NO SUCH THING AS "FREE" INTERNET: SAFEGUARDING PRIVACY AND FREE SPEECH IN MUNICIPAL WIRELESS SYSTEMS

*Nicole A. Ozer**

There is no such thing as a free lunch. Unfortunately, there is no such thing as "free" Internet either. Increasing access to the Internet is a very important mission; one that cities and all sectors of the community should be striving to achieve. However, far from "free" or low-cost, many of the municipal wireless programs currently in existence and in development require residents to bear heavy burdens for the system—such as paying for the networks with monthly fees, supporting the program infrastructure with their tax dollars, and often funding the business models with their privacy and free speech rights.

The advent of wireless Internet presents the opportunity for cities across the country to build a new public communications infrastructure. The public telephone booths that were once commonplace on street corners are giving way to wireless Internet routers dangling from city light poles. These routers can form a municipal wireless network, providing blanket outdoor coverage to communities and allowing individuals to log on to the Internet and communicate from

* Nicole A. Ozer is the Technology and Civil Liberties Policy Director at the American Civil Liberties Union of Northern California (ACLU-NC). Her website and blog are available at http://www.aclunc.org/tech. Information or opinions in this Article are not necessarily that of the ACLU of Northern California. Portions of this Article were originally published in *Companies Positioned in the Middle: Municipal Wireless and Its Impact on Privacy and Free Speech*, 41 U.S.F. L. REV. 635 (2007). 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, Senior Staff Attorney, Electronic Frontier Foundation (EFF). Part III of this article is 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. Special thanks also to the ACLU-NC Technology and Civil Liberties interns Travis Brandon, Alison Watkins, Mark Melahn, Chris Cercone, Anne Kelson, and T. Elizabeth Edwards and Policy Assistant, Heather Caughron, whose research and editing contributed to this Article.

their corner bakeries or a public square. While some high-profile municipal wireless proposals have hit snags and delays or have been cancelled, there are still 415 planned or completed projects in the country, and it is estimated that cities will spend more than $686.8 million by 2009 to build these municipal networks.[1]

These municipal wireless systems have the potential to be a beneficial new communications infrastructure for communities and to equalize access to essential information. However, many of the systems currently in development fall very short of these laudable goals. The business models currently being used or 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, and they would have to listen to advertisements for products based on their conversations. There would be no guarantee that the content of their conversations would not be shared with the government and third parties. This would have been an outrageous proposition forty years ago, and it remains so today. When cities are developing municipal wireless systems, they have a duty to protect the rights of their residents. Safeguards for privacy and free speech must be priorities, rather than 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 growth. Part III discusses the variety of business plans that cities have employed to develop municipal wireless networks. Part IV addresses the privacy and free speech implications of municipal wireless systems and describes the requisite protections that must be part of any proposed plan. Part V analyzes some recent examples of deployed and proposed municipal wireless programs and the failures and successes of incorporating protections for civil liberties.

I.
THE EMERGENCE OF MUNICIPAL WIRELESS

As more and more people communicate via email and Voice over Internet Protocol (VoIP) telephones and turn to the Internet to access

1. EarthLink pulled out of contracts with San Francisco as well as several other high-profile wireless plans in the fall of 2007 following a change in company leadership and reported financial difficulties leading to massive layoffs of company employees. See *infra* Part V for case studies of San Francisco, Silicon Valley, and Philadelphia. *See also* Ryan Kim, *Cities Go Beyond Wi-Fi Hype*, S.F. CHRON., Oct. 23, 2007, at B1.

essential information for their daily lives, there has been an explosion of interest in ubiquitous Internet access. More than fifty-six million Americans (28% of the population) have wireless Internet enabled devices.[2] As the costs associated with wireless Internet networks decrease, homes, businesses, and even entire communities are now setting up wireless networks.[3] In some homes, family members might be working on several computers in different rooms of the house. When one walks into a university, a private company, a hotel, a coffee shop, or even a public square—it is now normal to find a sea of laptop screens or portable WiFi-enabled devices with their owners busily working away on emails and accessing websites.[4] By 2006, approximately 208,000,000 users had been on more than 60,000 wireless hot spots across the United States.[5]

Wireless local area networks (WLAN) were originally developed to enable more efficient transfer of information between manufacturing and warehouse facilities.[6] 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.[7] 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.[8]

The most common type of WLAN network is known as WiFi.[9] WiFi networks are based on the Institute of Electrical and Electronics

2. FED. TRADE COMM'N STAFF, MUNICIPAL PROVISION OF WIRELESS INTERNET 9, (2006), *available at* http://www.ftc.gov/os/2006/10/V060021municipalprovwireless Internet.pdf [hereinafter FTC MUNICIPAL WIRELESS REPORT].

3. *Id.* at 8–9.

4. *Id.* at 6.

5. Central Intelligence Agency, World Factbook, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last visited Aug. 13, 2008). For an illustration of the continual growth of Internet wireless hotspots, see JiWire, WiFi Finder, http://www.jiwire.com/search-hotspot-locations.htm (last visited Aug. 13, 2008).

6. HEWLETT-PACKARD, UNDERSTANDING WI-FI 4 (2002), *available at* http://www.hp.com/rnd/library/pdf/understandingWiFi.pdf.

7. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 7.

8. *Id.* at 7–8.

9. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 6. 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-Fi Alliance, Certification Programs, http://www.wi-fi.org/certification_programs.php (last visited Aug. 13, 2008).

Engineers (IEEE) 802.11 standard for a WLAN.[10] The 802.11 standard refers to a particular family of technical specifications developed by the IEEE for the over-the-air interface necessary for wireless Internet access.[11] The WiFi radio waves travel over the 2.4 GHz and 5 GHz radio spectrum.[12] A second standard, worldwide interoperability for microwave access (WiMAX), describes another set of specifications (802.16) for wireless network technology that operates between 2 GHz and 66 GHz.[13] The IEEE approved this standard specifically for a Wireless Metropolitan Access Network, a "wireless communications network that covers a geographic area such as a city or suburb."[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]

Cities can create a wireless network that operates according to either WiFi or WiMAX standards. A municipal wireless network must work 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 a city, to connect to both 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 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

10. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 6–7.

11. Webopedia, 802.11, http://www.webopedia.com/TERM/8/802_11.htm (last visited Aug. 13, 2008).

12. Jim Geier, *2.4GHz vs. 5GHz Deployment Considerations*, WI-FI PLANET, Jan. 14, 2003, http://www.wi-fiplanet.com/tutorials/article.php/1569271.

13. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 9. *See generally* WiMAX Forum, Welcome to the WiMAX Forum, http://www.wimaxforum.org/home (last visited Aug. 13, 2008).

14. *Id.*

15. Galen Gruman, *What Is Municipal Wireless and What Can It Mean for You?*, DAILYWIRELESS, Oct. 31, 2006, http://www.dailywireless.com/features/muni-wireless-for-dummies/.

16. *Id.*

17. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 8.

18. Gruman, *supra* note 15; FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 8.

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 is connected to a high capacity wire connection (backhaul technology).[20] Since a wire connection can transfer data far more quickly than a wireless connection, it is this backhaul technology that is actually used to connect to the Internet.[21]

II.
THE DRIVE BEHIND MUNICIPAL WIRELESS

Many small and rural communities that lacked Internet infrastructure turned to municipal wireless to provide Internet resources to community members.[22] But, in the last few years, municipal wireless has swept the nation, spurred on by a confluence of dreams.[23] Wireless companies dream of side-stepping the stronghold of the telecommunications companies in providing Internet access and tapping into a lucrative market. City governments dream of a low-cost Internet infrastructure for city services such as law enforcement and meter reading. Communities often support the systems because they dream that municipal wireless programs will deliver "free" Internet access to diverse community members and conquer the digital divide. However, the reality of municipal wireless often falls far short of the ideals of community members, instead forcing them to pay a high price for these systems, while getting relatively little in return.

A. Incentives for Cities

1. Internet Infrastructure for Law Enforcement and City Services

Wireless systems are increasingly being marketed to cities as a means to give more tools to law enforcement, fire departments, and emergency services.[24] While many cities currently pay fees for mo-

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 F1.

20. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 8.

21. Gruman, *supra* note 15; FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 8.

22. Michael Alison Chandler, *Rural Areas Find Internet Answer in the Air: Wireless Connections Speedy but Can Be a Hassle,* WASH. POST, Mar. 14, 2006, at B4.

23. Kim, *supra* note 1.

24. TROPOS NETWORKS, SAVING LIVES WITH TROPOS METROMESH: CITY OF NEW ORLEANS, LOUISIANA 5 (2005), *available at* http://www.tropos.com/pdf/case_studies/tropos_casestudy_new_orleans.pdf [hereinafter TROPOS-CITY OF NEW ORLEANS]; TROPOS NETWORKS, GRANBURY: MODERNIZING COMMUNICATIONS IN THE CITY "WHERE TEXAS HISTORY LIVES" 5 (2007), *available at* http://www.tropos.com/pdf/case_studies/tropos_casestudy_granbury.pdf [hereinafter TROPOS-GRANBURY]; TROPOS NETWORKS, CORPUS CHRISTI PIONEERS METRO-WIDE WI-FI MESH 3 (2007),

bile data access for city employees, such as services that allow police officers to access information from their squad cars, many of these systems are slow or lack capabilities.[25] Wireless companies are touting to cities the ways by which wireless Internet access could increase the efficiency of city workers by providing mobile access to databases, facilitate the production of more in-field reports,[26] track the location of police cars and fire engines, improve communications among employees,[27] and even automate some city services like meter reading.[28]

Municipal networks are also increasingly being sold as a backbone from which to expand options for public video surveillance in cities.[29] By linking municipal wireless and public video surveillance, a city might be able to apply for Department of Homeland Security (DHS) grants to fund the system. Through 2006, DHS has provided over $230 million in grants to local governments for video surveillance cameras and systems.[30] In the 2003 DHS grant program, California received over $45 million dollars in funds, with over $31.5

---

available at http://www.tropos.com/pdf/case_studies/tropos_casestudy_corpus_christi.pdf [hereinafter TROPOS-CORPUS CHRISTI TEXAS].

25. TROPOS NETWORKS, Metro-Scale Wi-Fi for Public Safety: San Mateo Police Department 3 (2007), *available at* http://www.tropos.com/pdf/case_studies/tropos_casestudy_smpd.pdf.

26. *Id.*

27. *Id.*

28. *See* EARTHLINK MUN. NETWORKS & GOOGLE, SAN FRANCISCO TECHCONNECT COMMUNITY WIRELESS BROADBAND INITIATIVE 52, 65–69 (2006), *available at* http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/EarthLink_SanFrancisco_RFP_2005-19_PUBLIC.pdf; RON SEGE, MUNICIPAL WIRELESS—JUST THE FACTS, PLEASE! (2005), http://www.tropos.com/pdf/muni_wireless-the_facts.pdf; *see also* TROPOS-GRANBURY, *supra* note 24, at 5; TROPOS-CORPUS CHRISTI TEXAS, *supra* note 24, at 3.

29. MARK SCHLOSBERG & NICOLE A. OZER, UNDER THE WATCHFUL EYE: THE PROLIFERATION OF VIDEO SURVEILLANCE SYSTEMS IN CALIFORNIA (2007), *available at* http://www.aclunc.org/docs/criminal_justice/police_practices/under_the_watchful_eye_the_proliferation_of_video_surveillance_systems_in_california.pdf.

30. Melissa Ngo, Senior Counsel & Dir. of Identification & Surveillance Project at the Elec. Privacy & Info. Ctr., Public Workshop CCTV: Developing Privacy Best Practices, Remarks at the Department of Homeland Security Privacy Office 26 (Dec. 18, 2007) (transcript available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Developing_Privacy_Best_Practices_Panel.pdf; Nicole Ozer, Tech. & Civil Liberties Policy Dir., ACLU of N. Cal., Public Workshop CCTV: Developing Privacy Best Practices, Remarks at the Department of Homeland Security Privacy Office 4 (Dec. 18, 2007) (transcript available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Developing_Privacy_Best_Practices_Panel.pdf); *see also* Martha T. Moore, *Cities Opening More Video Surveillance Eyes*, USA TODAY, July 18, 2005, at A3 (discussing the additional one billion dollars available in state grants).

million dollars for equipment allocations.[31] The equipment that was authorized to be purchased with DHS funds included video surveillance cameras for "critical infrastructure."[32] In the last five years, video surveillance has doubled to become a $9.2 billion industry.[33] Joe Freeman, a security industry consultant, estimates that the industry will grow to $21 billion dollars in 2010.[34]

Companies market municipal wireless as an economic and efficient way to coordinate 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.[35] Such capabilities would have grave implications for privacy and free speech, as police may 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.[36] The ability to wirelessly control the cameras and do live monitoring raises the concern that the cameras may be used as a tool for discriminatory targeting.[37] Studies of live-monitored cameras in the United Kingdom reveal that while the cameras do not prevent or reduce crime or make people feel safer, "the young, the male, and the black are systematically and disproportionately targeted, not because of their involvement in crime or disorder, but for 'no obvious reason.'"[38] It was also discovered that one in ten women were "targeted for entirely 'voyeuristic' reasons by male operators" and that forty percent of people were "targeted for 'no obvious reason,' mainly 'on the basis of belonging to a particular sub-cultural group.'"[39] Community members often are not aware of the law enforcement goals for municipal wireless systems and the potential ramifications for privacy, free speech, and discriminatory targeting.

