

Companies Positioned in the Middle: Municipal Wireless and Its Impact on Privacy and Free Speech

By NICOLE A. OZER*

FORTY YEARS AGO, the United States Supreme Court ruled in *Katz v. United States*¹ that the Fourth Amendment protects people and not places and that public telephone conversations were entitled to protection.² This ruling allowed Americans to be confident in the privacy and security of their private phone conversations, regardless of whether they were on a telephone in their bedroom or in a public telephone booth in Times Square.³ A new public communications infrastructure, in the form of municipal wireless systems, is currently being built in cities around the nation. The public telephone booths that used to be commonplace on street corners have given way to wireless internet routers dangling from city light poles. These routers form a municipal wireless network, providing blanket outdoor coverage to communities and paving the way for individuals to log onto the Internet and communicate from their corner bakery or public square.

* Nicole A. Ozer is the Technology and Civil Liberties Policy Director at the American Civil Liberties Union of Northern California ("ACLU-NC"). Website and blog are available at www.aclunc.org. Information or opinions in this Article are not necessarily those of the ACLU-NC. Special thanks to Chris Hoofnagle, formerly of the Electronic Privacy Information Center ("EPIC") and currently Senior Staff Attorney at the Samuelson, Law, Technology, and Public Policy Clinic at Boalt Hall, University of California, Berkeley School of Law, and Kurt Opsahl, Staff Attorney, Electronic Frontier Foundation ("EFF"). Section III and the Appendices of this Article are based on materials produced together in response to the San Francisco TechConnect Wireless Initiative and Wireless Silicon Valley. More information and copies of these materials are available at <http://www.aclunc.org/tech>.

1. 389 U.S. 347 (1967).

2. *Id.* at 351-52.

3. Activities of the federal government since September 11, 2001, including warrantless wiretapping and the alleged disclosure of millions of call records to the National Security Agency ("NSA") by major communications companies, have improperly eroded the rights of Americans to the privacy of their telephone calls. The ACLU is currently engaged in litigation against the NSA and the telecommunications companies for illegal and unconstitutional actions. See ACLU-NC Government Surveillance Issues, http://www.aclunc.org/issues/government_surveillance/index.shtml (last visited Mar. 23, 2007).

More than 300 American municipalities across the country are looking to offer wireless service, and it is estimated that cities will spend more than \$700 million in the next three years to build these municipal networks.⁴

While increasing access to the Internet is an extremely important endeavor, many of the municipal wireless plans lack a thorough exploration of all the issues involved in the deployment of such a program. Many wireless programs in existence and in development require residents to bear a heavy burden for the system—paying for the networks with monthly fees, supporting the infrastructure for the programs with their tax dollars, and funding the business models with their privacy and free speech rights. Many of the business models currently being considered for systems around the country are tantamount to a city allowing the installation of public telephone booths on every corner forty years ago. However, in order to use these telephones, individuals would have to agree that all conversations would be monitored and recorded, that they would have to listen to advertisements for products based on their conversations, and that there would be no adequate safeguards that the content of conversations would not be shared with the government and third parties. This would have been an unfair and inappropriate bargain forty years ago, and it remains so today.

When a city institutes a municipal wireless system, it is building a new communications infrastructure on behalf of its residents. Like our rights to privacy in our public telephone communications, individuals have the right to a municipal wireless network that respects privacy and free speech, allowing users to explore all that the Internet offers without worrying where information about their online activities will end up or how it will be used or abused. Cities have a duty to protect the privacy and free speech rights of their residents, and safeguards for these rights must be priorities, not afterthoughts.

Parts I and II of this Article provide a brief background on municipal wireless, exploring the incentives for both cities and businesses that are driving the growth of municipal wireless. Part III discusses the privacy and free speech implications of municipal wireless systems and articulates general privacy and free speech protections that must be part of any municipal wireless system. Lastly, Part IV analyzes some

4. Dailywireless.org, 300 Municipal WiFi Systems in the U.S., <http://www.dailywireless.org/2007/01/02/300-municipal-WiFi-systems-in-us/> (last visited Mar. 23, 2007).

recent examples of municipal wireless programs and their protections for civil liberties.

I. The Emergence of Municipal Wireless

As more and more people communicate via e-mail and Voice over Internet Protocol ("VoIP") telephones and turn to the Internet to access essential information for their daily lives, there has been an explosion of interest in ubiquitous internet access. More than 56 million Americans, 28% of the population, have wireless internet enabled devices. As the costs associated with wireless internet networks decrease, homes, businesses, and even entire communities are now setting up wireless networks.⁵ In some homes today, family members might be working on several computers in different rooms of the house. Walk into a university, a private company, a hotel, or a coffee shop, and even a public square—it is now normal to view a sea of laptop screens, with their owners busily working away on e-mails and accessing websites.⁶ More than 30 million users log onto more than 150,000 wireless networks across the United States.⁷

Wireless local area networks ("WLAN") were originally developed to enable more efficient transfer of information between items in manufacturing and warehouse facilities.⁸ The desired mobility was created using radio technology. Each WLAN consists of a radio antenna and one or more wireless client radios. The antenna, or wireless router, transmits the radio waves to client radios that are within its range, often up to 300 feet.⁹ Wireless client radios can be incorporated into a wireless card installed in a desktop, USB adapter, or PC card or integrated into a notebook or handheld device. Recently purchased laptops usually come pre-installed with internal wireless connectivity, while wireless internet cards can be purchased and installed in older laptops.¹⁰

5. FED. TRADE COMM'N STAFF, FED. TRADE COMM'N, MUNICIPAL PROVISION OF WIRELESS INTERNET 8–9 (Sept. 2006), <http://www.ftc.gov/os/2006/10/V060021municipalprovwirelessInternet.pdf> [hereinafter FTC MUNICIPAL WIRELESS REPORT].

6. *Id.* at 6.

7. *Id.* at 7. For an example of the continual growth of internet wireless hotspots, see JiWire.com, JiWire Find WiFi Hotspots, <http://www.jiwire.com/search-hotspot-locations.htm> (last visited Mar. 23, 2007).

8. HP INVENT, UNDERSTANDING Wi-Fi 4 (Jan. 2002).

9. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 7.

10. *Id.* at 7–8.

The most common type of WLAN is known as "WiFi."¹¹ WiFi networks are based on the Institute of Electrical and Electronics Engineers ("IEEE") "802.11" standard for a WLAN.¹² WiFi radio waves travel over the 2.4 GHz and 5 GHz radio spectrum. A second standard, "worldwide interoperability for microwave access" ("WiMAX") describes another set of standards for wireless network technology.¹³ The WiMAX family of specifications (802.16) operates between 2 GHz and 66 GHz. The IEEE approved this standard specifically for a Wireless Metropolitan Access Network.¹⁴

A coffee shop or a household typically creates a WiFi network by installing one or more routers that serve as access points to send and receive the radio signals that connect the individual computers (or other devices) in the network.¹⁵ Each router has a direct broadband connection so that it can accommodate the accumulated transfers of information.¹⁶

Municipal wireless refers to a wireless network that is deployed throughout a city or region. Cities can create a wireless network that operates according to either WiFi or WiMax standards. A municipal wireless network must operate slightly differently than a wireless network in an individual store or household because it covers a much larger area. Because it would be very expensive to hard-wire the many wireless routers needed to provide coverage throughout the city, both to the Internet and to each other, municipal wireless networks utilize what is called a "mesh network."¹⁷ A mesh network is created by installing wireless routers every few feet, most often on street posts and light poles, so that their radio signal range overlaps with each other

11. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 6. See generally Wi-FiAlliance.org, Wi-Fi Alliance Knowledge Center, http://www.wi-fiAlliance.org/knowledge_center_overview.php?type=3#W (last visited Mar. 23, 2007). Wi-Fi is a registered trademark term promoted by the Wi-Fi Alliance, a group of wireless internet hardware and software providers that certify "802.11" products for network interoperability. Wi-FiAlliance.org, Wi-Fi Alliance Certification Program, http://www.wi-fi.org/certification_programs.php (last visited Mar. 23, 2007).

12. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 6–7.

13. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 9; see generally WiMAXForum.org, Welcome to the WiMAX Forum, <http://www.wimaxforum.org/home> (last visited Mar. 23, 2007).

14. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 9; see generally Welcome to the WiMAX Forum, *supra* note 13.

15. Dailywireless.com, Municipal Wireless for Dummies, <http://www.dailywireless.com/features/muni-wireless-for-dummies/> (last visited Mar. 23, 2007).

