

BALANCING THE BENEFITS AND PRIVACY CONCERNS OF MUNICIPAL BROADBAND APPLICATIONS

*E. Casey Lide*¹

INTRODUCTION

The continuing emergence in the United States and elsewhere of municipal broadband networks²—citywide Internet Protocol-based communication networks³ supported and used by local government entities⁴ and sometimes by the general public—has produced ample debate in telecommunications policy circles over their advisability, impact, and prognosis. Governments use these networks to do everything from monitoring street traffic to providing government employees with remote file access. These and other municipal applications require both the availability of uninterrupted network connectivity and

1. Casey Lide is a principal attorney in the Washington, D.C. office of the Baller Herbst Law Group, P.C., and regularly represents local governments and public power systems on a broad range of matters involving telecommunications and Internet services. The views expressed in this paper are those of the author, and do not necessarily represent the views of the Baller Herbst Law Group, or its attorneys, staff, or clients.

2. Municipal broadband systems may utilize wireless networks (the focus of this Article), wireline networks (such as fiber-to-the-premises (FTTP) infrastructure), or a combination of transmission technologies. As of August 2007, there were ninety-two city/region-wide municipal wireless networks in operation, with two hundred and fifteen deployments in planning stages by cities or counties. MuniWireless, Updated: August 2007 List of US Cities and Counties with WiFi, <http://www.muniwireless.com/2007/08/12/updated-august-2007-list-of-us-cities-and-counties-with-wifi/> (last visited Aug. 5, 2008).

3. Internet Protocol (IP) is a general term for the network-layer transmission protocol in the overall Internet protocol suite. Data travels over an IP network in the form of packets. See, e.g., INFO. SCIENCES INST., RFC 791, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY INTERNET PROGRAM PROTOCOL SPECIFICATION *passim* (Jon Postel ed., 1981), available at <http://www.faqs.org/rfcs/rfc791.html>.

4. This Article's analysis of applications and privacy issues is limited to the use of municipal broadband networks by government entities to carry out day-to-day business. Connectivity provided to the general public using such networks, whether free or on a subscription model, may implicate a number of additional issues such as filtering and targeted advertising. See Sascha D. Meinrath, *Municipal Wireless Success Demands Public Involvement, Experts Say*, GOV'T TECH., Apr. 8, 2008, <http://www.govtech.com/dc/articles/271842>. While these topics are related and are worthy of debate, they are outside the scope of this Article.

the assurance that such connectivity will be robust and secure, which can arguably only be guaranteed by a centrally-controlled network. While within a locality Wi-Fi signals may exist in coffee shops, libraries, residences, and businesses, municipal governments are unlikely to effectively rely upon such ad hoc connectivity to support the deployment of certain municipal broadband applications. As a result, municipalities are increasingly providing their own networks.⁵

This Article suggests that we are only at the beginning of a steady, ongoing emergence of municipal broadband applications and the development of the infrastructure necessary to support them. Such applications go well beyond merely providing access to the Internet:⁶ they have potentially enormous positive implications for government efficiency, public safety, and citizen interaction. As technological capabilities have increased, municipal broadband applications have become more inventive and more productive, but also, some would argue, more likely to invade personal privacy.

To the extent privacy concerns exist, this Article argues that they may be effectively addressed through enlightened local policymaking and reliance on existing legal structures. Privacy issues need not hamstring the development and deployment of potentially revolutionary municipal applications and services that rely on citywide broadband networks. Longstanding procedures and protections of “good government” at the local level—such as open records and sunshine laws—coupled with the diligent oversight of privacy advocates, can provide sufficient checks to ensure that municipal broadband applications remain sensitive to privacy concerns.

As a final introductory point, this Article’s use of the term “the government” must be explained. Government entities operating mu-

5. See BEN SCOTT & FRANNIE WELLINGS, *FREE PRESS, TELCO LIES AND THE TRUTH ABOUT MUNICIPAL BROADBAND NETWORKS* *passim* (2005), available at http://www.freepress.net/files/mb_telco_lies.pdf; Al Sherwood et al., *The Vital Role of Local Governments in Wireless Broadband*, *GOV’T TECH.*, Oct. 17, 2006, <http://www.govtech.com/gt/articles/101716>; Memorandum from Jim Baller & Casey Lide to the Tenn. Broadband Coal. *passim* (Mar. 4, 2006), http://www.baller.com/pdfs/BHLG_White_Paper_Tenn_3-4-06.pdf; SAINT PAUL BROADBAND ADVISORY COMMITTEE, *SAINT PAUL: AMERICA’S MOST CONNECTED CITY* *passim* (2007), available at <http://www.ci.stpaul.mn.us/DocumentView.asp?DID=3821>.