---

31. DEPARTMENT OF HOMELAND SECURITY, FISCAL YEAR 2003 STATE HOMELAND SECURITY GRANT PROGRAM 7 (2003) (on file with New York University Journal of Legislation and Public Policy).

32. *Id.* at G-6.

33. Jessica Bennett, *Big Brother's Big Business*, NEWSWEEK, Mar. 15, 2006, *available at* http://www.newsweek.com/id/47242.

34. *Id.*

35. *See* TROPOS-CITY OF NEW ORLEANS, *supra* note 24, at 5–6.

36. SCHLOSBERG & OZER, *supra* note 29, at 5, 8.

37. *Id.* at 10.

38. *Id.* at 10 (*citing* ADRIENNE ISNARD, AUSTRALIAN INST. OF CRIMINOLOGY, CAN SURVEILLANCE CAMERAS BE SUCCESSFUL IN PREVENTING CRIME AND CONTROLLING ANTI-SOCIAL BEHAVIORS? 12 (2001), http://www.aic.gov.au/conferences/regional/isnard1.pdf).

39. ADRIENNE ISNARD, AUSTRALIAN INST. OF CRIMINOLOGY, CAN SURVEILLANCE CAMERAS BE SUCCESSFUL IN PREVENTING CRIME AND CONTROLLING ANTI-SOCIAL BEHAVIORS? 12, http://www.aic.gov.au/conferences/regional/isnard1.pdf.

2. Increased Efficiency for City Services

In addition to reducing the existing costs of Internet access for employees, some cities are banking on municipal wireless to save money by replacing workers with automated systems.[40] 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.[41] The city of Corpus Christi, Texas formerly employed twenty-five individuals to read utility meters.[42] Now, gas, water, and electric meters transmit readings over the wireless network, and the city employs only a few staff members for oversight.[43] Proponents of municipal wireless say that between smart meters and increased efficiency of other workers such as maintenance and building inspectors, municipal wireless can save cities millions of dollars.[44] The city of Philadelphia estimated that a municipal wireless program could save two million dollars a year in existing expenses.[45]

Other cities are also looking at municipal wireless systems to increase efficiency and save costs by using the new communication network to publicize municipal issues and events.[46] Chaska, Minnesota, has installed a municipal wireless service that increases municipal employee productivity and provides subscribers with a "What's happening in Chaska" home page that keeps them informed about local issues and events.[47] Minneapolis will develop up to ninety location-based community log-in sites for residents in order to keep them informed of

40. *On the Media: Wi-Fi America* (National Public Radio radio broadcast Jan. 5, 2007) (transcript available at http://www.onthemedia.org/transcripts/2007/01/05/05).

41. SMART VALLEY WIRELESS SILICON VALLEY TASK FORCE, JOINT VENTURE: SILICON VALLEY NETWORK, A VISION OF A WIRELESS SILICON VALLEY 3-4 (2005), *available at* http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/documents/WirelessSiliconValleyVision.pdf; *On the Media: Wi-Fi America*, *supra* note 40.

42. *On the Media: Wi-Fi America*, *supra* note 40.

43. *Id.*

44. Kim, *supra* note 19.

45. *Id.* at F1.

46. *See* TROPOS NETWORKS, CHASKA.NET AND TROPOS UNWIRE: CHASKA, MINNESOTA 9 (2004), *available at* http://www.tropos.com/pdf/case_studies/tropos_casestudy_chaska.pdf [hereinafter TROPOS-CHASKA]; JOSHUA BREITBART, NEW AM. FOUND., THE PHILADELPHIA STORY: LEARNING FROM A MUNICIPAL WIRELESS PIONEER 6, 38 (Sascha D. Meinrath ed.), *available at* http://www.newamerica.net/files/NAF_PhilWireless_report.pdf (last visited Aug. 13, 2008); Wireless Broadband Internet Access Network Agreement Between the City and County of San Francisco and EarthLink, Inc., Jan. 5, 2007, at 25, *available at* http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/process/SanFranciscoWirelessNetworkAreementFinal.pdf [hereinafter San Francisco Agreement].

47. *See* TROPOS-CHASKA, *supra* note 46, at 9.

current events.[48] San Francisco's draft wireless contract with EarthLink and Google entitled the city to post six hyperlinks regarding community notices and municipal purposes on the Internet login page which would be seen by all users of the municipal wireless system.[49]

The possibility that municipal wireless will provide more tools and cost savings to cities makes it very attractive. The deal for cities appeared even more attractive when early wireless contracts promised these increased efficiencies and budget savings without demanding any money from the city.[50] Some municipal wireless contracts offered unlimited, free access to the wireless system for city purposes in exchange for the right (of the company) to install wireless routers on light poles and other publicly-owned infrastructure and to sell wireless services to community members.[51] In other cases, cities were being offered both free access and additional funds for the rental of the light poles and other city resources.[52] For example, the draft contract between EarthLink and San Francisco for its proposed wireless system stipulated that the company would pay the city a $600,000 non-refundable lump sum payment and five percent of its quarterly gross revenues.[53] Hence, for many cities, municipal wireless looked like a win-win proposition. The city would get greater access to the Internet, save money on existing and future expenses, and even make some money in the process.

48. BREITBART, *supra* note 46, at 38.

49. *See* San Francisco Agreement, *supra* note 46, at 25.

50. 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. *See infra* Part II.B.

51. *See*, *e.g.*, CITY OF SANTA MONICA, REQUEST FOR PROPOSALS TO PROVIDE CITYWIDE BROADBAND WIRELESS NETWORK 1–2 (2006), *available at* http://www.muniwireless.com/reports/docs/SantaMonica-wirelessRFP.pdf; *see also* Esme Vos, *Long Beach, CA Issues RFP for Citywide Wireless Network*, MUNIWIRELESS, Feb. 3, 2006, http://www.muniwireless.com/2006/02/03/long-beach-ca-issues-rfp-for-citywide-wireless-network/; Esme Vos, *Santa Monica Issues RFP for Citywide Wi-Fi Network; Interview with City CIO*, MUNIWIRELESS, Apr. 28, 2006, http://www.muniwireless.com/2006/04/28/santa-monica-issues-rfp-for-citywide-wi-fi-network-interview-with-city-cio/.

52. San Francisco Agreement, *supra* note 46, at 9–11.

53. *Id.* EarthLink pulled out of the San Francisco deal as well as several other high-profile municipal wireless plans in the fall of 2007 following a change in company leadership and reported financial difficulties leading to massive layoffs of company employees. *See infra* Part V.

3. Economic Development

The hope that municipal wireless will spur greater economic development also attracts cities to the technology. While it appears that no thorough studies have shown that wireless access has such an impact, cities envision that the infrastructure will provide an extra incentive for businesses to locate in the community, encourage conventions to come to the city, bring visitors to hotels and restaurants, and build a more vibrant downtown community in which high-income professionals choose to live, work, and play.[54] Some communities even look to public wireless networks as a panacea for high rates of unemployment, anticipating that access to a wireless network will somehow turn an inactive workforce into entrepreneurs.[55]

4. Digital Divide

Finally, many cities have touted municipal wireless as a means to minimize the disparity of access to technology resources, often referred to as the digital divide.[56] When Mayor Gavin Newsom announced his plan to implement municipal wireless in San Francisco, the digital divide took center stage: San Francisco TechConnect was touted as "a citywide Digital Inclusion initiative to bridge San Francisco's digital divide amongst San Francisco's socio-economically diverse communities."[57] 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

54. *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.

55. *See id.*

56. *See* THE BOSTON FOUND., BOSTON UNPLUGGED: MAPPING A WIRELESS FUTURE 5 (2006), *available at* http://www.cityofboston.gov/wireless/Boston%20Unplugged.pdf (discussing work of community leaders to bridge the digital divide). In Boston, sixty percent of households and close to eighty percent of Boston public school children do not have Internet access at home. *On the Media: Wi-Fi America*, *supra* note 40. Rural communities often have difficulty obtaining Internet service. *See All Things Considered: Widening the Internet Highway to Rural America*, (National Public Radio radio broadcast Dec. 14, 2005) (transcript available at http://www.npr.org/templates/story/story.php?storyId=5053488).

57. Press Release, S.F. Mayor's Office of Communications, Mayor Newsom and Department of Telecommunications and Information Services Announces $49,900 State Grant for City's Digital Inclusion Initiative (Aug. 2, 2007), *available at* http://www.sfgov.org/site/mayor_page.asp?id=65419.

separates too many communities from the enormous benefits of technology."[58]

The framing of municipal wireless as a digital divide issue can help build a broad base of support for a city's initiative and draw attention away from the other city incentives, such as law enforcement interests, that underlie many of the efforts to institute municipal wireless. However, now that the initial euphoria of the early municipal wireless rush has subsided, many communities realize that unless the programs are planned properly to ensure adequate safeguards and affordable access rates, and unless funding is obtained to subsidize computer purchases, municipal wireless often ends up being a disappointment.[59] As Michael Armstrong, the director of municipal information services for Corpus Christi (which was an early adopter of municipal wireless) said after its system was sold to EarthLink, "[i]t was a fever that became a plague. . . . I think there were lots of false expectations for this system."[60]

City officials may highlight the potential of municipal wireless networks to bridge the digital divide, but 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 less expensive or greater access to the Internet. However, disadvantaged members of the community may still be without Internet access because of the expenses of computers and monthly service payments and the inability of the service to work indoors and at fast enough speeds.

Computers are still out of reach for many low-income Americans, with laptops and desktops costing at least several hundred dollars.[61] While there are some innovative programs, such as MIT's One Laptop Per Child (OLPC) that aims to develop a "low cost" laptop,[62] 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 house-

58. Press Release, S.F. Mayor's Office of Communications, Mayor Newsom Announces First of Its Kind Wireless Initiative (Jan. 5, 2007), *available at* http://www.sfgov.org/site/mayor_index.asp?id=52549.

59. BREITBART, *supra* note 46, at 4–5.

60. *Earthlink What a Disappointment*, CORPUS CHRISTI WIFI NEWS, http://www.ccwifinews.com/blog/?p=118 (last visited Aug. 13, 2008).

61. Dell, Latitude Laptops/Notebooks, http://www.dell.com/content/products/category.aspx/latit?c=us&cs=04&l=en&s=bsd&~ck=mn (last visited Aug. 13, 2008).

62. One Laptop Per Child Foundation, http://laptop.org/ (last visited Aug. 18, 2008).

holds still did not have home computer access in 2003.[63] San Francisco did unveil a companion digital inclusion program, the TechConnect PC Purchase Program, to its plan for municipal wireless that provides the opportunity for San Francisco working families to apply for a loan to purchase a discounted computer and receive six months of free Internet service over a working phone line.[64] Philadelphia also developed a digital inclusion program and planned to supply 10,000 TEACH (Training, Education, Access, Content, Hardware) bundles to low-income families. By December 2007, the city had distributed 613.[65]

While these digital inclusion programs are important steps, many wireless programs have continuing costs that also may be difficult to afford.[66] The discounted service proposed for low-income San Franciscans to obtain high speed municipal wireless service was $12.95 per month or "a price mutually agreed upon by the Parties."[67] In Philadelphia, individuals making less than $13,000 per year were

63. DEP'T. OF TELECOMMUNICATIONS AND INFO. SERVICES, CITY OF SAN FRANCISCO, SAN FRANCISCO DIGITAL INCLUSION STRATEGY 11 (2006) (draft), *available at* http://www.ci.sf.ca.us/site/uploadedfiles/dtis/tech_connect/DraftSFDigitalInclusion-Framework.pdf [hereinafter SAN FRANCISCO DIGITAL INCLUSION STRATEGY]; U.S. Census Bureau, Current Population Survey, Definitions and Explanations, http://www.census.gov/population/www/cps/cpsdef.html (last visited Aug. 18, 2008); Jason B. Johnson, *U.S. Census Finds More Are Poor, but Number Lacking Health Insurance Remains Steady*, S.F. CHRON., Aug. 31, 2005, at A2.

64. City and County of San Francisco, TechConnect PC Purchase Program, http://www.sfgov.org/site/digitalinclusion_index.asp?id=71165 (last visited Aug. 18, 2008); City and County of San Francisco, TechConnect PC Purchase Program – Frequently Asked Questions (FAQ), http://sfgov.org/site/digitalinclusion_index.asp?id=72524 (last visited Aug. 18, 2008), (explaining that after the six month period, the families are responsible for securing their own service).

65. Greg Goldman, Status Report: Wireless Philadelphia (Dec. 11, 2007) (transcript available at http://wirelessphiladelphia.org/gg_testimony_city_council_121107.pdf).