16. *Id.*

17. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 8.

and creates a continuous network.¹⁸ Depending on the topography of a city, adequate coverage may require at least thirty and perhaps more than one hundred wireless routers per square mile.¹⁹ These wireless routers pass the radio signals to each other within the mesh network until the signal reaches one of the wireless routers that actually is connected to a high capacity wire connection (which is called “backhaul technology”).²⁰ Since the wire connection can transfer data far more quickly than the wireless connection, it is this backhaul technology that is actually used to tap into the Internet.²¹

II. The Drive Behind Municipal Wireless

Municipalities have a range of incentives to develop and deploy municipal wireless networks, including increasing the efficiency and reducing the costs of city services, strengthening economic development, and providing greater technology access to community members. Companies have a simple and very strong incentive to market the development of municipal wireless systems—to make money.

A. Incentives for Cities

1. Low-Cost Internet Infrastructure for Law Enforcement and Other City Services

Municipal wireless is often a good way for the city to develop an inexpensive internet infrastructure for its city services, including law enforcement. Right now, many cities pay fees for mobile data access for municipal workers. For example, police departments across the country pay for services to enable their police officers to access information from their squad cars.²² However, many of these systems are very slow and do not have all the capabilities that police officers would like in the field.²³ Wireless companies are courting cities by touting ways that wireless internet access could increase the efficiency of city

18. Municipal Wireless for Dummies, *supra* note 15; FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 8.

19. Ryan Kim, *Wi-Fi in the City: Curtain About to Go Up on Productions in S.F.*, *Philadelphia*, S.F. CHRON., Oct. 17, 2005, at F-1, available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/Chronicle/archive/2005/10/17/BUGH3F84JS1.DTL&type=business>.

20. FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 8.

21. Municipal Wireless for Dummies, *supra* note 15; FTC MUNICIPAL WIRELESS REPORT, *supra* note 5, at 8.

22. TROPOS NETWORKS CASE STUDY, San Mateo Police Dep't, Metro-Scale Wi-Fi for Public Safety 3 (Mar. 2004), http://www.tropos.com/pdf/SMPD_Casestudy.pdf [hereinafter TROPOS—SAN MATEO POLICE DEP'T].

23. *Id.*

workers and even automate some city services with little to no additional costs.²⁴

Wireless systems are marketed to cities as a means to give greater tools to law enforcement, fire departments, and emergency services.²⁵ Companies promote municipal wireless as a way for central dispatch to track the location of the police cars or fire engines and improve communications among employees from police to building inspectors. Companies also market municipal wireless as providing the potential for city workers to have mobile access to databases, to produce more in-field reports, and to submit and retrieve other information to improve city services.²⁶

Many municipal networks, including that being developed in San Francisco, California, are also being touted as a backbone from which expand options for public video surveillance in the cities.²⁷ Since September 11, 2001, public video surveillance has proliferated—much of it funded by the new Department of Homeland Security (“DHS”) bureaucracy. DHS has provided over \$800 million in grants to local governments for video surveillance cameras and systems.²⁸ In the 2003 DHS grant program, California received over \$45 million in funds, with over \$31.5 million for equipment allocations.²⁹ The equipment authorized to be purchased with the DHS funds included video surveillance cameras for “critical infrastructure.”³⁰ In 2005, the City of

24. See TECHCONNECT CMTY. BROADBAND NETWORK, CITY AND COUNTY OF SAN FRANCISCO RFP RESPONSE 52, 65–69 (Feb. 21, 2006), http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/EarthLink_SanFrancisco_RFP_2005-19_PUBLIC.pdf [hereinafter SAN FRANCISCO RFP RESPONSE]; RON SEGE, MUNICIPAL WIRELESS—JUST THE FACTS, PLEASE! (Feb. 2005), <http://www.muniwireless.com/reports/docs/MunicipalWirelessFacts.pdf>; see also TROPOS NETWORKS CASE STUDY, CITY OF NEW ORLEANS, LA., Saving Lives with Tropos Metromesh 5 (June 2005), http://www.tropos.com/pdf/new_orleans_casestudy.pdf [hereinafter TROPOS—CITY OF NEW ORLEANS]; TROPOS NETWORKS CASE STUDY, GRANBURY, TEX. & FRONTIER NETWORK BROADBAND, PUBLIC SAFETY AND PUBLIC ACCESS 5 (Nov. 2005), http://www.tropos.com/pdf/casestudy_granbury.pdf [hereinafter TROPOS—GRANBURY, TEXAS & FRONTIER BROADBAND]; TROPOS NETWORKS CASE STUDY, CITY OF CORPUS CHRISTI, TEX., PIONEERING MULTI-USE METRO-SCALE WI-FI (June 2005), http://www.tropos.com/pdf/corpus_casestudy.pdf [hereinafter TROPOS—CORPUS CHRISTI TEXAS].

25. See, e.g., TROPOS—CITY OF NEW ORLEANS, *supra* note 24; TROPOS—GRANBURY, TEXAS & FRONTIER BROADBAND, *supra* note 24; TROPOS—CORPUS CHRISTI TEXAS, *supra* note 24.

26. TROPOS—SAN MATEO POLICE DEP'T, *supra* note 22.

27. See TROPOS—CITY OF NEW ORLEANS, *supra* note 24. See also SAN FRANCISCO RFP RESPONSE, *supra* note 24.

28. Martha T. Moore, *Cities Opening More Video Surveillance Eyes*, USA TODAY, July 18, 2005, http://www.usatoday.com/news/nation/2005-07-17-cameras-cities_x.htm. The article also mentions an additional \$1 billion available in state grants. *Id.*

29. 2003 DHS Grant Audit.

30. *Id.*

Ripon, California, a town of 13,000 people and twenty-five police officers, used \$75,000 in DHS funds to install a wireless internet system to connect twenty surveillance cameras to protect the "critical infrastructure" of three truck stops, public parks, and some downtown locations.³¹ According to Ripon's Police Chief, Richard Bull: "Thousands of vehicles go through there [truck stops] on a daily basis carrying everything from diapers to extremely hazardous materials. We wanted a good means of having surveillance out there. One of the things that has been brought up is hijacking of tanker trucks or other hazardous materials."³² In the last five years, video surveillance has doubled to become a \$9.2 billion industry. J.P. Freeman, a security industry consultant, estimates that the industry will grow to \$21 billion in 2010.³³

Companies market municipal wireless as an economic and efficient way to coordinate all of these public surveillance cameras. Sending footage wirelessly to a central location for storage enables police and other officials to access the footage from the field and to control the cameras from any internet connection.³⁴ Such capabilities will have grave implications on privacy and free speech; police can use these sophisticated cameras to monitor and record the movements of people innocently walking down the street, sharing an embrace, or participating in a political protest.³⁵

2. Increased Efficiency for City Services

In addition to reducing the existing costs for internet access for employees, many cities are banking on municipal wireless to save money by replacing workers with automated systems. Rather than having staff assigned to monitor parking, utility, and water quality meters, cities are hoping that automated meters communicating over the wireless network will do the job instead. The City of Corpus Christi, Texas, used to employ twenty-five individuals to read utility meters. Now, gas, water, and electric meters transmit readings over the wireless network

31. Naomi Graychase, *Muni-Mesh Fights Crime*, WI-FI PLANET, June 10, 2005, <http://www.wi-fiplanet.com/columns/article.php/3511836>; Dibya Sarkar, *City of Ripon Goes Wireless*, FED. COMPUTER WK., June 20, 2005, <http://www.fcw.com/article89302-06-20-05-Print>.

32. Graychase, *supra* note 31.

33. Moore, *supra* note 28; Jessica Bennett, *Big Brother's Big Business*, NEWSWEEK, Mar. 15, 2006, <http://www.msnbc.msn.com/id/11832024/site/newsweek/>.

34. See TROPIS—CITY OF NEW ORLEANS, *supra* note 24.

35. ACLU-NC Surveillance Issues, *Say No to Video Surveillance and I Spy with My Big Eye: Video Surveillance in Northern California*, http://aclunc.org/issues/technology/say_no_to_video_surveillance.shtml (last visited Mar. 23, 2007). While this Article was being published, ACLU-NC had not yet released, *I Spy with My Big Eye: Video Surveillance in Northern California*.

and the city employs only four staff members for oversight.³⁶ According to a member of the city's information technology department, the wireless system "eliminates costs, it avoids costs and has reduced costs."³⁷ According to some proponents of municipal wireless, between smart meters and increased efficiency of other workers, like maintenance and building inspectors, municipal wireless can save cities millions of dollars.³⁸ Philadelphia estimates that its municipal wireless program will save \$2 million in existing expenses.³⁹

Other cities are also looking at the municipal wireless system to increase efficiency and save costs by using the new communication network to publicize municipal issues and events. In San Francisco, the contract entitles the city to post six hyperlinks regarding community notices for municipal purposes on the internet login page, which is seen by all the people using the municipal wireless system.⁴⁰

The possibility that municipal wireless will provide more tools to a city and will save costs makes it very attractive. The deal becomes sweeter still when wireless companies promise these increased efficiencies and budget savings without demanding any money from the city, or even paying the city money to use the existing infrastructure.⁴¹ Many municipal wireless contracts offer unlimited, free access to the wireless system for city purposes in exchange for the company being able to install wireless routers on light poles and other publicly-owned infrastructures, and to be able to sell wireless services to the community members.⁴² In some cases, cities both get free access and are paid additional funds for the "rental" of the light poles and other city re-

36. *Wi-Fi America* (NPR Media Transcript Jan. 5, 2007), available at <http://www.onthemediamedia.org/transcripts/2007/01/05/05>.

