

# **WiFi Hot Spots Must Not Chill Privacy and Free Speech**

Nicole A. Ozer

Technology and Civil Liberties Policy Director

ACLU of Northern California

[nozer@aclunc.org](mailto:nozer@aclunc.org)

- Strongly support WiFi, but must not be forced to pay with privacy and free speech rights.
- Business models track who you are, what you are looking at, where you are looking at it from
  - political information
  - health information
  - looking for a new job
- Proposals are tantamount to monopoly for public telephones on every corner
  - Every conversation monitored.
  - Advertisements based on what you say.
  - No adequate safeguards that content of your conversation won't be shared with other businesses and the government.
- Once information is collected, don't know where it might end up. NSA, AOL.
- Inalienable right to privacy- can't be bought, sold or bargained away.
- Intrusive business models undermine the goals of muni WiFi. If you have money, get to keep privacy and free speech. If you don't have money, you pay for WiFi with your rights.
- Businesses are not doing us a favor- massive market and it is up to WSV to ensure that the people of this community get a fair bargain.

Wireless Silicon Valley Proposals	<b>Privacy Gold Standard</b>	<b>MetroFi</b>	<b>Silicon Valley Metro Connect</b>	<b>VeriLan</b>
<b>Track Users from Session to Session?</b>	Providers should take all reasonable steps to design the system to prevent tracking from session to session. Anonymous and pseudonymous access should be available.	Requires a user login that can be used to track individual usage from session to session.	Requires a user login, tied to the user's address and credit card, which allows for what the proposal describes as "user tracking."	Requires a user login that can be tracked 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
<b>Commercialize User Data?</b>	Providers should not commercialize personal information without voluntary, opt-in consent.	The proposal states that "no personally identifiable information will be shared with 3 <sup>rd</sup> parties." However, includes a targeted advertising business model that fails to explain how user data will be used to target the advertisements.	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 advertisements.	Proposal promises "highly targeted" advertising but neither the proposal nor the EULA constrains any limitations on how will share user data with third parties or how user data will be tied to advertisements.
<b>Proper Policies for Legal Demands for Users' Personal Information?</b>	Providers should require a warrant and give the user notice of the legal demand before complying.	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.	Will disclose personal information in response to criminal and civil subpoenas. No policy giving users notice of subpoenas.	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.
<b>Data Retention Policy that Minimizes Storage?</b>	Data retention schedule should specify that data are kept only for so long as needed to operate the network.	Maintains logs capable of user tracking. No limitations on how long data is retained.	Maintains logs capable of user tracking. No limitations on how long data is retained.	Maintains logs capable of user tracking. No limitations on how long data is retained.

Green = Privacy Friendly/ Yellow = More information needed but may be privacy friendly / Red = Privacy invasive