66. *See $100 Laptops Aim to Bring Children the World,* SEATTLE TIMES, Nov. 17, 2005, at A1; CITY OF BOSTON WIRELESS TASK FORCE, WIRELESS IN BOSTON 55 (2006), *available* at http://www.masstech.org/converge_9_06/BostonWirelessTaskForceReportFinal.pdf; SAN FRANCISCO DIGITAL INCLUSION STRATEGY, *supra* note 63, at 10. Other cities have proposed similar programs. *See, e.g.,* SAN DIEGO FUTURES FOUND. & DELL COMPUTER CORP., A BLUEPRINT: FROM DIGITAL DIVIDE TO DIGITAL PROVIDE (2001), *available at* http://www.dell.com/downloads/us/slg/digital.pdf; Seattle Department of Information Technology, Home Computer and Internet Security Workshop for Community Members, http://www.seattle.gov/tech/ (last visited Aug. 18, 2008); THE WIRELESS PHILA. EXECUTIVE COMM., WIRELESS PHILADELPHIA BUSINESS PLAN 13, 42 (2005), *available at* http://www.wirelessphiladelphia.org/get_wireless.cfm; WIRELESS MINNEAPOLIS DIGITAL INCLUSION TASK FORCE, FINAL REPORT, (2006), *available at* http://www.digitalaccess.org/documents/MDITF%20complete.pdf.

67. San Francisco Agreement, *supra* note 46, at 23.

obligated to pay $9.95 per month for wireless service.[68] These rates are more than twice the cost of subsidized local telephone services and may price many low-income families out of the opportunity to have Internet access.[69]

Many of the discounted wireless systems are also slow or do not work effectively indoors, making them less useful for low-income individuals.[70] While San Francisco's proposed system offered the high speed, one megabit per second paid service through EarthLink, the no-fee basic service provided by Google would run at a very slow speed—only 300 kilobits per second.[71] Further, the no-fee services in San Francisco were not likely to be effective inside higher-density residential buildings, such as subsidized housing developments.[72] Residents would most likely have needed to purchase a Customer Premise Equipment device (CPE) for an additional $80 to $200 to strengthen the signal and access the system indoors.[73]

Now that companies such as EarthLink have pulled away from offering no-fee municipal wireless, contending that it is not viable, it has become clearer that reducing the digital divide is not the primary motivation for many programs.[74] "What you'll find is that cities are now selling the networks on things that are quantifiable, like public safety or public works. You've got to establish that before you can pursue other social goals," said Craig Settles, a wireless consultant.[75]

---

68. Wi-Fi America, *supra* note 40; Wireless Philadelphia, How to Connect, http://www.wirelessphiladelphia.org/get_wireless.cfm (last visited Aug. 18, 2008).

69. Regular local plans offered by AT&T California cost $13.95/month. AT&T New Local Phone Service, http://www.att.com/att-phone-service.html (last visited Aug. 18, 2008). The Universal Lifeline service gives individuals and families that make up to $29,200 the same service at 50% of the cost. AT&T, Life Line California, http://www.att.com/gen/general?pid=10278 (last visited Sept. 16, 2008).

70. *See* Susannah Patton, *More Cities and Towns Want Their Own Wi-Fi*, CIO, Apr. 1, 2006, http://www.cio.com/article/19686/More_Cities_and_Towns_Want_Their_Own_Wi_Fi; San Francisco Agreement, *supra* note 46, at 23; Kim, *supra* note 19 (explaining that Silicon Valley has given up on indoor coverage because it would be too expensive); Jim Geier, *Extending Municipal Wi-Fi Mesh Indoors*, Wi-Fi Planet, Mar. 30, 2007, http://www.wi-fiplanet.com/tutorials/article.php/3669001.

71. Bambi Francisco, *Google, EarthLink Win Wi-Fi Contract from S.F.*, Investors.com, Apr. 6, 2006, http://www.investors.com/breakingnews.asp?journalid=36047882&brk=1; Elinor Mills, *Google in San Francisco: 'Wireless Overlord'?*, CNET News, Oct. 1, 2005, http://www.news.com/Google-in-San-Francisco-Wireless-overlord/2100-1039_3-5886968.html.

72. Harvey M. Rose, Fiscal Feasibility Analysis of a Municipally-Owned Citywide Wireless Broadband 5 (2007), at 27, *available at* http://www.sfgov.org/site/budanalyst_page.asp?id=53280.

73. *Id.* at 28.

74. *Earthlink to Cut Half Its Workforce*, BroadcastEngineering, Aug. 31, 2007, http://broadcastengineering.com/news/earthlink-cuts-workforce-0831/.

75. Ryan Kim, *Cities Go Beyond Wi-Fi Hype*, S.F. Chron., Oct. 23, 2007, at B1.

B. The Incentive for Companies

Companies do not seek wireless contracts as a favor to city governments or as a philanthropic effort to reduce the digital divide. They do it to make money. Early municipal wireless bidders such as EarthLink, Google, and MetroFi, and newer entrepreneurial companies with innovative business models, want to tap into a lucrative market that has been largely controlled by the telecommunications and cable companies.[76] As discussed above, municipal wireless networks normally operate using a mesh network.[77] The mesh network architecture is an innovative end-run 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.[78] It would be prohibitively expensive for another 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 new companies to enter the Internet provider market.[79] However, a mesh network and permission from a city to install wireless routers on existing city infrastructure or other outdoor spaces puts companies in a position to create extremely profitable networks without an overwhelming initial investment.[80] When Philadelphia awarded EarthLink the contract to build its municipal wireless system on the back of existing city infrastructure, it allowed EarthLink to bypass Comcast cable lines and Verizon phone lines and directly reach potential customers.[81] San Francisco was set to hand over a monopoly for municipal wireless to EarthLink and Google, and Silicon Valley is

76. Jesse Drucker et al., *Google's Wireless Plan Underscores Threat to Telecom*, WALL ST. J., Oct. 3, 2005, at A1.

77. FTC MUNICIPAL WIRELESS REPORT, *supra* note 2, at 8.

78. Patton, *supra* note 70.

79. *Id.*

80. Olga Kharif, *EarthLink's Big Bet on Broadband*, BUSINESSWEEK, June 2, 2006, http://www.businessweek.com/technology/content/jun2006/tc20060602_708224.htm?campaign_id=rss_tech ("A wireless network is relatively inexpensive to build, costing between $25,000 and $100,000 per square mile.").

81. Wireless Philadelphia Broadband Network Agreement, Feb. 21, 2006, at 10, *available at* http://www.wirelessphiladelphia.org/documents/Network_Agreement_for_PDF.pdf [hereinafter Wireless Philadelphia Agreement].

still negotiating to allow companies to have a direct conduit to millions of potential users in the forty cities of Silicon Valley.[82]

The economic threat posed by municipal wireless was not lost on established telecommunications and cable companies.[83] Companies like Comcast and Verizon waged local lobbying efforts to influence the debate in Philadelphia.[84] Some companies attempted to stifle the spread of municipal wireless with state and federal legislation preventing wireless companies from circumventing existing telecommunications infrastructure.[85] Despite these efforts, 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 implementing systems.[86]

III.
All Municipal Wireless Programs Are Not Created Equal

Hundreds of municipal wireless programs are being considered or have already been implemented throughout the United States. But, the goals, business models, and impact on privacy and free speech of the programs can vary substantially depending on the purpose and structure of the wireless system.

A. Public Utilities

Several early municipal wireless programs were developed by cities as a new form of public utility and are owned and operated by cities.[87] For example, in 2004, the small town of Chaska, Minnesota, set out to build a municipal wireless system to provide access to its community members and spur economic development.[88] With an initial $600,000 loan from the Chaska Electric Utility, city workers installed the outdoor wireless system in two months.[89] The network offers fixed and mobile broadband service (1–1.2 Mbps) to the city's 23,000 residents for $17.99 per month and to business subscribers for

82. *See* San Francisco Agreement, *supra* note 46; Joint Venture: Silicon Valley Network, Wireless Silicon Valley, http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/wireless.html (last visited Sept. 16, 2008).

83. Wi-Fi America, *supra* note 40.

84. *Id*.

85. Patton, *supra* note 70.

86. *See* Nicole A. Ozer, *Companies Positioned in the Middle: Municipal Wireless and Its Impact on Privacy and Free Speech*, 41 U.S.F. L. Rev. 635 (2007).

87. *See*, *e.g.*, Tropos-Chaska, *supra* note 46, at 9.

88. *Id.* at 2.

89. *Id.*

$27.99 per month.[90] After a second city investment of $700,000 to pay for the growing usage and number of subscribers, the network provides 95% broadband coverage to the fourteen-square mile city, and 28% of the city residents subscribed to the network.[91] A low-cost indoor Wi-Fi bridge is included for subscribers to extend the signal from the wireless network indoors.[92] The city forecasts being able to reduce its residential rates to $6.72 per month and to break even sometime in 2009, five years from its launch date.[93]

In March 2006, the small town of St. Cloud, Florida, launched its Cyber Spot™ municipal wireless service for its fifteen-square mile city.[94] It is provided without a fee as a public service by the city for use by residents, businesses, and visitors.[95] For a fee, residents can also purchase a wireless bridge to strengthen the signal so that they can access wireless service inside their homes.[96] Within a year, more than 77% of the city's 11,000 households had registered for the service.[97] Other cities such as Culver City, California, have developed and deployed smaller hot-spots for town centers.[98] In September 2004, this small city just west of Los Angeles used redevelopment funds to build a one-square mile wireless network and offered no-fee wireless access in its downtown area.[99]

B. Contracts with Nonprofit Entities

Some cities, like Boston, work with a nonprofit entity to build and operate a network.[100] In early 2006, Boston Mayor Thomas Menino announced his plan to construct a wireless network for his city. It was estimated that 57 percent of the city's 600,000 residents

90. Chaska.net, Standard Pricing, http://www.chaska.net/mkpage.cgi?services_pricing+services_pricing (last visited Sept. 16, 2008).

91. TROPOS-CHASKA, *supra* note 46, at 2, 5.

92. *Id*. at 6.

93. *Id*. at 9; Chaska.net, *supra* note 90.

94. City of St. Cloud, Florida, Cyber Spot Terms and Conditions, http://www.stcloud.org/index.asp?nid=499 (last visited Sept. 16, 2008) [hereinafter CITY OF ST. CLOUD].

95. *Id*.

96. *Id.*

97. Esme Vos, *One Year Later, St. Cloud Citywide Wi-Fi Network Shows Impressive Results*, MUNIWIRELESS, Mar. 6, 2007, http://www.muniwireless.com/2007/03/06/one-year-later-st-cloud-citywide-wi-fi-network-shows-impressive-results/.

98. Culver City Wireless Hotspot, http://www.wirelesshotspot.com/culvercity.php (last visited Sept. 16, 2008).

99. Press Release, Proxim Wireless, Culver City Launches Free Wireless Internet Access in Downtown District (Sept. 7, 2004), *available at* http://www.terabeam.com/news/pressreleases/pr-20040907_culver.php.

100. Essex, *supra* note 54.

and 80 percent of its school students lacked Internet access at home.[101] In March 2007, openairboston.net, a private, non-profit entity, was incorporated and tasked with building and managing the wireless Internet network that would foster economic development and innovation, bridge the digital divide, and improve the quality and efficiency of city services.[102] An Internet access pilot program is up and running, but plans to complete the city-wide Internet network by the end of 2008 have unfortunately been delayed.[103] Openairboston is still working to raise the $16-20 million dollars in private funds needed to fully fund the project.[104]

C. Contracts with Private Companies

The majority of cities are contracting or cooperating with private entities to build and operate systems.[105] Some systems have no fee at all, such as Google's partnership with the city of Mountain View, California.[106] Others, like Philadelphia and Silicon Valley, developed plans to partner with companies to have them build and operate the network in exchange for the company having the opportunity to charge all residents a monthly fee to use the system and collect information to use for targeted advertising and other products.[107] San Francisco considered a mixed system, partnering with EarthLink to sell a service with a monthly charge and with Google to provide a no-

101. Openairboston.net, Frequently Asked Questions, http://www.openairboston.net/faq/index.html (last visited Sept. 16, 2008); Press Release, Mayor's Press Office, City of Boston, Mass., Menino Announces City's First WiFi Pilot Project (Oct. 16, 2006), *available at* http://www.openairboston.net/pdf/Hot%20Spot%20Press%20Release.pdf.

102. Press Release, Mayor's Press Office, City of Boston, Mass., Mayor Menino's Wireless Initiative Moves Forward: Openairboston.net to Serve Among Nation's First Non-Profit Wireless Networks (Mar. 13, 2007), *available at* http://www.openairboston.net/pdf/OPENAIR%20Press%20Release.pdf.

103. Brett Arends, Op-Ed., *Good Call, City Hall, in Reviving Hub's Wi-Fi*, BOSTON HERALD, Jan. 17, 2007, at 21.

104. *Id.*; Openairboston.net, *supra* note 101.

105. Khali Henderson, *Public-Private Partnerships for Muni Wireless Evolving, Experts Say*, XCHANGE, Feb. 14, 2007, http://www.xchangemag.com/hotnews/72h1417239.html.

106. 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.