37. *Id.*

38. Kim, *supra* note 19, at F-1.

39. *Id.*

40. See WIRELESS BROADBAND INTERNET ACCESS NETWORK AGREEMENT BETWEEN THE CITY AND COUNTY OF SAN FRANCISCO AND EARTHLINK, INC. § 11.2.4 at 23, http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/process/SanFrancisco.Wireless.Network.Agreement.Final.pdf [hereinafter SAN FRANCISCO AGREEMENT].

41. Wireless companies are anxious to obtain contracts with cities since a contract can translate into significant revenue for the company through the sale of paid internet services to community members and increased advertising revenue due to greater volume of internet users for their services. For a full discussion, see *infra* Part II.B.

42. See, e.g., CITY OF SANTA MONICA, REQUEST FOR PROPOSALS TO PROVIDE CITYWIDE BROADBAND WIRELESS NETWORK 2006, <http://www.muniwireless.com/reports/docs/SantaMonica-wirelessRFP.pdf>; see also Esme Vos, *Long Beach, CA Issues RFP for Citywide Wireless Network*, MUNIWIRELESS, Feb. 6, 2006, <http://www.muniwireless.com/article/articleview/5014/1/23/>; Esme Vos, *Santa Monica Issues RFP for Citywide Wi-Fi Network; Interview with City CIO*, MUNIWIRELESS, Apr. 28, 2006, <http://www.muniwireless.com/article/articleview/5154/1/23/>.

sources.⁴³ For example, EarthLink is paying San Francisco a \$600,000 non-refundable, lump-sum payment and 5% of its quarterly gross revenues.⁴⁴ Hence, for many cities, municipal wireless is a win-win situation—the city gets greater access to the Internet, saves money on existing and future expenses, and may even make some money in the process.

3. Economic Development

Cities are also attracted to municipal wireless with the hope that it will spur greater economic development. While it appears that no thorough studies have been conducted that show that wireless has such an impact, cities hope that such an infrastructure will provide an extra incentive for businesses to locate in the community, will encourage conventions to come to the city, will bring visitors to hotels and restaurants, and will build a more vibrant downtown community in which high-income professionals choose to live, work, and play.⁴⁵ Some communities even look to public wireless networks as a panacea for high rates of unemployment, with inexpensive access to a wireless network somehow turning an inactive workforce into entrepreneurs.⁴⁶

4. Digital Divide

Finally, some city officials see municipal wireless as a low-cost way to bridge the disparity of access to technological resources among members of a community, often referred to as the digital divide. Many municipalities frame the decision to install wireless as one primarily motivated by an interest in providing more access to low-income individuals and those living in rural areas where it is difficult to obtain broadband access.⁴⁷ When Mayor Gavin Newsom introduced the San

43. See SAN FRANCISCO AGREEMENT, *supra* note 40, at 10; see also San Francisco Tech-Connect Process Index Website, http://www.sfgov.org/site/tech_connect_index.asp?id=52501 (last visited Feb. 27, 2007).

44. SAN FRANCISCO AGREEMENT, *supra* note 40, at 10–11.

45. See David Essex, *Cities Make Financial Sense of WiFi Projects*, GOV'T COMPUTER NEWS, Sept. 18, 2006, http://www.gcn.com/print/25_28/41979-1.html.

46. *Id.*

47. See BOSTON FOUND., BOSTON UNPLUGGED: MAPPING A WIRELESS FUTURE 5 (2006), <http://www.cityofboston.gov/wireless/wirelessdocuments.asp> (discussing work of community leaders to bridge the digital divide). In Boston, sixty percent of the households and close to eighty percent of the Boston public school children do not have internet access at home. *Wi-Fi America*, *supra* note 36. Rural communities often have difficulty in obtaining internet service. See *Widening the Internet Highway to Rural America* (NPR All Things Considered Dec. 14, 2005), available at <http://www.npr.org/templates/story/story.php?storyId=5053488>.

Francisco wireless program, its impact on the digital divide took center stage: "San Francisco TechConnect is a strategy to promote digital inclusion by ensuring affordable internet access, affordable hardware, community-sensitive training and support, and relevant content to all San Franciscans, especially low-income and disadvantaged residents."⁴⁸ When EarthLink and Google were selected as the vendors, the city also focused on the digital divide issues, stating that "[t]his agreement to bring free universal wireless internet access to San Francisco is a critical step in bridging the digital divide that separates too many communities from the enormous benefits of technology."⁴⁹

The framing of municipal wireless as a digital divide issue can help build a broad base of support for the city's initiative and draw attention away from the other city incentives, such as law enforcement interests, that undergird many of the efforts to institute municipal wireless. However, the unfortunate reality is that municipal wireless often does much more for cities and for the bottom line of companies than it does for disadvantaged members of the community.

A municipal wireless system does not solve the digital divide problem because individuals still need to have a wireless device in order to access the Internet and often must pay for a monthly municipal wireless service. Computers are still out of reach for many low-income Americans, with laptops and desktops costing several hundred dollars.⁵⁰ While there are some innovative programs, like MIT's One Laptop Per Child ("OLPC"), which is trying to develop a \$100 laptop,⁵¹ the digital divide persists. Even in San Francisco, a city near the hub of technological innovation, with one of the lowest poverty rates in the country, 15,000 low-income families and 45,000 low-income households did not have home computer access in 2003.⁵²

48. San Francisco TechConnect Homepage, http://www.ci.sf.ca.us/site/tech_connect_page.asp?id=33899 (last visited Feb. 26, 2007).

49. *Id.*

50. Dell Computers Products Page, <http://www.dell.com/content/products/category.aspx?latit?c=us&cs=04&l=en&cs=bsd&~ck=mn> (last visited Feb. 26, 2007).

51. MIT Media Laboratory, One Laptop per Child Project, <http://laptop.media.mit.edu/> (last visited Feb. 27, 2007).

52. DEP'T OF TELECOMM. & INFO. SERVICES, CITY OF SAN FRANCISCO, SAN FRANCISCO DIGITAL INCLUSION STRATEGY 11 (Oct. 18, 2006), *available at* http://www.ci.sf.ca.us/site/uploadedfiles/dtis/tech_connect/DraftSFDigitalInclusionFramework.pdf [hereinafter DIGITAL INCLUSION STRATEGY]. The United States Census defines families as "a group of two people or more (one of whom is the householder) related by birth, marriage, or adoption and residing together" and compared to a household, which "consists of all the people who occupy a housing unit." U.S. Census Bureau, Current Population Survey (CPS)—Definitions and Explanations, <http://www.census.gov/population/www/cps/cpsdef.html> (last visited Apr. 3, 2007). "With a poverty rate of 10 percent in San Francisco and 11 percent in

If an individual is able to overcome financial obstacles and acquire a computer, many of these municipal wireless programs have continuing costs that may be difficult to afford.⁵³ For example, the discounted service to low-income San Franciscans is still \$12.95 per month or "a price mutually agreed upon by the Parties."⁵⁴ In Philadelphia, Pennsylvania, individuals making less than \$13,000 per year will still have to pay \$9.95 per month for wireless service.⁵⁵ These rates are more than twice the cost of subsidized local telephone service and may price many low-income families out of the opportunity to have internet access.⁵⁶ Further, many of the discounted wireless systems may be so slow or may not work effectively indoors, making it less useful for low-income individuals for whom this would be their primary or only way to access the Internet.⁵⁷

San Jose, the two cities also were among the 10 cities nationwide with the lowest poverty rates." Jason B. Johnson, *U.S. Census Finds More Are Poor, but Number Lacking Health Insurance Remains Steady*, S.F. CHRON., Aug. 31, 2005, at A-2, available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/C/a/2005/08/31/MNGR9EFN5I1.DTL>.