6. Recent trends in municipal broadband projects nationwide indicate a shift away from the concept of a network reliant on advertising and the sharing of user data. Accordingly, this Article does not address in detail privacy issues concerning the provision of pure Internet access, including the use of user identities, location tracking, and sharing information with third parties for advertising purposes. For a perspective of such issues from the ACLU, 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 *passim* (2007).

nicipal broadband systems that provide service to the public need not be law enforcement bodies, and, in fact, operationally they usually most resemble privately owned providers. The mere fact that “the government” may provide the broadband service does not mean that surveillance by law enforcement or others is more likely to occur. This is true for both online (Internet and email) surveillance⁷ as well as applications such as a video camera system or wireless sensor network.

Part I of this Article begins with a discussion of some of the benefits of municipal broadband applications, focusing on three categories: mobile workforce applications; embedded wireless sensor applications that monitor and communicate information about the physical environment; and video camera systems, also referred to as closed-circuit TV (CCTV). This Part will highlight the efficiencies gained through the use of these applications, such as the maintenance of constant Internet access for government employees in the field; the use of sensors to remotely compile information on, for example, residential and commercial electricity usage; and the improvements to public safety enabled by CCTV. Part II explores some of the privacy issues related to the expanded use of broadband applications by municipal networks. Part III will then discuss legal tools available to address the privacy concerns, beginning first with a brief discussion of the inadequacy of relying on the Fourth Amendment to address fears of a surveillance society, and then focusing on the important role of state and local open records and sunshine laws in this context. Part IV turns to public policy considerations, and recommends that local governments accept responsibility for developing thoroughly considered and publicly-accessible policies on the collection and use of information by municipal broadband applications. It will conclude with a review of factors policymakers might consider in light of the emerging technologies and the existing legal frameworks.

I.

BENEFITS OF MUNICIPAL BROADBAND APPLICATIONS

A. *Positive Impact of Municipal Broadband Applications*

This section provides an overview of several prototypical government applications that rely upon a municipally-supported communications infrastructure and that confer demonstrable benefits to local

7. For a discussion of government online surveillance, see Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 *passim* (2004).

governments and their citizens. The focus will be on three categories of municipal broadband applications that raise potential concerns regarding the privacy of municipal networks: mobile workforce applications; embedded wireless sensor applications that monitor and communicate information about the physical environment; and video camera systems, also known as CCTV (closed circuit TV).

1. *Mobile Workforce Applications*

According to some estimates, more than fifty percent of municipal employees are mobile, that is, they do not work at a desk or computer workstation. These municipal employees working “in the field” include firefighters, park rangers, and building inspectors. While these employees frequently are equipped with a mobile phone or some other radio device, the development of wireless broadband infrastructure enables a new family of multimedia applications to help them do their jobs more effectively.⁸

A municipal broadband wireless system enables emergency workers to obtain critical information while in the field. Building floor plans and egress information can be transmitted to fire departments via a wireless network, and firefighters can access the plans directly while en route to a fire. One report estimates that trucks can leave the station ninety seconds faster as a result.⁹ To the extent that various city departments make data available in a usable format, firefighters could also access and transmit relevant information from other jurisdictions and departments, such as traffic control, transit authorities, county inspectors, the Federal Bureau of Investigations (FBI), and Homeland Security. Medical personnel and other first responders can also take advantage of broadband. For example, a recent initiative in the City of Corpus Christi, Texas allows first responders and Emergency Response (ER) personnel to access individuals’ medical data if they are unable to speak.¹⁰ Dozens of municipalities nationwide have implemented similar projects.¹¹

8. CRAIG SETTLES, MUNI WIRELESS MOBILE APPLICATIONS: A VIEW FROM THE FIELD 4–5 (2007), available at <http://www.successful.com/msp/Snapshot-1-07.pdf>.

9. *Id.* at 4, 13 (quoting Charles Hewitt, CIO, Providence, RI).

10. *Id.* at 7 (quoting Leonard Scott, Business Unit Manager of Corpus Christi, Texas).

11. Notable cities include Los Gatos, CA and Annapolis, MD. Carol Ellison, *Los Gatos Ca., Unwires Municipal Areas*, MUNI WIRELESS, Mar. 20, 2008, <http://www.muniwireless.com/2008/03/20/los-gatos-ca-unwires-municipal-areas/>; Mike Perkowski, *Annapolis Readies Wireless for Public Safety*, MUNI WIRELESS, Jan. 29, 2008, <http://www.muniwireless.com/2008/01/29/annapolis-readies-wireless-for-public-safety/>. For a list of cities with municipal wireless initiatives, see MuniWireless, City Initiatives Directory (Jan. 18, 2007), http://muniwireless.com/downloads/mw_initia

The potential efficiencies extend beyond emergency personnel. Remote access to all sorts of files can improve the effectiveness of other mobile employees. For example, in Macomb County, MI, social workers who make home visits can view entire case files remotely, inputting updates at the site and accessing other information and resources as needed. Environmental inspectors can take samples and make observations much more accurately with geographic information system (GIS) mapping and global positioning systems (GPS).¹² Municipal building and construction inspectors can expedite the permitting process if, when in the field, they can transmit pictures immediately to an engineer or other expert resource, and can download, complete, and issue permits and other statements at the time of the visit. The cities of Milpitas, CA and Providence, RI estimate that, by not having to travel back and forth to an office, code inspectors save at least an hour per day.¹³ Carl Dresher, who has been actively engaged in municipal wireless projects as the IT Director for Tucson, AZ, noted, "Once you put something in place you'll see opportunities that you never thought of before."¹⁴ Indeed, these are but a few examples of the potential benefits of a pervasive, reliable, centrally-controlled broadband infrastructure.