107. *On the Media: Wi-Fi America*, *supra* note 40; Paul Krill, *Wireless Program Aims to Cover Silicon Valley*, INFOWORLD, Oct. 24, 2007, http://www.infoworld.com/article/07/10/24/wireless-valley_1.html.

fee service at slower speeds.[108] However, this no-fee service would have a price—a user's personal information. Pursuant to Google's draft contract with San Francisco to be the only no-fee game in town, each time a San Franciscan logged onto the system, Google would know the identity of the individual, what he or she was searching for online, and his or her physical location.[109] Google could obtain a wealth of data about tens of millions of individuals who might not otherwise provide such specific information about their daily activities and interests.[110] All of this information would further increase Google's ability to develop new targeted products or allow for greater targeted advertising that it could sell at an even higher premium.[111]

D. Privately-Supported Municipal Wireless Networks

Some cities, such as San Francisco, are now moving in a new direction, relying on both private citizens and businesses to support a municipal wireless program.[112] Companies like Meraki and FON make wireless devices and software that enable hard-wire Internet connections to become wireless nodes for a mesh network that can potentially be used to cover whole cities with wireless signals.[113] By

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

109. *See* San Francisco Agreement, *supra* note 46, at 23.

110. *See id*.; Letter from Christopher Sacco to Christopher Vein (June 20, 2006), *available at* http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/SFGooglePrivacyResponseJune06.pdf [hereinafter Google Privacy Response Letter]; San Francisco Agreement, *supra* note 46, at 40. The Google Privacy Response Letter provides some further indications of the privacy policy for the Google Service. Unlike the privacy options for the Subscriber services, there is no option for Basic Service subscribers to opt-out of location based tracking. *Id.,* at 2. Google knows the approximate location of an individual based upon the wireless router node that the user logs onto. It is estimated that between 30 and 100 nodes per square mile are necessary for an effective municipal wireless system. Kim, *supra* note 19.

111. Google CEO, Eric Schmidt, has discussed using the targeted ad system for every form of advertising. Eric Schmidt, Google CEO, Search Engine Roundtable (Aug. 9, 2006) (transcript available at http://www.seroundtable.com/archives/004343.html).

112. Meraki, About the Company, http://meraki.com/about/ (last visited Aug. 18, 2008); FON, Frequently Asked Questions, http://www.sharethecastro.com/FON_FAQ.pdf (website no longer active because the initiative has been discontinued, on file with New York University Journal of Legislation and Public Policy).

113. Meraki is based in Mountain-View, California and is funded by Google, Sequoia, Sequoia Capital, DAG Ventures and Northgate Capital. Meraki About the Company, *supra* note 112; Kevin J. Delaney, *Meraki Aims to Link Up a City: Plan for Free Web Access in San Francisco Is a Bet on Technology, User Help*, WALL ST. J., Jan. 4, 2008, at B3. Meraki case studies describe several examples of mesh networks in action, from small inns to cities. MERAKI, VIU PROVIDES WIFI ACCESS TO THE COUNTRY'S INTERNATIONAL TOURISM FAIR, http://meraki.com/collateral/case_studies/

purchasing routers produced by these companies, plugging them into their hard-wire Internet connection inside their homes, and then placing the wireless repeater nodes on their roof or balcony, individuals can create a wireless Internet gateway for other users in the nearby vicinity.[114] The more wireless nodes that users add that overlap and then extend the range of existing nodes, the greater the coverage of the network.[115] The more routers that users purchase and agree to plug into hard-wire Internet connections to function as Internet gateway access points, the more robust and reliable the wireless network.[116]

Meraki and FON both used San Francisco as a model to highlight how their systems can support municipal wireless. Meraki is using its own funding, with support from investors such as Google, to distribute no-fee wireless devices throughout the city.[117] FON distributed no-fee devices in the Castro neighborhood of San Francisco in early 2008.[118] San Francisco has worked with both companies to "support and partner with these efforts—helping publicize and grow the network without the bureaucracy and politics that challenged [the city's] last effort to bring free Wi-Fi to San Francisco," according to Meraki spokesman Nathan Ballard.[119] Since each wireless device—indoor and outdoor repeater antennas—lives on private property, the plans bypassed the public hearings and approval process that took place for the proposed plan with EarthLink and Google to build a municipal wireless system.[120]

---

meraki_cs_viu.pdf; MERAKI, ALASKA HERITAGE TOURS BRINGS EASY INTERNET OPTIONS TO LODGES, http://meraki.com/collateral/case_studies/meraki_cs_alaska_heritage.pdf.

114. Naomi Graychase, *Meraki Frees the 'Net in San Francisco,* WI-FI PLANET, Jan. 4, 2008, http://www.wi-fiplanet.com/news/article.php/3719825. Meraki mini routers have an anticipated range of 100 to 150 feet and Meraki outdoor routers have an anticipated range of 600 feet. Meraki, Meraki Indoor, http://meraki.com/oursolution/hardware/mini/ (last visited Sept. 16, 2008).

115. Meraki, Business Solutions, http://meraki.com/yourgoal/openwireless/ (website no longer active, on file with New York University Journal of Legislation and Public Policy).

116. *Id.*

117. Stephen Lawson, *San Francisco's New Wi-Fi Provider Plays It Safe*, PC WORLD, Jan. 5, 2008, *available at* http://www.pcworld.com/printable/article/id,141051/printable.html; Ryan Kim, *S.F. Is Offered Citizen-Based Wi-Fi for Free*, S.F. CHRON., Jan. 4, 2008, at A1.

118. Ryan Kim, *Share and Cher Alike with Wi-Fi in Castro*, S.F. CHRON., Jan. 22, 2007, at C1.

119. Kim, *supra* note 117.

120. Eric Griffith, *The Politics of San Francisco Wi-Fi*, WIFI PLANET, Nov. 21, 2006, *available at* http://www.wi-fiplanet.com/news/article.php/3645121; Kim, *supra* note 117.

Meraki estimates that it will cost five million dollars and require 15,000 wireless devices to provide service throughout San Francisco.[121] While the company normally recoups costs and makes money by selling its wireless devices, asking people to share their hard-wire Internet service with wireless users, and then targeting users with weather updates, news, and advertisements, it is forsaking a portion of its revenue model for the San Francisco pilot project.[122] The company is distributing no-fee repeater nodes, handing out no-fee indoor routers to boost the outdoor signal and bring it indoors, and providing Internet access so that individuals do not have to share their personal Internet connections. This is an incentive for people to agree to host the wireless router and enable the company to "us[e] the city as a showroom of sorts to sell its products to other municipalities and communities around the world."[123]

However, Meraki users may be paying for this product with their private information. Meraki's CEO stated in January 2008 that the company will not gather "private user data" in its San Francisco pilot.[124] However, the Meraki website reveals that while the system may not be collecting names of individuals, unless San Francisco users read the fine print and affirmatively opt-out, the company will track the IP address and hardware addresses of devices, the searches made, the websites visited, and the location of the repeaters used to access the Internet.[125] Users already see a Meraki toolbar that shows targeted headlines and that will eventually include targeted, sponsored content that Meraki "think[s] you might enjoy."[126] San Francisco users are able to opt-out of the "information tracking" features. If they do so, content and advertisements will still appear, but will not be customized.[127]

---

121. Ryan Kim, Mountain View's Meraki proposes free Wi-Fi network for S.F., S.F. CHRON. at A-1, Jan. 4, 2008, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/MNCDU8UKU.DTL&tsp=1 (last visited Sep. 17, 2008).

122. Meraki currently has two models of wireless router available: the Meraki Indoor ($149) and a weatherproof outdoor version ($199). They are set to release a solar powered outdoor router soon that could be a true "set and forget" network extender. *See* Meraki, Meraki Outdoor, http://meraki.com/products_services/hardware/ (last visited Sep. 17, 2008); Meraki Introduces First Solar Powered Outdoor WiFi Access Kit, http://meraki.com/press-releases/2007/06/03/meraki-introduces-first-solar-powered-outdoor-wi-fi-access-kit/ (last visited Sep. 17, 2008).

123. Kim, *supra* note 121.

124. *Id.*

125. *See* Meraki, Meraki Privacy Policy, http://meraki.com/legal/privacy/ (last visited Aug. 18, 2008).

126. *See* Meraki, Free the Net San Francisco, http://sf.meraki.com/faq (last visited Aug. 18, 2008).

127. *Id.*

FON also gave up its normal business model of selling wireless devices for its limited pilot in the Castro neighborhood. However, unlike the Meraki pilot program, those who volunteered to host no-fee routers in San Francisco had to agree to share a portion of their bandwidth.[128] FON's router produces two WiFi signals.[129] One is unencrypted for the use of the public, and the other is encrypted and used by the router's owner.[130] Individuals who have purchased a wireless router and are sharing Internet access can use any other FON access point for free, and receive half of the proceeds from any sales of access cards sold to the public to use the FON service that are made over their node.[131] FON sells access cards to the public to use the network for $3/day or $10 for a five day pass.[132] Members of the public can also obtain fifteen minutes of no-fee usage time per day if they agree to watch an advertising video.[133]

If a company is able to distribute and maintain enough wireless devices throughout the city (including low-income neighborhoods), provide indoor routers to boost the signal, and pay for enough Internet access that the system works smoothly, then such a program could have potential for San Francisco. But, that is a lot of ifs. As Phil Beranger, whose company Novarum tests municipal wireless networks, has cautioned, San Francisco is "not a repeatable model."[134] San Francisco is a pilot program. All the freebies that Meraki and FON provided for San Francisco are not likely to be duplicated for residents of other cities. FON has already discontinued its program of distributing free hardware, deciding to be "more cautious" with its money.[135] Meraki states on its website that users living in other cities "may be required to pay a fee for that access if they choose to opt-out" of the information tracking features.[136] As other communities ap-

128. FON, Frequently Asked Questions, http://www.sharethecastro.com/FON_FAQ.pdf (website no longer active because the initiative has been discontinued, on file with New York University Journal of Legislation and Public Policy).
129. *Id.*
130. *Id.*
131. *Id.*
132. *Id.*
133. FON, Frequently Asked Questions, *supra* note 128.
134. Dailywireless.org, Meraki Proposes Free SF Wi-Fi Network, http://www.dailywireless.org/2008/01/04/meraki-proposes-free-sf-wi-fi-network/ (last visited Sep. 16, 2008).
135. Boris Veldhuijzen van Zanten, *FON Raises $9.5 Million: No More Free Hardware?,* THE NEXT WEB, Apr. 12, 2008, http://thenextweb.org/2008/04/12/fon-raises-95-million-no-more-free-hardware/ (last visited Sept. 18, 2008); FON, http://www.sharethecastro.com/ (website no longer active because the initiative has been discontinued, on file with New York University Journal of Legislation and Public Policy).
136. Meraki Privacy Policy, *supra* note 125.

proach these companies to follow in San Francisco's footsteps, they should expect to pay for their wireless devices, provide existing Internet access to make the system work, and be subject to collection of substantial private information for advertising. Other cities will have to carefully examine the costs of these systems, both in dollars and in privacy and free speech, and whether the realities of a particular city make this type of plan a viable method for reducing the digital divide.

E. Federal Surveillance Funding

If community members are not paying for municipal wireless by providing personal data to a company, they may be paying for it by agreeing to a surveillance system where private information about who you are, where you are going, and what you are doing is flowing directly to law enforcement. As discussed in Part II.A.1, some cities are relying on federal funds from the Department of Homeland Security to pay for municipal wireless systems. In 2005, Ripon, California, a town of 13,000 people and 25 police officers, used DHS funds to install a wireless Internet system, connecting WiFi-enabled video cameras to protect the "critical infrastructure" of truck stops, public parks, and some downtown locations.[137] Police officers can use the wireless network to pull up video feeds in their cars and also broadcast live from cameras in their cars.[138]

Richmond, California, recently drafted a four million dollar deal to develop a municipal wireless system to support 116 new video surveillance cameras in the city and at its port.[139] The cameras are being paid for by a combination of federal funds and city dollars.[140] The company developing this system predicts that "other city and local governments will soon follow" and deploy municipal wireless technology for surveillance infrastructure.[141] Richmond originally consid-

137. 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*, FCW.COM, June 20, 2005, http://www.fcw.com/article89302-06-20-05-Print.

138. Graychase, *supra* note 137.

139. Press Release, Business Wire EON, City and Port of Richmond Select ADT to Design and Install Public Security Camera Systems to Help Deter Crime and to Bolster Homeland Security (Feb. 25, 2008) (transcript available at http://eon.businesswire.com/releases/richmond/security/prweb722014.htm).

140. *Id*.

141. *Id*.

ered linking its mesh wireless system for video surveillance with public wireless Internet access.[142]

San Francisco has also considered a dual purpose system. The proposal by EarthLink and Google to provide a municipal wireless system noted its potential use as a backbone for video surveillance.[143] San Francisco's 2005 pilot program of two video surveillance cameras has grown to seventy-four on street corners, monitoring and recording activities of individuals in diverse neighborhoods throughout the city.[144] The city has already spent $900,000 on the cameras, which have been disappointing in preventing or solving crime.[145] The Director of the Mayor's Office of Criminal Justice hoped that the city would purchase additional cameras and begin actively monitoring video feeds.[146] But, in June 2008, the San Francisco Board of Supervisors cut funding for new cameras pending a report on camera effectiveness.[147] Mayor Newsom has made municipal wireless a "top priority" but was thwarted by EarthLink's pulling out of the deal due to the company's financial problems.[148] As the city's criminal justice staff is pushing for more sophisticated and intrusive cameras but is limited by the city budget and oversight by the Supervisors, San Francisco could potentially turn to federal funding to try to accomplish both expanded surveillance and a municipal wireless program.