53. Governor Mitt Romney proposed legislation to spend \$54 million to buy one of the \$100 laptops for every elementary school student in Massachusetts. See BOSTON FOUND., BOSTON UNPLUGGED: MAPPING A WIRELESS FUTURE, *supra* note 47, at 7. Boston is also sponsoring a program to aid low-income families in purchasing a computer. WIRELESS TASK FORCE, CITY OF BOSTON, WIRELESS IN BOSTON WIRELESS TASK FORCE FINAL REPORT BROADBAND FOR BOSTON 15 (July 31, 2006), <http://www.cityofboston.gov/wireless/Boston%20Wireless%20Task%20Force%20Report%20-%20Final.pdf>. San Francisco proposes to fund a similar project in its Digital Inclusion Strategy. DIGITAL INCLUSION STRATEGY, *supra* note 52, at 10. Other cities have proposed similar programs. See, e.g., SAN DIEGO FUTURES FOUND. & DELL COMPUTERS, A BLUEPRINT: FROM DIGITAL DIVIDE TO DIGITAL PROVIDE (Nov. 2001), <http://www.dell.com/downloads/us/slgs/digital.pdf>; Seattle Community Technology Program, <http://www.seattle.gov/tech/> (last visited Mar. 23, 2007); THE WIRELESS PHILADELPHIA EXECUTIVE COMM., WIRELESS PHILADELPHIA BUSINESS PLAN (Feb. 9, 2005), http://www.wirelessphiladelphia.org/documents/Wireless_Philadelphia_Business_Plan_.pdf; WIRELESS MINNEAPOLIS, DIGITAL INCLUSION TASK FORCE, FINAL REPORT (July 17, 2006), <http://www.digitalaccess.org/documents/MDITF%20complete.pdf>.

54. SAN FRANCISCO AGREEMENT, *supra* note 40, § 11.1.2 at 23.

55. *Wi-Fi America*, *supra* note 36.

56. Regular local plans offered by AT&T California are \$13.95 per month. AT&T General Information, <http://www.att.com/att-phone-service.html> (last visited Mar. 23, 2006). The Universal Lifeline service gives individuals and families that make up to \$29,200 the same service at fifty percent of the cost. AT&T, Low Income Phone Service in California, http://www02.sbc.com/Products_Services/Residential/1,68-1-3-3,00.html (last visited Mar. 23, 2006).

57. Susannah Patton, *Wi-Fight*, CIO MAGAZINE, Apr. 1, 2006, <http://www.cio.com/archive/040106/WiFi.html>. "The Network may provide multiple Premium Services, provided that the Network shall include at least one product that has a minimum average symmetric throughput of one (1) Mbps." SAN FRANCISCO AGREEMENT, *supra* note 40, § 11.1.1 at 23. "The Basic Service will be available at a minimum average symmetric throughput of 300 Kbps (best effort) . . ." *Id.* at 24. Silicon Valley has given up on indoor coverage because it would be too expensive. Kim, *supra* note 19, at F-1.

City officials may highlight the potential of municipal wireless networks to bridge the digital divide, however, the end result of many contracts may actually be the perpetuation of unequal access to technological resources. The city may receive greater access to the Internet, and middle class or wealthy individuals may get cheaper or greater access to the Internet, but disadvantaged members of the community may still be without access to the resources available on the Internet because of the expenses of computers, monthly service payments, and the inability of the service to work indoors and at fast enough speeds to enable effective internet access.

B. The Incentive for Companies

Companies are not putting up wireless networks as a favor to city governments. These companies are aggressively competing for wireless contracts because each one translates into the potential to tap into a lucrative market that until now has been largely controlled by the telecommunications and cable companies.⁵⁸ As discussed above, municipal wireless networks normally operate using a mesh network. The mesh network architecture innovatively works around the infrastructure advantages held by the telecommunications companies. Phone companies and cable providers have spent billions of dollars and many years installing poles and wires throughout communities in the United States. When the commercial Internet came into existence, these companies used their existing infrastructure to provide internet access in addition to their existing telephone or cable service.⁵⁹ It would be very expensive for a wireless company to duplicate this level of investment, and with little incentive for telecommunications and cable companies to share their infrastructure with a competitor, it was difficult for wireless companies to enter the market.⁶⁰ However, a mesh network and a city contract that allows a company to install wireless routers on existing city infrastructure enable new companies to enter the internet provision market.⁶¹

58. Jesse Drucker, Kevin J. Delaney, & Peter Grant, *Google's Wireless Plan Underscores Threat to Telecom*, WALL. ST. J., Oct. 3, 2005, available at <http://online.wsj.com/article/SB112812593526357432.html>.

59. Patton, *supra* note 57.

60. *Id.*

61. See Jim Hu, *Cable, DSL Face Threats*, CNET NEWS, July 29, 2004, http://news.com.com/Broadband+Cable+DSL+face+threats/2009-1034_3-5261385.html (noting the cost savings of companies providing wireless internet access by mounting wireless relay stations on private property, which are comparable to cost savings from attaching wireless relay stations to municipal property).

Municipal wireless contracts put companies like EarthLink in a position to create networks without an overwhelming initial investment and then make money by also selling wireless internet connections. This business model is not just their traditional model for selling internet services. For instance, Philadelphia awarded EarthLink the contract to build its municipal wireless system, allowing it to bypass Comcast cable lines and creating a huge opportunity for potential profit.⁶² A wireless network is relatively inexpensive to build, costing between \$25,000 and \$100,000 per square mile.⁶³ Internal EarthLink research reveals that the company expected to get a return on its investment in just two years—with 50,000–80,000 subscribers paying \$22 per month for service by the middle of 2007.⁶⁴ The company further estimates that it could have as many as 600,000 subscribers in Philadelphia.⁶⁵ Industry analysts expect municipal wireless to become a \$1.2 billion market by 2010.⁶⁶ With every new subscriber, a company like EarthLink makes money by selling the internet connection, in its traditional capacity as an internet service provider, and by selling targeted advertising.⁶⁷

Even with business models in which subscribers do not pay a fee, like that offered by Google in San Francisco, municipal wireless providers may still make profits. The more people who are able to access the Internet, the more potential use of internet search services and other products, which could in turn lead to advertising revenue.⁶⁸ Further, if an individual accesses the Internet by logging onto a Google municipal wireless connection, that connection will track who they are through their login name, what internet sites they have visited, and the approximate location from which they have logged on.⁶⁹ Through

62. *Wi-Fi America*, *supra* note 36.

63. Olga Kharif, *EarthLink's Big Bet on Broadband: Will Building Municipal Wi-Fi Networks Pull the Company Out of Its Dial-Up Doldrums?*, BUSINESSWEEK ONLINE, June 2, 2006, http://www.businessweek.com/technology/content/jun2006/tc20060602_708224.htm?campaign_id=rss_tech.

64. *Id.*

65. *Id.*

66. Kristina Dell, *Welcome to Wi-Fi-ville*, TIME, Jan. 5, 2007, <http://www.time.com/time/magazine/article/0,9171,1574164-3,00.html>.

67. Kharif, *supra* note 63.

68. Ryan Kim, *Google Gives City Free Wi-Fi: Mountain View Service Could Give S.F. Project a Push*, S.F. CHRON., Aug. 16, 2006, at C-1, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/C/a/2006/08/16/BUGVJKJERS1.DTL>.

69. See SAN FRANCISCO AGREEMENT, *supra* note 40; Letter from Christopher Sacco to Christopher Vein, *Re: Privacy and the San Francisco Municipal WiFi Initiative* (June 20, 2006), available at http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/SFGooglePrivacyResponseJune06.pdf [hereinafter *Google Privacy Response Letter*]. Unlike the privacy policy

this interaction, the company may obtain literally a wealth of data about millions of individuals. Such data may increase its ability to develop new targeted products or allow for greater targeting advertising that could sell at an even higher premium to companies.⁷⁰

The economic threat posed by municipal wireless has not been lost on established telecommunications and cable companies. Some have attempted to stifle the spread of municipal wireless with legislation on both the state and federal levels.⁷¹ Legislators sympathetic to the telecommunications industry introduced legislation to prevent wireless companies from circumventing existing telecommunications infrastructure. For example, Representative Pete Sessions (R-Texas), who worked at Bell Labs for sixteen years prior to becoming a congressman, introduced legislation in May 2005 to prohibit state and local governments from offering telecommunications, telecommunications services, information services, or cable service "in any geographic area in which a private entity is already offering a substantially similar service." According to Representative Sessions, a bill taking state and local governments out of the broadband business was "for their own good."⁷² He wanted to discourage municipal governments from wasting taxpayer funds on building duplicative infrastructure while at the same time encouraging private companies to offer continually innovating service in underserved areas by removing the specter

for the Subscriber Service provided by EarthLink, the Agreement does not provide a specific privacy policy for the Basic Service to be provided by Google; it provides merely a generally phrased privacy "standard." SAN FRANCISCO AGREEMENT, *supra* note 40, § 10.4. The Google Privacy Response Letter provides further indications of the privacy policy for the Google service. Unlike the privacy options for the Subscriber Service, there is no option for Basic Service subscribers to opt-out of location-based tracking. SAN FRANCISCO AGREEMENT, *supra* note 40, § 10.4; *Google Privacy Response Letter* at 1. Google will know the approximate location of an individual because he or she will be logging onto a particular wireless router node on a light pole—the one closest to their location. It is estimated that between thirty and one-hundred nodes per square mile are necessary for an effective municipal wireless system. Kim, *supra* note 19, at F-1.

