to commercialize user 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. Therefore, it is especially important that Silicon Valley cities not bargain away privacy by choosing a service provider that commercializes users' data.

	<u>Privacy Compliant?</u>	<u>Does the Service Commercialize User Data?</u>
MetroFi	Maybe	The proposal states that "no personally identifiable information will be shared with 3 rd parties." However, the proposal includes a targeted advertising business model that fails to explain how user data will be used to target advertisements.
Silicon Valley Metro Connect	No	Neither the proposal nor the EULA contains any limitations on how Metro Connect will share user data with third parties or how user data will be tied to "targeted" advertisements.
VeriLan	No	Proposal promises "highly targeted" advertising but neither the proposal nor the EULA contains any limitations on how it will share user data with third parties or how user data will be tied to "targeted" advertisements.

3. The service must be prepared to resist demands for users’ personal data.

Service providers are the vital link between individuals and Internet resources and face pressures from other network users, industries, and governments to disclose personal information. Except in circumstances where law enforcement presents a court order binding the service provider to secrecy, the service provider should inform the user of a government request for information 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.

	<u>Privacy Compliant?</u>	<u>Are Policies in Place to Respond to Legal Demands for Users’ Personal Information?</u>
MetroFi	No	Will disclose personal information in response to what MetroFi vaguely calls “legal process.” Does not state whether it will resist civil subpoenas. No policy giving users notice of subpoenas.
Silicon Valley Metro Connect	No	Will disclose personal information in response to criminal and civil subpoenas. No policy giving users notice of subpoenas.
VeriLan	No	Will disclose personal information to law enforcement in response to “legal violations.” Does not state whether it will resist civil subpoenas. No policy giving users notice of subpoenas.

4. Server logs should be maintained for the minimum amount of time possible.

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.² 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.

	<u>Privacy Compliant?</u>	<u>Does the Service Have a Data Retention Policy that Minimizes Storage of Personalized User Data?</u>
MetroFi	No	Maintains logs capable of user tracking. No limitations on how long data is retained.
Silicon Valley Metro Connect	No	Maintains logs capable of user tracking. No limitations on how long data is retained.
VeriLan	No	Maintains logs capable of user tracking. No limitations on how long data is retained.

² Because of Constitutional and statutory regulations limiting government access to user data, we assume that the cities or the task force itself will not have access to personal data collected by the service provider absent appropriate legal process.

Conclusion

Any proposal to provide wireless service to Silicon Valley residents should include as a matter of course a comprehensive privacy proposal that addresses the issues raised above. A proposal should only be successful if it provides options that allow the user to access the Internet anonymously, does not commercialize data, clearly states that it will resist inappropriate legal requests for user information, and includes a data retention plan that minimizes the amount of time that user information is stored on the server. For a more detailed analysis of the privacy and free speech safeguards necessary for municipal wireless, please see our opinion letter of April 17, 2006, available at <http://www.aclunc.org/privacy/technology/060217-SVwifi.pdf>.

Nicole A. Ozer
Technology and Civil Liberties Policy Director, ACLU of Northern California
408.282.8970 x 303
nozer@aclunc.org