---

142. Letter from Nicole A. Ozer & Mark Schlosberg to Richmond, CA, City Council (Nov. 15, 2005) (on file with New York University Journal of Legislation and Public Policy).

143. Google Privacy Response Letter, *supra* note 110.

144. Demian Bulwa, *New Criminal Justice Chief Wants Cops Monitoring Cameras*, S.F. CHRON., Feb. 7, 2008, at B3.

145. *Id. See also* CTR. FOR INFO. TECH. RESEARCH IN THE INTEREST OF SOC'Y, PRELIMINARY FINDINGS OF THE STATISTICAL EVALUATION OF THE CRIME-DETERRENT EFFECTS OF THE SAN FRANCISCO CRIME CAMERA PROGRAM (2008), http://www.aclunc.org/issues/government_surveillance/asset_upload_file796_7024.pdf; *see also* American Civil Liberties Union of Northern California, San Francisco Crime Statistics, http://www.aclunc.org/issues/government_surveillance/san_francisco_crime_statistics.shtml (last visited Sept. 28, 2008).

146. Bulwa, *supra* note 144, at B3.

147. *See* American Civil Liberties Union of Northern California, San Francisco Budget Committee Cuts Funding for Surveillance, http://www.aclunc.org/issues/technology/blog/sf_budget_committee_cuts_funding_for_surveillance.shtml (last visited Oct. 29, 2008).

148. Press Release, S.F. Mayor's Office, San Francisco to Issue Request for Proposal to Create Universal, Affordable Wireless Broadband Network (Nov. 8, 2005), *available at* http://www.ci.sf.ca.us/site/tech_connect_page.asp?id=35822; Robert Selna, *S.F. Citywide Wi-Fi Plan Fizzles as Provider Backs Off*, S.F. CHRON., Aug. 30, 2007, at A1.

IV.
Safeguarding Privacy and Free Speech

Despite the great variation among municipal wireless plans, many of the wireless proposals being considered by cities are bad bargains for city residents because in addition to any dollar costs and city resources, people are being forced to pay for them with their privacy and free speech rights. Many of the business models include tracking personal information to use for targeted Internet products and advertising, which means companies have the incentive to collect as much information about people as possible and to keep it as long as possible to reap the greatest economic benefit.

A municipal wireless business that tracks the identities of users, what they are viewing on the Internet, and their locations 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 worry about who is watching their activities and 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 or create a new tool for intrusive monitoring of Americans.

Particularly in light of recent concerns about illegal and unconstitutional spying on Americans,[149] it is important to have safeguards to ensure that private information is properly protected. Adequate protections for privacy and free speech in municipal wireless systems are not merely things we *should* aspire to. When government entities are establishing or promoting a system that provides public electronic communications services, this may constitute "state action" for constitutional purposes and thus *require* compliance with 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.

149. *See* American Civil Liberties Union, NSA Spying, http://www.aclu.org/safefree/spying/. *See also* American Civil Liberties Union, Phone Companies Gave Private Customer Data to Government Without Consent or Court Order, http://www.aclunc.org/issues/privacy/phone_companies_gave_private_customer_data_to_government_without_consent_or_court_order.shtml (last visited Oct. 29, 2008).

The following sections will outline the general safeguards that should be in place for any municipal wireless system: 1) user identities and online activities should not be tracked, recorded, or commercialized, 2) the service must be prepared to resist demands for users' personal data, 3) municipal wireless providers should collect only minimal amounts of information and maintain user logs for the shortest period of time possible, 4) personal data should be protected from others, and 5) the service must provide open access to information.

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

A wireless provider must have some information about a computer in order to route Internet content, but the company does not need to know anything more about the individual who is accessing the Internet and need not keep any records about what sites the user visits. A municipal wireless service provider might want to track personal information about users, such as names, addresses, emails and unique usernames, or track Internet activities so that it can create detailed profiles for use in targeted advertising or to disclose to third parties.[150] Chaska, Minnesota's wireless service requires subscribers to log onto the system using a username and password and identifies each network device.[151] The St. Cloud, Florida, system also requires users to submit personal information to obtain a user name.[152] San Francisco's only limitation about the collection of login information in its proposed contract with EarthLink and Google was to limit Google to collecting only "minimal information." However, the term "minimal" was never defined and what a company labels as minimal may in fact be quite extensive information about an individual.[153] Such tracking and profiling is unacceptable in a municipal wireless network because it threatens an individual's right to privacy and his or her First Amendment rights to speak and associate anonymously. This tracking and profiling makes it difficult for people to maintain control over sensitive information about their activities and will chill their access to constitutionally protected information because of the fear that their Internet searches, activities, or interests might become known to

150. GOOGLE, MARKETING AND ADVERTISING USING GOOGLE: TARGETING YOUR ADVERTISING TO THE RIGHT AUDIENCE (2007), *available at* http://www.google.com/googlebooks/pdf/MarketingAndAdvertisingUsingGoogle.pdf.

151. PRONTO NETWORKS, CHASKA.NET CHASKA, MINNESOTA, A CASE STUDY 4, http://www.prontonetworks.com/ChaskaCaseStudy.pdf (last visited Oct. 29, 2008).

152. CITY OF ST. CLOUD, *supra* note 94.

153. San Francisco Agreement, *supra* note 46, at 22.

others. A city's responsibility to safeguard user identity and online activity must be taken seriously when considering plans for municipal wireless systems.

1. Invading 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.[154] Article I, Section 1 of the California Constitution guarantees an "inalienable" right to privacy.[155] California's 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 that data by the government and third parties. The Argument in Favor of 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 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.[156]

As the ballot proposal recognized, privacy is important because it gives people a zone of autonomy in which to explore intellectual interests, personal relationships, and other socially valuable ends without fear of intrusion and oversight.[157] 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."[158]

In *White v. Davis*,[159] 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.

---

154. U.S. CONST. amend. IV.

155. CAL. CONST. art. 1, § 1.

156. CAL. SEC'Y OF STATE, PROPOSED AMENDMENTS TO CONSTITUTION 27 (1972), *available at* http://library.uchastings.edu/ballot_pdf/1972g.pdf.

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

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

159. White v. Davis, 533 P.2d 222, 233 (Cal. 1975).

> The new provision's primary purpose is to afford individuals some measure of protection against this modern threat to personal privacy.[160]

As an inalienable right, a citizen's privacy should not be bought, sold, or bargained away and cities that enter into contracts for municipal wireless systems must take these rights into account.[161]

2. *Chilling Speech*

Allowing municipal wireless systems to track, record, or commercialize user identities and activities will also chill protected speech and infringe on First Amendment rights. Free speech rights are carefully safeguarded under both the First Amendment of the United States Constitution and Article I, Section 2 of the California State Constitution—which guarantees that "every person may freely speak, write and publish his or her sentiments on all subjects" and that "[a] law may not restrain or abridge liberty of speech."[162] California courts have held that safeguarding the right to free speech is a paramount concern because speech is "a freedom which is the matrix, the indispensable condition, of nearly every other form of freedom."[163]

The Internet has given people of all ages an important outlet to engage in free expression and increased access to information.[164] With the privacy of a computer screen, a person may feel safer or more confident expressing opinions, finding information, asking questions, and purchasing items that otherwise might have been too embarrassing or difficult in person. Whether it be due to an interest in health conditions, reproductive options, lesbian, gay and bisexual information, or unconventional politics—more and more people are turning to the Internet in order to express ideas and find information.[165]

A municipal wireless system that allows the tracking and profiling of users threatens to undermine the benefits of municipal wireless as a public service. People will stop and wonder whether or not it is safe for them to use the Internet as a trusted resource or vehicle for

---

160. *Id.* at 774.

161. *See, e.g.*, CAL. CIV. CODE § 1798.84(a) (West 2008) (making waivers of a variety of California-specific privacy protections inalienable by contract); CAL. CIV. CODE § 1785.36 (West 2008).

162. CAL. CONST. art. 1, § 1.

163. Ferlauto v. Hamsher, 88 Cal. Rptr. 2d 843, 848 (Cal. Ct. App. 1999).

164. Memorandum from Mary Madden, Research Specialist, Pew Internet & Am. Life Project 1 (Apr. 2006), http://www.pewInternet.org/pdfs/PIP_Internet_Impact.pdf.

165. 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.*

free expression. "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."[166] Once people know that they are being "observed and recorded, their habits change; they change."[167] When we are being watched, we are more self-conscious, we worry about what others think, and our actions are influenced accordingly. "To the extent that a person experiences himself as subject to public observation, he . . . will tend to act in ways that are publicly acceptable."[168] A municipal wireless system that tracks and profiles users brings to the municipal wireless system the social conformity barriers that keep people from accessing necessary information in person. In this way, rather than bridging the digital divide, a municipal wireless system could add a worrisome barrier to Internet usage that would 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 them to target advertising could mean that users would receive physical mail, phone solicitations, emails, or pop-up advertisements about particular products or topics. The result might be categorized as a mere annoyance—for example, automatically receiving information about a competitor's products when you search for a particular item. Sometimes it could be frustrating; a family member might stumble upon information sent to your home or to a shared laptop that ruins a surprise present or dream vacation. Other results could be very serious. For instance, if a family computer is used to research a sensitive and private issue such as health concerns or political activity, a later user of the same computer could be presented with advertising pertaining to the subject matter of the earlier browsing and will be privy to information that the original user really needed to keep private.

166. Richard Wasserstrom, *Privacy: Some Arguments and Assumptions*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 317, 328 (Ferdinand David Schoeman ed., 1984).
167. Nicholas C. Burbules, *Privacy, Surveillance, and Classroom Communication on the Internet*, ACCESS (1997), *available at* http://faculty.ed.uiuc.edu/burbules/papers/privacy.html.
168. 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).

4. *Privacy and Free Speech Protections Necessary for Equal Access*

It is particularly important that we ensure that municipal wireless systems have adequate privacy and free speech safeguards if bridging the digital divide is indeed a primary goal of the system. Rather than reducing the digital divide, a municipal wireless system without proper privacy and free speech protections would instead perpetuate a further divide. People who have money will have the option to pick another Internet service provider that has 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. In order to properly safeguard privacy and free speech and enable community members to safely use the system to access important information, it is imperative that cities implement systems that do not track, record and commercialize user identities and online data.

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

As an intermediary, a service provider may find 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. Service providers inherently face pressures from other network users, industries, and governments to disclose personal information about their users. While people might expect their identities, browsing history, or location information to be held in confidence by the municipal wireless provider, the reality is that without the appropriate safeguards, much of that information is not protected by the Fourth Amendment because of the third party doctrine.[169] Without safeguards built into a contract and delineated in privacy policies, once that information is collected by the company, community members' private information will be susceptible to a broad range of disclosure requests, not just from law enforcement agencies, but also from private attorneys. For example, MetroConnect, the consortium of companies that was origi-

169. *See* United States v. Miller, 425 U.S. 435, 442 (1976) (stating that the Fourth Amendment does not apply because there is no reasonable expectation of privacy in banking records, including financial statements and deposit slips, when information was voluntarily revealed to a third party bank); *see also* Smith v. Maryland, 442 U.S. 735, 743 (1979) (stating that the Fourth Amendment does not apply because there is no expectation of privacy in numerical information about telephone records held by the 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.").

nally selected by Silicon Valley to provide region-wide wireless, submitted an end user license agreement that proposed disclosure of user information in response to both criminal and civil subpoenas and gave users no notice prior to disclosure.[170] As courts have noted, users "who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identities."[171] Municipal wireless contracts and privacy policies should include safeguards to require companies to ensure that this in fact does not happen.

The issue of disclosure and the need for safeguards is especially sensitive in the municipal wireless context, where a city may be involved in the provision of the service and its own law enforcement agencies may be seeking information. St. Cloud, Florida, is a prime example. The city collects statistical data about its wireless users. It released data after the first year of the system, including the number of households registered (8,492 or 77.2% of the city), the number of websites visited (more than 410 million), and the average session length (3.5 hours).[172] It is likely that the city could, or does already, collect other more detailed data about who is looking at what websites, from where, and when.[173] However, the Cyber Spot™ Privacy Policy that purportedly delineates what information is actually collected, what is disclosed, and for what purpose, appears not to exist.[174] The Cyber Spot™ terms of use and accepted use policy has a blank space in every area where the Internet address for the privacy policy is supposed to be listed.[175] St. Cloud and other municipalities may face substantial pressure from its own city services to set low thresholds for law enforcement and other agencies to obtain information about individuals' Internet use. Therefore, there must be clear, robust, publicly available rules for how the private information of community members will be safeguarded.