70. Google CEO, Eric Schmidt, has spoken quite extensively about expanding targeted advertising revenue:

We are thinking about using our ad system for every form of advertising. Because it is a big opportunity to provide value to both advertisers and consumers (more targeted ads to you). One of the outcomes, if they do this right, is that you should end up with fewer but more relevant ads, in more context. Google's analysis says they have a "good shot at this."

Search Engine Roundtable, *A Conversation with Eric Schmidt*, <http://www.seroundtable.com/archives/004343.html> (last visited Mar. 23, 2007).

71. Patton, *supra* note 57; see also Dell, *supra* note 66.

72. Roy Mark, *Legislation Aims to Stop Muni Wi-Fi*, WI-FI PLANET, June 3, 2005, <http://www.wi-fiplanet.com/news/article.php/3509961>.

of government competition.⁷³ Senator John Ensign (R-Nevada) introduced Senate Bill 1504 in July 2005, which included a provision to limit local governments' abilities to deploy public broadband systems. Florida Governor Jeb Bush signed a bill similar to Sessions' federal law in 2005, and legislation creating obstacles to municipal wireless was also passed in Pennsylvania, with Philadelphia receiving an exception.⁷⁴ However, Senators John McCain (R-Arizona) and Frank Lautenberg (D-New Jersey) introduced Senate Bill 1294, a bill to preserve the ability of municipalities to offer broadband service.⁷⁵

Telecommunications and cable companies have not been successful in stopping the municipal wireless movement and, as discussed above, hundreds of cities are in the process of planning or deploying systems. These systems vary, with some being owned and operated by the city and supported through tax dollars, like that in Chaska, Minnesota.⁷⁶ However, the majority of big cities have chosen to develop their wireless networks with a private entity to reduce the cost to the city.⁷⁷ Some cities, like Boston, Massachusetts, are working with a nonprofit entity to build and operate the network and then sell network access to a range of internet service providers.⁷⁸ Other cities like Philadelphia and San Francisco have partnered with companies to both build and provide the services. Some cities have chosen to charge all residents. In Philadelphia, for example, EarthLink will provide services to the public for a fee of \$22.⁷⁹ Other cities, like San Francisco, have a mixed system, in which they have partnered with EarthLink, to sell a service with a monthly charge, and with Google, to provide a no-fee service at slower speeds.⁸⁰ Some systems have no fee at all attached, such as Google's partnership with the city of Mountain View, California.⁸¹

73. *Id.*

74. *Id.*

75. Patton, *supra* note 57.

76. See TROPOS NETWORKS CASE STUDY, Chaska, Minn., Chaska.net and Tropos Unwire 3 (June 2005), http://www.tropos.com/pdf/chaska_casestudy.pdf.

77. Khali Henderson, *Public-Private Partnerships for Muni Wireless Evolving, Expert Says*, XCHANGE ONLINE, Feb. 14, 2007, <http://www.xchangemag.com/hotnews/72h1417239.html>.

78. Essex, *supra* note 45 at 5.

79. *Wi-Fi America*, *supra* note 36.

80. Dawn Kawamoto, *EarthLink and Google Win San Francisco*, CNET NEWS, Apr. 6, 2006, http://news.com.com/EarthLink+and+Google+win+San+Francisco+Wi-Fi+bid/2100-7351_3-6058432.html.

81. Elinor Mills, *Google Blankets City with Free Wi-Fi*, CNET NEWS, Nov. 16, 2005, http://news.com.com/Google+blankets+city+with+free+Wi-Fi/2110-7351_3-5956837.html.

III. Safeguarding Privacy and Free Speech

Whether subscribers pay a monthly fee or no fee, many of the wireless proposals being considered by cities are ending up as bad bargains for individuals. In addition to any dollar costs and city resources, people are also being asked to pay for these proposals with their privacy and free speech rights. Many of the business models are based in whole, or in part, on tracking personal information to use for targeted internet products and advertising. This type of business model gives companies an incentive to collect as much information about people and to keep it as long as possible in order to be able to reap the greatest economic benefit.

A municipal wireless business that tracks the identity of users, what they are viewing on the Internet, and the location of where they are looking at it, may create higher advertising revenue, but it also has the potential to invade people's privacy and chill their ability to learn about sensitive topics. Fewer people will feel safe using a municipal wireless system to access sensitive information if they have to worry about who is watching their activities, where the information will end up, or how it will be used. Tracking user patterns and maintaining such records creates a wealth of information that may be of interest to government officials who would like access to such information for other purposes. Municipal wireless is meant to benefit the public, not increase the profits of business and create a new tool for intrusive monitoring of Americans.

Particularly in light of recent revelations about illegal and unconstitutional spying on Americans, it is important that there be safeguards to ensure that private information is properly protected. Adequate protections for privacy and free speech in municipal wireless systems are not merely aspirational. When government entities are engaged in establishing a system that provides public electronic communications services, it may constitute "state action" for constitutional purposes and thus require compliance with the dictates of both the United States Constitution, including the First and Fourth Amendments, and state constitutions. As a city considers the implementation of a municipal wireless network, it must thoroughly address the privacy and free speech implications and require companies to include adequate protections for these fundamental civil liberties. There are several general safeguards that should be in place for any municipal wireless system which will be outlined in the following sections.

A. User Identities and Online Activities Should Not Be Tracked, Recorded, or Commercialized

A wireless provider must know some information about a computer in order to route internet content, however, the company does not need to know anything more about the individual who is accessing the Internet or keep any records about what sites a user visits. A municipal wireless service provider might prefer to require personal information about users, such as names, addresses, e-mails, and unique usernames, and track internet activities so that it can create detailed profiles to use for targeted advertising, for selling, or for trading to third parties. However, such tracking and profiling is unacceptable in a municipal wireless network because it threatens both an individual's right to privacy and First Amendment rights to speak and associate anonymously. Such tracking and profiling makes it difficult for individuals to maintain control over sensitive information about their activities and will chill their ability to access constitutionally protected information due to fear that their internet searches, activities, or interests might become known to others.

1. Invades Privacy

Privacy rights are guaranteed by the Fourth Amendment prohibition against unreasonable search and seizure and in some states, such as California, by a state constitutional right to privacy.⁸² Article I, Section 1 of the California Constitution guarantees an "inalienable" right to privacy.⁸³ The Privacy Amendment, overwhelmingly passed by ballot proposition in 1972, was specifically intended to safeguard informational privacy by preventing the expansion of data collection and the potential misuse of such personal data by the government and third parties. Proposition 11 stated:

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

82. U.S. CONST. amend. IV. ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

83. CAL. CONST. art. 1, § 1. ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

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.⁸⁴

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.⁸⁵ The “ability to speak one’s mind without the burden of [another] party knowing all the facts about one’s identity can foster open communication and robust debate.”⁸⁶

In *White v. Davis*,⁸⁷ the first California Supreme Court case to interpret the Privacy Amendment, the court further solidified rights to informational privacy.

[T]he moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision’s primary purpose is to afford individuals some measure of protection against this modern threat to personal privacy.⁸⁸

As an inalienable right, a citizen’s privacy is not to be bought, sold, or bargained away, and cities entering into contracts for municipal wireless systems must take these rights into account.⁸⁹

2. Chills Speech

Allowing municipal wireless systems to track, record, or commercialize user identities and activities will also chill protected speech. The Internet has been integral in giving people of all ages better overall access to information and an outlet to seek answers.⁹⁰ Within the privacy of a computer screen, an individual may feel safer finding information, asking questions, and purchasing items that otherwise

84. CAL. SEC’Y OF STATE, PROPOSED AMENDMENTS TO CONSTITUTION FOR THE NOVEMBER 7, 1972 ELECTION 27 (1972), available at http://library.uchastings.edu/ballot_pdf/1972g.pdf.

85. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

86. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

87. 533 P.2d 222 (Cal. 1974).

88. *Id.* at 774.

89. *See, e.g.*, CAL. CIV. CODE § 1798.84(a) (West 2000) (making waivers of a variety of California-specific privacy protections inalienable by contract); Consumer Credit Reporting Agencies Act, CAL. CIV. CODE § 1785.36 (West 2000).

90. PEW INTERNET AND AMERICAN LIFE PROJECT, DATA MEMO 1 (Apr. 2006) http://www.pewInternet.org/pdfs/PIP_Internet_Impact.pdf.

might have been too embarrassing or difficult in the physical world. From health conditions, to reproductive options, to lesbian, gay, and bisexual information, to news about current events and politics that might differ from the prevailing viewpoint in a particular community—more and more people are turning to the Internet as a resource.⁹¹

A municipal wireless system that allows the tracking and profiling of users threatens to undermine the potential power of municipal wireless as a public service. People will have to stop and wonder whether it will be safe for them to use the Internet as a trusted resource. “No matter how innocent one’s intentions and actions at any given moment . . . persons would think more carefully before they did things that would become part of the record.”⁹² Once individuals know they are being “observed and recorded, their habits change; they change.”⁹³ When we are watched, we are more self-conscious, we worry about what others think, and our actions are influenced. “To the extent that a person experiences himself as subject to public observation, he . . . will tend to act in ways that are publicly acceptable.”⁹⁴ A municipal wireless system that tracks and profiles users migrates the social conformity barriers that keep people from accessing necessary information in the physical world to the municipal wireless system. In this way, rather than bridging the digital divide, the municipal wireless system could add a worrisome barrier to internet usage that could further impede equal access to important information.

3. Additional Harms

In addition to invading privacy and chilling speech, a municipal wireless service that monitors and tracks internet usage could lead to other harms. Tracking browsing habits and using it to target advertising could lead to users receiving physical mail, phone solicitations, e-

91. Seventy-three percent of Americans now use the Internet; twenty percent of Americans report that the Internet has “greatly improved the way they get information about health care.” *Id.*

92. Richard Wasserstrom, *Privacy: Some Arguments and Assumptions*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY 325–26 (Ferdinand David Schoeman, ed., 1984), cited in Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 243 (2002).

93. Nicholas C. Burbules, *Privacy, Surveillance, and Classroom Communication on the Internet*, ACCESS (1997), available at <http://faculty.ed.uiuc.edu/burbules/papers/privacy.html> (last visited Mar. 23, 2007), cited in Slobogin, *supra* note 92, at 244.

94. See Jeffrey Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 38–41 (1995), cited and discussed in Slobogin, *supra* note 92, at 243.

mails, or pop-up advertisements about particular products or topics. The results might be categorized as mere annoyances, such as receiving information about a competitor's products when you search for a particular item. Sometimes they could be frustrating, such as a family member seeing information sent to your home or to a shared laptop that ruins a surprise present or dream vacation. Others could be very serious. For instance, if a family computer is used to research a sensitive and very private issue such as health concerns or political activity, it is very possible that a later user of the same computer could be presented with advertising pertaining to that earlier browsing and learn information that the original user really needed to keep private. Such monitoring could also lead to unforeseen government uses of sensitive data about health issues and political involvement.

4. Privacy and Free Speech Protections Necessary for Equal Access

Ensuring that municipal wireless systems have adequate privacy and free speech safeguards is particularly important if bridging the digital divide is indeed a primary goal of the system. The goal of equal access to information is undermined without such safeguards. Rather than reducing the digital divide, a municipal wireless system would instead perpetuate a further divide. People who have money can select another internet service provider with more privacy and free speech-friendly provisions, while those who cannot afford to pay money for internet access will be forced to pay for it with their privacy and free speech. It is imperative that cities deploy systems that properly safeguard privacy and free speech and enable everyone to feel comfortable accessing sensitive information. Accordingly, municipal wireless systems should not track, record, and commercialize user identities and online data.

B. The Service Must Be Prepared to Resist Demands for Users' Personal Data

Service providers inherently face pressures from other network users, industries, and governments to disclose personal information about their users. 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 iden-

ties.”⁹⁵ Typically, when user information is sought, the service provider is the first entity informed of the request.

This issue is especially sensitive in the municipal wireless context, where the same state actor may be involved in the provision of service and the request for information. A municipality may face additional pressures from its own city services to set low thresholds for law enforcement and other agencies to obtain information about individuals’ internet use. There should be high standards for and narrow circumstances in which personal information will be disclosed to law enforcement and in civil litigation. The service provider should be prepared to litigate to avoid disclosing data if the request is legally insufficient. Except in circumstances where law enforcement presents a court order binding the service provider to secrecy, the service provider also should provide the user with notice prior to disclosing the information.

A municipal wireless program should have adequate policies and procedures to allow users a real opportunity to protect their personal information, including: (1) providing notice, within no more than seven days of receipt of a subpoena, to each person whose personal information is sought; (2) allowing the user at least fourteen days from the time notice is received to file a motion to quash; and (3) not disclosing any information prior to the disposition of any motion to quash.

C. Municipal Wireless Providers Should Only Collect Minimum Amounts of Information and Maintain User Logs for the Least Amount of Time Possible

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. Since any information held by this third-party service provider is unfortunately not protected by the Fourth Amendment because of the third party doctrine, it will be susceptible to a broad range of law enforcement requests.⁹⁶ As a result, any municipal wire-

95. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

96. *See United States v. Miller*, 425 U.S. 435 (1976) (Fourth Amendment does not apply because there is no reasonable expectation of privacy in banking records, including financial statements and deposit slips, because information is voluntarily revealed to the third-party bank); *see also Smith v. Maryland*, 442 U.S. 735, 742–43 (1979) (Fourth Amendment does not apply because there is no expectation of privacy in numerical information

less service provider must deal with requests from law enforcement and lawyers to hand over private user information and logs.

Reducing the amount of information collected and the time that the system stores that information will enhance privacy and reduce the costs and burdens of responding to requests for user data. 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. Cities should ensure that municipal wireless vendors adopt clear procedures to limit the amount of data collected and the duration of time that it is kept. Clear policies will conserve resources, help safeguard private data, and preserve freedom of expression online.

D. Personal Data Should Be Protected from Others

Cities must also ensure that wireless network providers take measures to protect information transmitted by users from interception by others, or people will not feel comfortable using a municipal wireless network for sensitive personal activities. The WiFi standard was cracked by researchers in 2001, and recent reports have also shown just how easy it is to pick up the 2.4 GHz radio frequency. It is widely acknowledged by leading security experts that WiFi is extremely vulnerable to intrusion, even when the networks have an initial layer of protection through encryption. Tools necessary to attack the system and access sensitive data are "freely available on the internet."⁹⁷ In addition to ensuring that municipal wireless networks incorporate adequate technological protections, users should be educated about the full protections available on the network and ways to best protect their personal information.

E. Free Access to Information—No Filtering

In order for a municipal wireless system to accomplish its goal of increasing access to information, it also must not filter constitutional content. Contract provisions that require individuals to waive access to the full range of internet content, as well as technological measures

about telephone records held by telephone company since individuals "know that they must convey numerical information to the phone company" and so cannot "harbor any general expectation that the numbers they dial will remain secret.").

97. Marc Delehanty, *Wifi Links Vulnerable Even with Encryption*, PERS. COMPUTER WORLD, July 27, 2006, <http://www.crn.com.au/story.aspx?CIID=57402>.

installed on the system that filter out available content, are incompatible with the First Amendment. Filtering content also undermines the goal of bridging the digital divide, creating a system in which people who have money and can pay for other forms of internet access get full access to information, while others only get a portion of the information. All Americans have the right to free speech and access to information. It is improper for municipal wireless systems to filter content and infringe on these rights.

IV. Case Studies: Privacy and Free Speech Safeguards in Existing and Developing Municipal Wireless Programs

Several cities are taking steps to protect some aspects of privacy and free speech. For example, the Philadelphia wireless contract provides subscribers with the opportunity to opt-out of data collection as well as receiving marketing information.⁹⁸ Personal information also cannot be sold, rented, or given away to third parties.⁹⁹ Portland's agreement also provides some positive protections for the personal information of users. Portland's service provider may not collect more "personally identifiable information beyond what is required to operate Services and will only share information for purposes necessary to operate Services, except as required by law or authorized by this Agreement."¹⁰⁰

However, much more must be done to safeguard the privacy and free speech of individuals. It is wholly improper for cities like Boston and Philadelphia to publish vision and business plan documents that do not contain a single word about privacy and free speech.¹⁰¹ Request for Proposals ("RFPs") from regions like Silicon Valley should not only ask vendors how fast the network will operate for the munic-

98. WIRELESS PHILADELPHIA BROADBAND NETWORK AGREEMENT, EXHIBIT R: PRIVACY REQUIREMENTS at R-1 through R-2 (2003), http://www.wirelessphiladelphia.org/documents/WP_EL_Network_Agreement_Exhibits.pdf.

99. *Id.* at R-2.

100. UNWIRE PORTLAND, NETWORK CONNECTIVITY LICENSE AGREEMENT, NONEXCLUSIVE LICENSE 22 (June 22, 2006) <http://www.portlandonline.com/index.cfm?a=129511&c=43149>. The agreement goes on to define personally identifiable information as including, but not limited to, "any identifiers that are linked to the individual, such as "usernames" assigned by service, e-mail addresses, given names, street addresses, phone numbers, other personally identifiable demographic data, and other sensitive or personal financial information, such as credit card numbers, login IDs, passwords or bank account numbers." *Id.*

101. WIRELESS TASK FORCE, CITY OF BOSTON, *supra* note 53; WIRELESS PHILADELPHIA, REQUEST FOR PROPOSALS FOR A CITYWIDE WIRELESS NETWORK (Apr. 5, 2005), http://www.wirelessphiladelphia.org/pdfs/WP_RFP_4-5-05_rev_v4-CLEAN.pdf.

pality, but also whether the network will safeguard the privacy and free speech rights of its citizens. Cities like Culver City, California, should not have municipal wireless programs that have software filters that stop individuals from accessing constitutionally protected speech and require them to waive their First Amendment rights to use the systems.¹⁰²

Many cities across the country look to the Bay Area as a model for innovation and methods to safeguard the rights of individuals. However, thus far, neither San Francisco nor Silicon Valley has succeeded in developing a municipal wireless system that adequately safeguards the rights of its people and really provides equal access to information.

A. San Francisco

Municipal wireless in San Francisco started in a promising manner. The city stated in its request for proposals that “the City anticipates a Network that protects the privacy of users, respects consumer choice, and fosters diversity of information and ideas.” The city also asked a specific question in the RFP about privacy, requiring 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,” but, when the proposals were submitted, the privacy and free speech rights of residents were largely overlooked by almost all the vendors.¹⁰³ The vendor proposals contained wholly inadequate safeguards against user tracking and commercialization of data. There were few limitations on the amount of information collected and how long it was kept and few pledges for how the companies would protect private information from third-party demands. The joint proposal by EarthLink and Google, which was ultimately selected by San Francisco, contained truly abysmal privacy and free speech protections.¹⁰⁴

The final contract between San Francisco and EarthLink and Google made little progress.¹⁰⁵ The contract not only failed to provide options for anonymity, but it did not actually limit the amount of personal information that could be collected about users and how it was

102. Dell, *supra* note 66.

103. For a comparison chart of vendors and privacy and free speech recommendations, see ACLU-NC & Electronic Privacy Information Center, *A Privacy Analysis of the Six Proposals for San Francisco Municipal Broadband*, Feb. 21, 2006, at 6–11, http://aclunc.org/issues/technology/asset_upload_file655_4446.pdf (last visited Feb. 27, 2007).

104. See *infra* Appendix A; see also SAN FRANCISCO RFP RESPONSE, *supra* note 24, at 141–54.

105. SAN FRANCISCO AGREEMENT, *supra* note 40.

commercialized. The only safeguards in place for the amount of personal information that could be collected was that Google (no fee service) agreed to collect "minimal information" about the user during registration and log-in; however, "minimal" was not defined in the contract.¹⁰⁶ Additionally, EarthLink, but not Google, agreed to allow individuals to opt-out of tracking their location information. Aside from requiring that EarthLink not store location information about users for more than sixty days, there were also no limits to how long either company could maintain logs of user information and transactional data. In terms of resisting demands for users' information, the companies were allowed broad disclosure provisions. They can provide information, without requiring a warrant, and without providing prior notice, for law enforcement and national security investigations. The companies did say, though, that when allowed by law, they shall require "court ordered documentation." In response to a civil legal demand, both companies will provide notice to the individual prior to disclosing the information, when allowed by law. However, the timing of the notice, and whether it would afford the user an ability to move to quash, was not delineated.¹⁰⁷ After almost two years, San Francisco is still considering a contract that has little protections for the fundamental rights of individuals.

B. Silicon Valley Regional Wireless Plans Have Inadequate Privacy and Free Speech Protections

The future for privacy and free speech in Silicon Valley may be even worse. In April 2006, Joint Venture Silicon Valley, a non-profit business-government coalition in San Jose, California, released an RFP for the development of a very ambitious region-wide wireless system.¹⁰⁸ The system would cover forty-two cities across a region of 1500 square miles, with a population of 2.4 million.¹⁰⁹ Nothing in the extensive vision and planning documents discussed privacy and free

106. *Id.* at 22.

107. Before the wireless network is built, the Board of Supervisors and the Public Utilities Commission must approve the system. At the time of writing, this process has not yet been completed. SAN FRANCISCO AGREEMENT, *supra* note 40, at 14, 47.

108. WIRELESS SILICON VALLEY, SAN MATEO COUNTY TELECOMM. AUTH., REQUEST FOR PROPOSAL FOR A REGIONAL BROADBAND WIRELESS NETWORK FOR SILICON VALLEY (Apr. 28, 2006), <http://www.jointventure.org/programs-initiatives/wirelessiliconvalley/documents/Wireless%20Silicon%20Valley%20RFP%20April%2028%202006.doc> [hereinafter SILICON VALLEY RFP].

109. Press Release, IBM, 2.4 Million Silicon Valley Residents Go Wireless (Sept. 6, 2006), http://www.marketwire.com/mw/release_html_b1?release_id=160114.

speech considerations.¹¹⁰ Prior to the release of the Request for Proposals in April, the ACLU-NC, along with the Electronic Frontier Foundation ("EFF") and the Electronic Privacy Information Center ("EPIC"), submitted a letter detailing the privacy and free speech concerns that must be taken into account when selecting a municipal wireless vendor. These 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.

Wireless Silicon Valley declined to include a specific question about privacy or free speech in the RFP, but rather agreed to ask each vendor to submit its end-user license agreement ("EULA")—the agreement that a customer clicks on and agrees to prior to using the system. Wireless Silicon Valley also pledged at the request for proposal release event to take privacy and free speech into account in its decision. The organizations expressed at that time that without a specific question in the request for proposal, the vendors would not properly address privacy and free speech issues. As feared, the EULAs submitted were extremely general and none of the three proposals selected by the task force as finalists, MetroFi, VeriLan, or Silicon Valley Metro Connect, even discussed privacy or free speech apart from merely stating that its EULA was attached to the proposal. A careful reading of the EULAs resulted in finding that each of the proposals had deep privacy and free speech flaws.¹¹¹ Follow-up meetings and a public forum followed, including presentations about privacy and free speech issues.

However, Wireless Silicon Valley chose a vendor, MetroConnect (a consortium of Cisco, IBM, and others), whose proposal contained very few privacy and free speech safeguards. Its proposal required a user login tied to the user's address and credit card, which allowed for what the proposal even described as "user tracking." Neither the proposal nor the EULA contained any limitations on how MetroConnect would share user data with third parties or how user data would be tied to targeted advertisements. It also had no proper safeguards for resisting demands for user information. The company planned to disclose personal information in response to criminal and civil subpoenas, without giving users any notice. Finally, there were no limitations on how long data would be stored about users. Following the selection

110. SILICON VALLEY RFP, *supra* note 108.

111. *Id.* at Appendix C.

of MetroConnect, Wireless Silicon Valley pledged to closely consider the privacy and free speech concerns and asked professors from Stanford University Law School and Santa Clara University School of Law to research and submit models for privacy policies and contract terms that would incorporate adequate safeguards.¹¹² These professors presented their findings to Wireless Silicon Valley, but there has been no public action yet taken to incorporate their suggestions.

Conclusion

Municipal wireless has the potential to be an important public service, increasing access to the Internet for many community members. But, as technology advances, civil rights cannot be left behind. Many of the business models currently being considered for systems around the country do not have adequate safeguards for privacy and free speech. Without these protections, the civil liberties of individuals will be infringed. The goal of municipal wireless to provide increased access to information will also be undermined because individuals cannot feel comfortable using the service to access sensitive information if they are not assured that such information will remain private. Forty years ago in *Katz*, the Supreme Court ensured that conversations on public telephones would remain private. Now, steps must be taken to safeguard the privacy and security of internet activities on municipal wireless systems. As cities usher in a new communications infrastructure for their citizens, they must take care that individuals are not forced to pay for the system with their privacy and free speech rights.