Whether the municipal wireless program is owned and operated by a city or a private entity, there should be high standards and narrow circumstances for disclosure to law enforcement and pursuant to civil litigation. The service provider should be prepared to litigate to avoid disclosing data if the request is legally inadequate. Except in circum-

170. *See infra* Part V.
171. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).
172. Vos, *supra* note 97.
173. *Id.*
174. *See* City of St. Cloud, Florida, Cyber Spot Terms of Service and Accepted Use, http://www.stcloud.org/index.asp?nid=499 (last visited Aug. 13, 2008).
175. *Id.*

stances 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 afford users a real opportunity to protect their personal information, namely (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 Collect Only Minimal Amounts of Information and Maintain User Logs for the Shortest Period of Time Possible

As discussed above, service providers can be the focus of extraordinary requests for users' data. Reducing the amount of information collected and minimizing 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 never 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 that it is kept. Clear policies will conserve resources, protect 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 and city officials from interception by others. 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.[176] It is widely acknowledged by leading security experts that wireless networks are extremely vulnerable to intrusion, even when they have an initial layer of protec-

176. For an example of research detailing 802.11 security vulnerabilities see Department of Computer Science, Univ. of MD: 802.11 Security Vulnerabilities, http://www.cs.umd.edu/~waa/wireless.html (last visited Aug. 18, 2008); Dan Verton, *Flaws in Wireless Security Detailed: Cracked Algorithm, Holes in 802.11 Spec Mean Companies Need More Authentication*, COMPUTERWORLD, July 16, 2001, http://www.computerworld.com/securitytopics/security/story/0,10801,62220,00.html.

tion through encryption. Tools necessary to attack the system and access sensitive data are "freely available on the Internet."[177] Too few cities are thoroughly considering the potential harms that can result when Internet users transmit personal information through Internet sessions or emails on the system.

Cities like Chaska, Minnesota, simply warn community members that their wireless system is insecure, noting:

> The truth is that you are connecting to the open web and someone could potentially "see" your traffic on our wireless network, or after your data leaves our network and is on the wired connection using certain types of programs. This is no different than any other providers network and this could give anyone access to any unencrypted passwords or data.[178]

St. Cloud, Florida, clearly states in its terms of use that it does not provide "security against unauthorized access by others, who may access or monitor your activity and conduct while you are using the Cyber Spot™ services."[179] However, unlike Chaska, which encourages its users to take precautions by encrypting passwords and data, the St. Cloud Terms of Use prohibits users from using the service to "publish any material that is encrypted."[180] Municipal wireless networks should not only incorporate adequate technological protections to protect the transmission of sensitive information, but users should be educated about the full protections available to protect their personal information and be allowed to use those methods.

Cities that are using their municipal wireless networks to enable city workers, from law enforcement to housing inspectors, to send sensitive information wirelessly, must also take clear steps to secure transmission of data. The privacy and security risks inherent in video surveillance and the possibility for costly data breaches from city and law enforcement databases only multiply when it becomes possible for third parties to improperly access this information through an insecure wireless network.

---

177. Marc Delehanty, *WiFi Links Vulnerable Even With Encryption*, CRN AUSTRALIA, July 27, 2006, http://www.crn.com.au/story.aspx?CIID=57402.

178. Chaska.net Residential Connectivity, http://www.chaska.net/mkpage.cgi?services_residential_connect+residential_details (last visited Aug. 18, 2008).

179. CITY OF ST. CLOUD, *supra* note 94.

180. *Id.* ("You acknowledge and agree that you will not use the Cyber Spot™ services for any of the following prohibited activities . . . . publishing any material that is encrypted.").

E. The Service Must Provide Open Access to Information

In order for a municipal wireless system to accomplish its goal of increasing access to information, it also must reject restrictive use policies or software filters that deny or block access to constitutionally protected material. Municipal wireless systems that do not allow users to access the full range of constitutionally protected material—due to prohibitive use policies or filtering—undermine the goal of bridging the digital divide and instead create a system in which people who have the money to pay for other forms of Internet access get full access to information, while others only get a portion of the information. The protection of access to constitutional content is not merely a nice thing for a city to do. When there is state action through municipally owned or supported systems, constitutional rights *must* be safeguarded. The law is well-defined and as to adults, outside of certain categories such as obscenity or child pornography, "the First Amendment bars the government from dictating what we see or read or speak or hear."[181] Cities should be concerned about potential liability if they incorporate restrictive use policies or Internet filters that prohibit the receipt or transmission of constitutionally protected material.

1. Use Policies Must Not Interfere with Speech

Some cities, such as Culver City, California, and St. Cloud, Florida, have included restrictive wireless use policies that interfere with speed. The Culver City Internet use policy stipulates that it may prohibit access to certain websites that it deems "malicious or inappropriate."[182] St. Cloud, Florida, currently prohibits individuals from publishing language or material that is not only "obscene," but also any material deemed to be "profane . . . indecent, disturbing, illegal, infringing, scandalous, outrageous, offensive, defamatory, abusive, harassing, or hateful."[183] Other cities may not even realize that the company with whom they contract for municipal wireless has a restrictive use policy and unless the city negotiates otherwise, use access to constitutionally protected material may be limited. For example, Portland, Oregon selected MetroFi for its municipal wireless plan. MetroFi's Acceptable Use Policy prohibits use of its network for the distribution of "offensive materials" including "pornographic" and

181. Ashcroft v. Free Speech Coal., 535 U.S. 234, 245 (2002); U.S. v. Playboy Entm't Group, Inc., 529 U.S. 803, 811 (2000); Reno v. ACLU, 521 U.S. 844, 874 (1997); Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1989).
182. Culver City Wi-Fi HotSpot, Wifi Access, http://www.culvercity.org/it/culvercitywifi/wifi_access.html (last visited Aug. 18, 2008).
183. CITY OF ST. CLOUD, *supra* note 94.

"indecent materials."[184] Vague and overbroad restrictions on speech have no place in municipal wireless use policies.

2. *Filtering Systems Must Not Block Protected Speech*

Cities should also exclude filtering systems that inappropriately block access to protected speech. Culver City employs a content filtering system to identify and block material that it deems "undesirable or unlawful."[185] A filtering system that makes blocking decisions based on vague and overbroad standards will inevitably prohibit rightful access to constitutionally protected material. Even filtering software that is programmed to target only material that is obscene, "harmful to minors," or that constitutes child pornography, nevertheless blocks vast amounts of protected speech. In 2002, the Kaiser Family Foundation found that "on average, filters incorrectly blocked about one in ten sites on safe sex, condoms, or health issues pertaining to gays."[186] In 2005, Consumer Reports found that blockers were continuing to stop many sites that they should not, including sites about "health issues, sex education, civil rights, and politics"—including KeepAnd BearArms.com, a site advocating gun owners' rights, and the National Institute on Drug Abuse.[187] In 2006, the Free Expression Policy Project at the New York University School of Law found that filtering software over-blocked sites as diverse as the U.S. State Department's Embassy website and whitehouse.org, a political satire site with no adult content.[188] The overblocking problem is due in part because a software program is simply incapable of making fine legal distinctions. Even with advances in software technology, over-blocking has not abated over the years.

---

184. MetroFi, Acceptable Use Policy, http://www.metrofi.com/acceptable_use_policy.html (last visited Aug. 18, 2008).

185. *Culver City, California Implements Pornography and Copyright Filtering Technology on Their Public Wireless Network*, MARKETWIRE, Aug. 22, 2006, http://www.marketwire.com/press-release/Audible-Magic-Corporation-697207.html.

186. VICTORIA RIDEOUT ET AL., THE HENRY J. KAISER FAMILY FOUND., SEE NO EVIL: HOW INTERNET FILTERS AFFECT THE SEARCH FOR ONLINE HEALTH INFORMATION (2002), *available at* http://www.kff.org/entmedia/upload/See-No-Evil-How-Internet-Filters-Affect-the-Search-for-Online-Health-Information-Executive-Summary.pdf.

187. Consumer Reports, Filtering Software Better, But Still Fallible, June 2005, http://www.consumerreports.org/cro/electronics-computers/resource-center/Internet-filtering-software-605/overview/index.htm.

188. MARJORIE HEINS ET AL., BRENNAN CTR. FOR JUSTICE AT NYU SCH. OF LAW, INTERNET FILTERS: A PUBLIC POLICY REPORT (2d ed. 2006), *available at* http://www.fepproject.org/policyreports/filters2.pdf.

3. *Policy and Filtering System Must Not Implicate Fair Use Rights*

Cities must also be very careful that any restrictive policies or filtering systems that are aimed at curbing use of the system for copyright infringement are not interfering with free speech rights. Copyright law provides a set of six exclusive, limited-time rights to copyright holders to serve as an incentive for them to create works.[189] But these ownership rights are buffered by the fair use doctrine which guarantees individuals the right to use copyrighted materials, without seeking a copyright holder's permission, for activities like parody, satire, criticism, news reporting, teaching, scholarship, research, and transformative works.[190] Fair use guarantees a "breathing space" that helps to reconcile the tension that would otherwise exist between copyright law and the First Amendment's guarantee of freedom of expression.[191]

Municipal wireless systems—like that in Culver City, which include use policy language that prohibits using the wireless network to "download any copyrighted matter" and employs a filtering system to prohibit individuals from accessing such material—chills free speech by hampering the ability to create, enjoy, and transmit fair use material.[192] Fair use material can be swept up improperly when automated systems scan content and search for keywords in content titles or when companies search for material that may be incorporating copyrighted material.[193] For example, takedown notices have been issued for "Stop the Falsiness," a parody that included clips of The Colbert Report, and the Universal Music Group targeted political pundit Michelle Malkin's video critique of rapper, Akon, which contained excerpts of his videos.[194]

---

189. CORNELL LAW SCHOOL, Copyright Overview, http://www.law.cornell.edu/copyright/copyright.table.html.

190. U.S. Copyright Office, Fair Use, http://www.copyright.gov/fls/fl102.html (last visited Aug. 18, 2008).

191. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).

192. *See* Kevin Donovan, *Automatic Copyright Enforcement Threatens Fair Use*, FREECULTURE.ORG, Oct. 16, 2007, http://freeculture.org/blog/2007/10/16/automatic-copyright-enforcement-threatens-fair-use/.

193. Kevin J. Delaney, *YouTube Magic: Now You See It, Now You Don't*, WALL ST. J., Aug. 8, 2007, at A1.

194. *See* Elec. Frontier Found., MoveOn, Brave New Films v. Viacom, http://www.eff.org/cases/moveon-brave-new-films-v-viacom (last visited Feb. 19, 2008); Fred von Lohmann, *YouTube's Copyright Filter: New Hurdle for Fair Use?*, ELEC. FRONTIER FOUND., Oct. 15, 2007, http://www.eff.org/deeplinks/2007/10/youtubes-copyright-filter-new-hurdle-fair-use.

Culver City, perhaps aware of the free speech implications of its restrictive policy and filtering system, included language in its user policy that asks individuals to agree to waive their First Amendment claims arising from blocked access to constitutionally protected material. However, such waiver language may not hold up in court. Due to its foundational importance as discussed *supra*, the California courts closely scrutinize any alleged waivers of First Amendment rights, "indulge every reasonable presumption against waiver," and are "unwilling to find waiver in circumstances which fall short of being clear and compelling."[195] Under the clear and compelling standard, First Amendment waivers require knowledge of the right or privileged being waived.[196] It is unclear that an individual could have knowledge of the right or privilege being waived because of the vague and overbroad standard and a lack of information regarding which constitutionally protected sites were being blocked from view. All community members have the right to free speech and access to information. It is improper for municipal wireless systems to contain restrictive use policies or filter content that infringe on these rights. Cities that are developing these programs and residents in those cities must be aware of the implications of these restrictive policies and take steps to ensure that free speech rights are appropriately safeguarded.

V.
CASE STUDIES: PRIVACY AND FREE SPEECH SAFEGUARDS IN EXISTING AND DEVELOPING MUNICIPAL WIRELESS PROGRAMS

Few cities have adequately considered the privacy and free speech ramifications of municipal wireless systems and instituted necessary safeguards. Some, like Philadelphia and Silicon Valley, published municipal wireless vision and business plan documents that did not contain a single word about privacy or free speech.[197] Others, like San Francisco, asked the right questions but failed to negotiate adequate protections. However, some cities, such as Portland, asked the right questions and included many of the right safeguards. The following case studies serve as snapshots of both the failures and relative

195. Ferlauto v. Hamsher, 88 Cal. Rptr. 2d 843, 848 (quoting City of Glendale v. George, 208 Cal. App. 3d 1394, 1398 (1989)).

196. City of Glendale v. George, 208 Cal. App. at 1398.

197. WIRELESS PHILADELPHIA, REQUEST FOR PROPOSALS FOR A CITYWIDE WIRELESS NETWORK (2005), http://www.wirelessphiladelphia.org/pdfs/WP_RFP_4-5-05_rev_v4-CLEAN.pdf.

successes in safeguarding privacy and free speech in municipal wireless systems.