112. Stanford Law School, The Center for Internet and Society, <http://cyberlaw.stanford.edu/node/3179> (last visited Mar. 7, 2007) (posting PDF versions of model privacy policies and contract terms by Lauren Gelman of Stanford Law School and Al Hammond of Santa Clara Law School).

Appendix A

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|---|--|---|---|
| What personal information is collected about users? | None, if possible. Anonymous and pseudonymous access should be available. | Name, address, telephone number, billing information, and computer information. | E-mail address. |
| How is this information used? | Only when necessary for operation of the network. | For the provision of service and marketing. | To authenticate and login users. |
| 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. | As long as needed for business purposes. | Account usage information deleted regularly; never stored more than 180 days. |
| With whom is this information stored? | Only when necessary for operation of the network. | With affiliates. | With third parties (with opt-out rights). |
| Is this information commercialized in any way? | Providers should not commercialize personal information without voluntary, opt-in consent. | To market EarthLink services and to third parties (with opt-out rights). | Yes, used for personalized content and advertising. |
| 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. | Yes. | Yes, but it is regularly deleted. |
| 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. | Opt-out. | Opt-in for sensitive information; opt-out for other information. But this does not explain how the free service profiles and targets users based on surfing behavior. |
| 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. | Opt-out, once node-level tracking is available. | Non-responsive. |

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|--|--|---|---|
| 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. | Cookies are used, as is Doubleclick. | Cookies are used, but it appears as though users can disable them. |
| 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. | May disclose at company's sole discretion, policy does not specify whether notice to the user is given. | Yes, but policy does not specify whether notice to the user is given. |
| 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. | May access registration information. | Yes. |
| Are users provided with a mechanism to review 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. | Offers access and modification to personal information, but no apparent deletion. | Yes. |

Appendix B

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|--|---|--|---|
| What personal information is collected about users? | None, if possible. Anonymous and pseudonymous access should be available. | No limitation in contract regarding the type of information that EarthLink — can or will collect. Contract defines “Protected Personal Information” (“PPI”) for its privacy policies as “any information which personally identifies the person to which such information pertains . . . includ[ing] but not limited to: name, address, phone number, fax number, financial profiles, medical profiles, social security number, and credit card information.” Contract also defines “unique information,” including but not limited to: “a unique identifier, e-mail address, biometric information, Location Information, IP address or MAC address.” The contract classifies unique information as PPI only when it is associated with PPI and not by itself PPI. Information not connected to an identified individual in its then currently stored form is not considered PPI. | No specific limitation in contract regarding the type of information that Basic Service Provider can or will collect. “[U]sers shall be presented with options to register or login that require minimal information from the user.” (10.4.2) |
| How is this information used? | Only when necessary for operation of the network. | No limitation in contract about how EarthLink may use the collected information. | No limitation in contract about how Basic Service Provider may use the collected information. |

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|---|--|--|--|
| 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. | No limitation in contract regarding how long EarthLink can store PPI. EarthLink shall retain Location Information for no longer than sixty (60) days. However, this limitation does not apply to Aggregated Location Information ¹¹³ or as required by: (i) applicable law; (ii) an order of an governmental authority evidenced by court-supported documentation; or (iii) a pending internal investigation to determine if a fraud, crime, or network security breach of a material nature has occurred. (10.3.1.4.b) | No limitation in contract regarding how long the Basic Service Provider can store any information. |

113. Aggregated Location Information means Location Information that (a) is not associated with an individual user's PPI; or (b) is aggregated beyond the level of the individual account.

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|---|--|--|---|
| When is information shared? | Only when necessary for operation of the network. | Broad prohibition against sharing PPI with any person or entity without the voluntary, affirmative consent of the user with the following exceptions: • Third Party Suppliers ¹¹⁴ ("TPS") to deliver or promote EarthLink's services or to process pay- ments, collection, order fulfillment and service delivery. Users may opt-out of receiving marketing communications from EarthLink or TPS, but no opt-out for information-shar- ing. • Entities that jointly promote EarthLink's service to their cus- tomers. Again, users may opt out of receiving marketing communications from such entities or fro EarthLink but no opt-out for the infor- mation sharing. • Law enforcement • Other persons or entities in connec- tion with civil legal proceedings. | No contract limita- tion regarding shar- ing any information except with regard to the following: • Sharing with law enforcement • Google shall require the provider of the Basic Service, unless prohibited by applicable laws, to provide reasonable prior notice to the user before disclos- ing Basic Service PPI in response to a civil legal demand. |
| Is information com- mercialized? | Providers should not commercialize per- sonal information without voluntary, opt-in consent. | No limitations in contract regarding commercialization of data other than opt- out provision from receiving marketing communications. | No limitations in contract regarding commercialization of data. |

114. "Third Party Suppliers" means vendors or partners that provide products or services to EarthLink or the Subscribers of Fee Services on behalf of EarthLink. (1.87)

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|---|--|--|---|
| Is 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. | Yes. Login information required for access. No limitations in contract regarding the correlation of information with a specific user, with a device, or with a location. | Yes. Login information required for access. No limitations in contract regarding the correlation of information with a specific user, with a device, or with a location. Contract does stipulate that options for registration or login should "require minimal information from the user." Though contract includes no definition of what constitutes "minimal." |
| 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. | Opt-out option for location information. However, opt-out does not preclude EarthLink from using location information to: (i) enable a device to connect to the Network; (ii) provide other services which use location information from which the user has not opted out; (iii) comply with legal requests; or (iv) to protect EarthLink or its customers from a crime, fraud, or network security breaches of a material nature. | No provisions in the contract regarding any mechanisms available to allow users to opt-in or opt-out of any service that tracks information about the user's physical location. |
| 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. | No provisions in the contract for 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 uses of the Network. | No provisions in the contract for 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 user of the Network. |

| | Recommended Privacy and 1st Amendment Protections | EarthLink (monthly charge) | Google (no fee) |
|--|--|--|--|
| 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. | No specific provision in the contract regarding the assignment of a unique identifier. However, the inclusion of "a unique identifier" in the definition of "unique information" indicates the assignment of a unique identifier to users. | No specific provision in the contract regarding the assignment of a unique identifier. However, the inclusion of "a unique identifier" in the definition of "unique information" indicates the assignment of a unique identifier to users. |
| Are policies in place to respond to legal demands for users' personal information? | Providers should only provide user's personal information in response to a warrant. Unless directly prohibited by law, providers should give the user reasonable notice of the legal demand before complying. | Broad disclosure provisions without requiring a warrant and without prior notice to user for law enforcement and national security investigations, though shall require "court ordered documentation" when allowed by law. EarthLink shall provide reasonable prior notice to user, unless prohibited by law, before disclosing information in response to a civil legal demand. | Contract requires that Google at least comply with the same requirements as EarthLink. |
| 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. | No provisions in the contract to allow users to access any information collected about them. | No provisions in the contract to allow users to access any information collected about them. |
| 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. | No provisions in contract to provide users with a mechanism to review any personal information and to correct inaccuracies or delete information. | No provisions in contract to provide users with a mechanism to review any personal information and to correct inaccuracies or delete information. |

Appendix C

Users Should Not Be Tracked Between Sessions

| | Privacy Compliant? | Does the Service Track Users from Session to Session? |
|-------------------------------------|--------------------|--|
| MetroFi | No | Requires a user login that can be used to track individual usage between sessions. |
| 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. |

Server Logs Should Be Maintained for the Minimum Amount of Time Possible

| | Privacy Compliant? | Does the Service Have a Data Retention Policy that Minimizes Storage of Personalized User Data? |
|-------------------------------------|--------------------|---|
| 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. |

The Service Must Be Prepared to Resist Demands for Users' Personal Data

| | Privacy Compliant? | Are Policies in Place to Respond to Legal Demands for Users' Personal Information? |
|-------------------------------------|--------------------|---|
| MetroFi | No | Will disclose personal information in response to what MetroFi vaguely calls "legal process." Does not state whether it will resist civil subpoenas. Provides no policy giving users notice of subpoenas. |
| Silicon Valley Metro Connect | No | Will disclose personal information in response to criminal and civil subpoenas. Provides 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. Provides no policy giving users notice of subpoenas. |

The Service Should Not Attempt to Commercialize User Data

| | Privacy Compliant? | Does the Service Commercialize User Data? |
|-------------------------------------|--------------------|--|
| MetroFi | Maybe | The proposal states that "no personally identifiable information will be shared with 3rd 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. |