A. Philadelphia

Philadelphia is a sad story. The city established a non-profit entity, Wireless Philadelphia, to make its programs responsive to community needs.[198] But, it has ended up with an incomplete wireless system that also contains woefully poor privacy and free speech safeguards. Wireless Philadelphia contracted with EarthLink to own and operate its city-wide wireless.[199] However, with only eighty percent of its system installed, Wireless Philadelphia was left in the lurch when the company announced plans to sell its wireless business.[200] Those who are able to access the partially completed wireless system have spotty and disappointing service. Those in the low-income community who were relying on the municipal wireless system to be their bridge to Internet access are in a precarious position, seeing the digital inclusion resources dry up.[201]

Even if the system had gone exactly as planned, it still failed to provide important safeguards for privacy and free speech. EarthLink's contract did include a few limitations, requiring the company to inform the public how it will handle disclosure of information about the physical location of users, maintain its current policies for Philadelphians on how it tracks identity and usage, and comply with legal requests for information.[202] The contract also provided subscribers with the opportunity to opt-out of certain limited consumer data collection and marketing information.[203] Personal information could not be sold, rented, or given away by affiliated companies to third parties.[204] However, the fine print reveals that the privacy policies are

198. Breitbart, *supra* note 46, at 7.

199. Wireless Philadelphia Agreement, *supra* note 81, at 1.

200. Naomi Graychase, *EarthLink to Sell Off Its Muni Wi-Fi Business*, WI-FI PLANET, Feb. 8, 2008, http://www.wi-fiplanet.com/news/article.php/3726981; Marguerite Reardon, *EarthLink's Citywide Wi-Fi Biz for Sale*, CNET NEWS, Feb. 8, 2008, http://www.news.com/8301-10784_3-9867634-7.html.

201. Deborah Yao, *Philadelphia Wi-Fi Network Hits Snags*, USA TODAY, Nov. 18, 2007, http://www.usatoday.com/tech/wireless/2007-11-18-philadelphia-wifi_N.htm; Michael Hatamoto, *Philadelphia Wi-Fi Project Now in Jeopardy, EarthLink May Back Out*, BETANEWS, Nov. 19, 2007, http://www.betanews.com/article/Philadelphia_WiFi_project_now_in_jeopardy_EarthLink_may_back_out/1195487302; Goldman, *supra* note 65. Only 613 of the 10,000 digital inclusion bundles slated for distribution had been handed out by December 2007. *Id.* at 16.

202. Wireless Philadelphia Agreement, *supra* note 81, at R-1 .

203. *Id.*

204. *Id.*

superficial safeguards. The Philadelphia contract gave EarthLink expansive rights to collect vast amounts of data about the identity and activities of individuals.[205] Not only could EarthLink collect personal identity information such as name, address, and phone number when users signed up for the service, it could also track identity, online activities, and location information when they used the service, combining all this data with zip codes, demographics, and "other publicly available information from third-parties" to produce even more detailed profiles of individual users.[206] Once EarthLink had this information, it had the right to "disclose personal information or information regarding use of the Services if, for any reason, in our [EarthLink's] sole discretion, we [EarthLink] believe it is reasonable to do so."[207] Now, as Philadelphia considers the next steps for its wireless program, it has an opportunity to thoroughly explore the kind of system that would be appropriate for the city and the privacy and free speech safeguards that should be carefully considered and incorporated in any new plans.

B. Bay Area Cities

While many cities across the country look to the Bay Area as a model for innovation and methods to safeguard the rights of individuals, local cities have so far fallen far short in protecting privacy and free speech in municipal wireless systems. Neither Silicon Valley nor San Francisco has succeeded in developing a municipal wireless system that adequately safeguards the rights of its users and provides equal access to information.

1. Silicon Valley

The prognosis for a wireless system that protects privacy and free speech in the heart of Silicon Valley is not looking rosy. In April 2006, Joint Venture Silicon Valley, a non-profit business-government coalition in San Jose, California, released a request for proposals announcing its new initiative, Wireless Silicon Valley. Its goal was to help coordinate the development of a very ambitious region-wide wireless system to "anyone, anywhere, involving any device."[208] The

205. *See* Wireless Philadelphia Agreement, *supra* note 81, at R-2.

206. *Id.* at R-1.

207. *Id.* at R-3.

208. Paul Krill, *Wireless Program Aims to Cover Silicon Valley*, INFOWORLD, Oct. 24, 2007, http://www.infoworld.com/article/07/10/24/wireless-valley_1.html; *see also* SAN MATEO COUNTY TELECOMM. AUTH., REQUEST FOR PROPOSAL FOR A REGIONAL BROADBAND WIRELESS NETWORK FOR SILICON VALLEY (2006), *available at* http://

new wireless system would cover forty-two municipalities, across a region of 1500 square miles, with a population of 2.4 million.[209] The wireless system, which has been estimated to cost $100 to $150 million, would only work outdoors.[210]

Nothing in the extensive vision and planning documents discussed privacy and free speech considerations.[211] Prior to the release of the request for proposals in April, the ACLU of Northern California (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.[212] These organizations also requested that specific information about privacy and free speech be included in the request for proposals 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.[213]

Wireless Silicon Valley declined to include a specific question about privacy or free speech in the request for proposals but rather agreed to ask each vendor to submit its end user license agreement (EULA)—the agreement that a customer agrees to prior to using the system.[214] Wireless Silicon Valley also pledged at the request for proposals release event to take privacy and free speech into account in its decision.[215] The advocacy organizations expressed concerns that without a specific question in the request for proposals, the vendors would not properly address privacy and free speech issues.[216] As feared, the EULAs submitted were extremely general, and none of the

---

www.jointventure.org/programs-initiatives/wirelesssiliconvalley/documents/Wireless%20Silicon%20Valley%20RFP%20April%2028%202006.doc [hereinafter SAN MATEO RFP].

209. 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.

210. Krill, *supra* note 208.

211. SAN MATEO RFP, *supra* note 208.

212. Letter from Nicole A. Ozer, Technology and Civil Liberties Policy Director, ACLU of Northern California, et al. to Seth G. Fearey, Vice President and Chief Operating Officer, Joint Venture, Silicon Valley Network, (Apr. 17, 2006) *available at* http://www.aclunc.org/issues/technology/asset_upload_file928_6023.pdf.

213. *Id*.

214. Wireless Silicon Valley, End User Joint Venture Request for Proposal, http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/documents/Wireless%20Silicon%20Valley%20RFP%20April%2028%202006.doc.

215. Stephen Lawson, *Silicon Valley WiFi Group Nears Choice of Vendor,* NETWORKWORLD (2006), http://www.networkworld.com/news/2006/080306-silicon-valley-wi-fi-group-nears.html.

216. *See* Letter from Nicole A. Ozer et al., *supra* note 212.

three proposals selected by the task force as finalists—MetroFi, Veri-Lan, and Silicon Valley Metro Connect—even discussed privacy or free speech apart from merely stating that its license agreement was attached to the proposal.[217] A careful reading of the EULAs revealed that each of the proposals had deep privacy and free speech flaws.[218] Meetings and a public forum followed, including presentations about privacy and free speech issues.[219]

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."[220] 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. Neither had any proper safeguards for resisting demands about user information. The company planned to disclose personal information in response to criminal and civil subpoenas without giving users any notice.[221] Finally, there were no limitations on how long data would be stored about users.

In February 2007, Wireless Silicon Valley announced that it would begin the roll-out of the new municipal wireless system in two test markets, San Carlos and Palo Alto.[222] However, in December 2007, the program began to hit substantial snags. Azulstar, one of the primary vendors selected to build and operate the new network, announced that it would not be continuing with the deal because it had not been able to attract major investors.[223] Wireless Silicon Valley began searching for a new main contractor for the network and the

---

217. Joint Venture: Silicon Valley Network, http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/updates.html; MetroConnect Proposal 143, http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/documents/SVMetroConnect_Public_Response_to_SAMCAT_RFP_No_101.pdf.

218. NICOLE OZER, AM. CIVIL LIBERTIES UNION OF N. CAL., SILICON VALLEY WIRELESS: PRIVACY AND FREE SPEECH IMPLICATIONS, http://www.aclunc.org/issues/technology/asset_upload_file174_6023.pdf.

219. Joint Venture: Silicon Valley Network, Privacy and Security in a Wireless World, http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/privacy.html.

220. OZER, *supra* note 218.

221. *Id.*

222. Press Release, Joint Venture, Silicon Valley Network Announces Test Cities for Wireless Silicon Valley Initiative (Feb. 14, 2007) *available at* http://www.jointventure.org/inthenews/pressreleases/021407wireless.html (last visited Oct. 29, 2008).

223. *See* Glenn Fleishman, *Azulstar out as Lead in Wireless Silicon Valley,* WI–FI NET News, Dec. 5, 2007, http://wifinetnews.com/achives/008074.html.

two test markets were put on hold.[224] Wireless Silicon Valley also announced that while the system was originally marketed as a way to provide Internet access to greater numbers of Silicon Valley residents, in order to warm the increasingly cold feet of municipal wireless vendors, the network would now be primarily an economic development tool for use by local businesses with cities as anchor tenants.[225] As an anchor tenant, a city would agree to pay to use the service for municipal needs, thus ensuring that the company will have some guaranteed level of fee-based usage and profit.[226]

While a one square mile pilot program has been launched in San Carlos, the privacy and free speech protections that Wireless Silicon Valley long pledged to incorporate appear to remain grounded. Following the original selection of MetroConnect, Wireless Silicon Valley asked professors from Stanford 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.[227] These professors presented their findings to Wireless Silicon Valley,[228] but there has been no public action yet taken to incorporate these suggestions into the pilot program or any subsequent roll-outs of the system.

2. San Francisco

Unlike some other cities, municipal wireless in San Francisco started in a very promising manner. The city stated in its request for proposals that "the City anticipates a Network that protects the privacy

224. Stephen Lawson, *Silicon Valley Wireless Group Seeks New Builder*, NETWORK WORLD, Dec. 5, 2007, http://www.networkworld.com/news/2007/120507-silicon-valley-wireless-group-seeks.html.

225. Marguerite Reardon, *Citywide Wi-Fi Isn't Dead Yet*, CNET NEWS, Sept. 25, 2007, http://www.news.com/Citywide-Wi-Fi-isnt-dead-yet/2100-7351_3-6209837.html; SMART VALLEY WIRELESS SILICON VALLEY TASK FORCE, *supra* note 41; BRETT COLLINGWOOD ET AL., INTEL SOLUTION SERVICES, WIRELESS SILICON VALLEY TASK FORCE INITIATIVE, WIRELESS BUSINESS MODEL (2006), *available at* http://www.jointventure.org/programs-initiatives/wirelesssiliconvalley/documents/Business-Model.pdf.

226. Municipal WiFi, No Wires, Lots of Strings, http://svextra.com/blogs/gmsv/2007/08/municipal_wifi_—_no_wires_lots_of_strings.html (last visited Feb. 25, 2008).

227. TRAVIS BRANDON ET AL., THE CTR. FOR INTERNET & SOC'Y, STANFORD LAW SCH., PROPOSED CONTRACT TERMS AND PRIVACY POLICY FOR SILICON VALLEY METRO CONNECT, http://cyberlaw.stanford.edu/system/files/MuniWiFiStanford.pdf (last visited Sept. 9, 2008); University of California-Santa Clara, Privacy Agreement Terms and Conditions, http://cyberlaw.stanford.edu/system/files/MuniWifiUC-SantaClara.pdf (last visited Sept. 9, 2008).

228. Joint Venture: Silicon Valley Network, *supra* note 217.

of users, respects consumer choice, and fosters diversity of information and ideas."[229] The city also asked a specific question in the request for proposals about privacy, requiring vendors to specify the privacy policies and security standards that would be put in place "to protect the privacy of—and information transmitted by—users."[230] But when the proposals were submitted, some of the privacy and free speech rights of residents were overlooked.[231] The vendor proposals contained wholly inadequate safeguards against user tracking and commercialization of data.[232] There were few limitations on the amount of information collected and how long it was kept and few explanations of 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.[233]

The final contract between San Francisco and EarthLink and Google[234] made little progress. The contract not only failed to provide options for anonymity but also did not technically limit the amount of personal information that could be collected about users and how it was commercialized.[235] The only safeguards in place regarding 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; "minimal," however, was not defined in the contract.[236] Additionally, EarthLink, but not Google, agreed to allow individuals to opt-out of location tracking.[237] Aside from requiring that EarthLink not store location information about users for more than 60 days, no limits were implemented on how long either company could maintain logs of user information and transactional data.[238] The contracts also contained broad disclosure provisions, allowing the companies to share information for law

229. CITY AND COUNTY OF SAN FRANCISCO, REQUEST FOR PROPOSAL TECHCONNECT COMMUNITY WIRELESS BROADBAND NETWORK 9 (2005), *available at* http://www.sfgov.org/site/tech_connect_index.asp/id=36612.

230. *Id.*

231. ELECTRONIC PRIVACY INFORMATION CENTER, A PRIVACY ANALYSIS OF THE SIX PROPOSALS FOR SAN FRANCISCO MUNICIPAL BROADBAND (2006), http://epic.org/privacy/internet/sfan4306.html.

232. *See generally id.*

233. *See* EARTHLINK MUN. NETWORKS & GOOGLE, *supra* note 28.

234. Nicole A. Ozer, *Companies Positioned in the Middle: Municipal Wireless and Its Impact on Privacy and Free Speech*, 41 U.S.F. L. Rev. 635 app. at 664–68 (2007).

235. *See* San Francisco Agreement, *supra* note 46 at 20.

236. *Id.* at 22.

237. *Id.* at 21.

238. *Id.*

enforcement and national security investigations without requiring a warrant and without providing prior notice.[239] The companies did agree, however, that when allowed by law they would require "court ordered documentation."[240] In response to a demand for information in a civil case, both companies agreed, when allowed by law, to provide notice to the individual prior to disclosing the information.[241] The timing of the notice and whether it would afford the user an opportunity to move to quash was not specified.[242]

The drafting of the final contract was fortunately not the end of this story, and the people of San Francisco were not saddled with a system lacking safeguards. After Mayor Newsom introduced an ordinance asking the Board of Supervisors to approve the EarthLink and Google contract, the local lawmakers started paying attention to the fine print and asking hard questions about whether this system was really a good deal for the city and its community members. The Board of Supervisors began to look closely at several issues including the slow speed of the system and whether the signal could penetrate inside homes and provide needed access to low-income community members.[243] They also asked for critical cost-benefit studies that compared a municipally-owned and operated system to a contract with a private vendor.[244] Several members of the Board of Supervisors were very concerned about the lack of adequate privacy and free speech protections.[245] At a hearing, members of the Board of Supervisors asked the City Department of Telecommunications and Information Services (DTIS) to respond to the concerns of the ACLU of

239. *Id.* at 22.
240. *Id.*
241. *Id.* at 22.
242. *Id.*
243. The Supervisors worried that EarthLink could have potentially profited by limiting the quality of the free service, forcing residents to pay for the higher speed connection. As the wholesale network provider, EarthLink "would have an incentive to limit the amount or quality of competition on the network which limits EarthLink's profit margin as an Internet service provider." BD. OF SUPERVISORS OF THE CITY AND COUNTY OF SAN FRANCISCO, SAN FRANCISCO BUDGET ANALYST, FISCAL FEASIBILITY ANALYSIS OF A MUNICIPALLY-OWNED CITYWIDE WIRELESS BROADBAND NETWORK 26 (Jan. 11, 2007). While it sought to provide Internet access to residents of 95% outdoors and 90% indoors, up to the second floor of the building, individuals would have most likely needed a Customer Premise Equipment device, or CPE, for an additional $80 to $200, in order to strengthen the signal strength and access the system indoors. Residents would have had to pay for the CPE device, relied on the city to pay for the device, or have had to pay for the higher speed connection. *See id.* at 27–28.
244. *See id.* at 14–15, 21, 30, 40; Becca Vargo Daggett, *An Alternative to San Francisco's Wi-Fi Deal*, S.F. CHRON., Jan. 29, 2007, at B7.
245. Robert Selna, *Wi-Fi Plan Hits Snag on Supervisors Panel, Some Progressives on Board Say Terms Aren't Good Enough*, S.F. CHRON., May 15, 2007, at B1.

Northern California.[246] DTIS's response only confirmed the worries of those who felt that the privacy and free speech safeguards were wholly inadequate.[247] As a result of concerns, members of the Board started negotiating to amend the proposed EarthLink contract.[248]

While the Board was awaiting a response from EarthLink about some suggested modifications to the contract, the Mayor proposed a non-binding ballot measure, Proposition J.[249] Submitted five minutes before the deadline, the ballot measure asked the citizens of San Francisco to vote on whether they supported privately-operated municipal wireless.[250] While the ballot initiative was entitled, "Declaration of policy supporting a wireless broadband network that. . .protects user privacy," it contained inadequate privacy provisions.[251] The ballot language only limited the collection of user location information and company sharing of information with third parties. It lacked safeguards to stop the collection of login or use information and was void of protections to ensure that information was not used for targeted advertising or turned over to the government.[252]

However, prior to San Francisco's election and a vote on Measure J, EarthLink gave notice in August 2007 that it was pulling out of the proposed contract due to financial difficulties and a change in its leadership.[253] The company had encountered difficulties in other segments of its business and determined that it could not go forward with any new municipal Wi-Fi projects.[254] While the Mayor was disap-

246. *Id.*

247. DTIS Response to ACLU of Northern California, *available at* http://www.aclunc.org/issues/technology/dont_let_internet_hot_spots_chill_privacy_and_free_speech.shtml. Letter from Nicole A. Ozer & Kurt Opsahl to San Francisco Supervisor, Dep't of Telecommunications and Information Services (July 9, 2007), (on file with New York University Journal of Legislation and Public Policy).

248. S.F. PLANNING & URBAN RESEARCH ASS'N, BALLOT ANALYSIS: NOVEMBER 2007 (2007), http://www.spur.org/documents/1107_ballot_analysis.shtm [hereinafter SPUR BALLOT ANALYSIS].

249. Cecilia M. Vega & Wyatt Buchanan, *11th-Hour Welter of Ballot Measures: Wi-Fi, Horse Stables Among Issues That Just Make the Deadline*, S.F. CHRON., Aug. 4, 2007, at B1; SPUR BALLOT ANALYSIS, *supra* note 248.

250. Vega & Buchanan, *supra* note 249.

251. GAVIN NEWSOM, DECLARATION OF POLICY SUPPORTING A WIRELESS BROADBAND NETWORK THAT PROVIDES FREE HIGH-SPEED INTERNET ACCESS FOR ALL SAN FRANCISCANS AND PROTECTS USER PRIVACY (2007), *available at* http://www.aclunc.org/issues/technology/asset_upload_file809_6023.pdf.

252. *Id.*

253. Robert Selna, *S.F.'s Wi-Fi Plan Fades Away, Provider Bails*, S.F. CHRON., Aug. 30, 2007, at A1.

254. Nancy Gohring, *EarthLink Layoffs Signal Change in Muni Wi-Fi*, COMPUTER WORLD, Aug. 29, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9033439.

pointed that the high-profile plan to implement municipal wireless was stalled, Supervisor Ross Mirkarimi expressed relief that the contract was not finalized and that San Francisco, unlike Philadelphia, was saved from being "stuck with a questionable network and company. . . . 'EARTHLINK's meltdown confirms our concerns that the risks outweighed the benefits.'"[255] The fate of municipal wireless in San Francisco is uncertain. While Measure J stayed on the San Francisco ballot and forty-four percent of San Franciscans voted for it, no company has come forward to contract with the city for a new system.[256]

San Francisco has now entered another phase in its quest to develop city-wide wireless. As discussed in Part III, both Meraki and FON piloted innovative new wireless business models in the city.[257] FON has already discontinued its program of distributing free hardware, deciding to be "a little more cautious" with its money.[258] However, Meraki is still engaged in its "Free the Net" initiative.[259] While the company's records show that 110,000 users have logged onto a wireless router to experiment with its service, the company must have many more people in diverse portions of the city agree to host its routers if it hopes to provide access throughout San Francisco.[260] The fact that the routers are installed on private property rather than being maintained by the city might also make the overall system less dependable as machinery breaks down and there is no oversight by a government agency. Wireless consultant Craig Settles warns that Meraki's mesh network is a complement for, not a replacement for, traditional municipal Wi-Fi.[261]

There are also questions about whether using Meraki is a sustainable model for San Francisco. While the routers and Internet service is free now, will Meraki start charging community members to replace broken routers or force them to start sharing their Internet access in future years? Meraki is also using tracking technology to monitor and

255. Selna, *supra* note 253.

256. The ballot results for Measure J indicate that 44,998 people or 63.8% of voters were in favor of the measure while 25,532 or 36.2% of voters opposed it. SanFranciscoSentinel.com, San Francisco Ballot Results, November 7, 2007, http://www.sanfranciscosentinel.com/?p=6760 (last visited Sept. 9, 2008).

257. *See supra* Part III.D.

258. *See* van Zanten, *supra* note 135.

259. Meraki, Free the Net San Francisco, http://sf.meraki.com/faq (last visited Sept. 9, 2008).

260. Meraki, Meraki Is Bringing Free Wireless Internet to San Francisco, http://sf.meraki.com/ (last visited Sept. 9, 2008).

261. Naomi Graychase, *Meraki Frees the 'Net in San Francisco*, WI-FI PLANET, Jan. 4, 2008, http://www.wi-fiplanet.com/news/article.php/3719826.

record IP addresses, online activities, and location to serve targeted advertising and content.[262] Meraki is currently giving people in San Francisco the option of opting out of this data collection. But, is there anything to stop the company from reverting to its standard policy in a year or two after the routers are deployed and some community members start to rely on the system?[263] As the Meraki system has so far bypassed any public process or oversight, the thorough analysis and important questions that the Board of Supervisors asked about the EarthLink and Google contract have so far gone unasked and unanswered. Trouble may be looming ahead for privacy and free speech in San Francisco unless these issues are discussed and safeguards are put in place.

C. Portland

Amidst all of the cities that pushed forward with municipal wireless with nary a thought to privacy and free speech, Portland is a shining exception. In August 2006, it signed a nonexclusive use agreement with MetroFi to build a municipal wireless system.[264] This agreement articulated an overarching vision that included privacy protections and many of the fundamental safeguards on information collection, retention, and disclosure discussed in Part IV.[265]

The agreement includes an overarching statement that service providers "shall protect privacy of users."[266] It also requires that users be informed of the terms of use (including the privacy and data collection policies) upon initial connection to either a no-fee or subscription service, that the service provider shall obtain affirmative consent again where there is a material change to information collection or use policies, and that any entities that receive personally identifiable informa-

262. Meraki, *supra* note 125.

263. *Id.*

264. Network Connectivity Nonexclusive License Agreement Between the City of Portland and MetroFi, Inc., Aug. 2006, *available at* http://www.portlandonline.com/shared/cfm/image.cfm?id=129511 [hereinafter Portland Agreement].

265. *See id.* The status of the system may be in jeopardy. MetroFi seems to be slowing in its development of the system and is demanding more funds from the city to complete the network. Dailywireless.org, MetroFi Vs. Portland, http://www.dailywireless.org/2008/02/03/metrofi-vs-city-of-portland/ (last visited Sept. 9, 2008); The contract documents present this overarching vision of privacy protection. PORTLAND ONLINE GOVERNMENT SPECIAL PROJECTS UNWIRE PORTLAND DOCUMENTS (RFPs & Contracts), *available at* http://www.portlandonline.com/index.cfm?c=43149& (last visited Sept. 9, 2008).

266. Portland Agreement, *supra* note 264, at 22.

tion from the service provider shall be held to the same standards detailed in the agreement.[267]

The agreement also includes important limitations on the collection and retention of personal information. Service providers may not collect "any personally identifiable information beyond what is required to operate Services, except as required by law or authorized by this Agreement."[268] It defines personally identifiable information broadly, including any identifiers that are linked to an individual,[269] and stipulates that this data collection limitation applies to all aspects of the business relationship, from email server and firewall logs to customer databases.[270] Whatever personally identifiable information is collected can be maintained "only as long as it is operationally necessary, except as required by law."[271] Service providers are not permitted to link multiple Internet session activities or create a log of activities associated with personally identifiable information.[272] The service provider may compile and use anonymous profile information for advertising, but it must disclose this activity in the terms of use, and any usage history data must remain anonymous and can not be associated with personally identifiable information.[273] In addition, all of this anonymous usage history data has to be deleted after ninety days.[274]

The agreement also contains important limitations on disclosure of personally identifiable information. Service providers may not share any information with third parties, except as required by law or for purposes necessary to operate the services.[275] The agreement also stipulates that "necessary to operate services" does not include sharing personally identifiable information with advertisers or third-party advertisement delivery services.[276] Before data is used for marketing by affiliates or non-affiliates, a user must give consent (opt-in); moreover, the company cannot require users to agree to opt-in to the sharing of personally identifiable information as a pre-requisite for use of the service.[277]

---

267. *Id.* at 22–23.
268. *Id.* at 22.
269. *Id.*
270. *Id.* at 22–23.
271. *Id.* at 23.
272. *Id.*
273. *Id.*
274. *Id.*
275. *Id.*
276. *Id.*
277. *Id*.

The Portland contract lacks several important provisions, such as the provision of notice when a subpoena has been issued. It also fails to include adequate protections for free speech as discussed in Part IV.[278] But it is nevertheless a very strong model for how a city can incorporate the important safeguards discussed in this Article.

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 are not "free" because community members do not have adequate safeguards for privacy and free speech. Without these protections, the civil liberties of individuals are not properly protected. Furthermore, many of the current business models undermine the goal of municipal wireless to provide increased access to information; individuals cannot feel comfortable using the service to access sensitive information if they are not assured that such information will remain private. As cities usher in a new communications infrastructure for their citizens, now is the time to incorporate robust safeguards for civil liberties and ensure that community members are not forced to pay for systems with their privacy and free speech rights.

278. *See supra* Part IV.