2. *Embedded Wireless Sensor Networks*

The combination of ubiquitous broadband and embedded wireless sensor technology with automation presents a striking glimpse of municipal broadband's long-term possibilities, particularly as costs decrease and capabilities increase. As explained in the literature of UCLA's Center for Embedded Network Sensing, such a network involves "robust distributed systems of thousands of physically-embedded, unattended and often untethered devices."¹⁵ The concept mirrors

tives0116.pdf. Some suggest that public safety may present the strongest case for a viable return-on-investment for municipal wireless, particularly with the proliferation of available grant funds from the federal and state governments. While early municipal wireless projects tended to focus on providing "free Internet access for all," more recently these projects have concentrated on public safety and other applications used exclusively by the government. Press Release, ABI Research, Municipal Wi-Fi Needs a Paradigm Shift (Dec. 4, 2007) (quoting Stan Schatt, vice president and research director of ABI Research), <http://www.abiresearch.com/abiprdisplay.jsp?pressid=996>.

12. SETTLES, *supra* note 8, at 9, 12 (quoting Cindy Zerkowski, IT Director of Macomb County, MI).

13. *Id.* at 11, 13 (quoting Bill Marion, Information Services Director for Milpitas, CA, and Charles Hewitt, CIO, Providence, RI).

14. *Id.* at 12.

15. Center for Embedded Networked Sensing, What Is Embedded Networked Sensing (ENS)?, <http://research.cens.ucla.edu/about/whatisens/> (last visited Aug. 2, 2008).

a vision described over a decade ago by the late Mark Weiser, referred to as “the Internet of Things,” in which tiny, inexpensive radio transceivers are installed in various everyday items, “enabling new forms of communication between people and things, and between things themselves.”¹⁶ The potential for the presence of various types of radio-frequency identification devices (RFID) in items as diverse as inventory pallets,¹⁷ automobiles,¹⁸ passports, pets,¹⁹ and even human beings²⁰ presages a future in which the presence of embedded wireless devices becomes far more widespread. Many current examples of RFID tag usage do not rely upon a broadband connection requiring the close proximity of specialized sensor devices. The sensor devices themselves, though, may well be increasingly Internet-connected, and there is no shortage of innovative ideas for the future of this field.

There are several notable examples of innovative applications already in use that pair embedded wireless sensors and broadband connectivity. One such application is Automated Meter Reading (AMR), a technology now employed by numerous municipal electric utilities across the country.²¹ With AMR technology, cities can check meters (typically those measuring electricity, but also sometimes applied to those measuring natural gas and water) as often as necessary and can match usage with price fluctuations. The U.S. Energy Policy Act of 2005 recommends that utility regulators support a “time-based rate schedule [to] enable the electric consumer to manage energy use and

16. INT’L TELCOMM. UNION, STRATEGY AND POLICY UNIT, THE INTERNET OF THINGS 2 (2005), available at http://www.itu.int/dms_pub/itu-s/otp/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf; see Elizabeth Biddlecombe, *UN Predicts ‘Internet of Things,’* BBC NEWS, Nov. 17, 2005, <http://news.bbc.co.uk/1/hi/technology/4440334.stm>.

17. Laurie Sullivan, *Wal-Mart RFID Trial Shows 16% Reduction in Product Stock-Outs*, INFORMATIONWEEK, Oct. 14, 2005, <http://www.informationweek.com/showArticle.jhtml?articleID=172301246>.

18. The E-ZPass system of automatic toll collection uses a form of RFID tag. E-Z Pass, *How It Works*, <http://www.ezpass.com/static/info/howit.shtml> (last visited Aug. 2, 2008); Claire Swedberg, *RFID Provides ETAs to N.Y. Drivers*, RFID JOURNAL, Oct. 12, 2007, <http://www.rfidjournal.com/article/articleview/3673/1/1/>.

19. The Humane Society of the U.S., *Microchips: Common Questions*, http://www.hsus.org/pets/issues_affecting_our_pets/common_questions_about_microchips.html (last visited Aug. 2, 2008).

20. The Eastman Kodak Company has a patent on a digestible RFID tag used to monitor ingestion of medicine. Beth Bachelder, *Kodak’s RFID Moment*, RFID JOURNAL, Feb. 28, 2007, <http://www.rfidjournal.com/article/articleview/3100/1/1/>. School children in Japan have begun to wear RFID tags to increase their safety on the way to and from school. Claire Swedberg, *RFID Watches over School Children in Japan*, RFID JOURNAL, Dec. 16, 2005, <http://www.rfidjournal.com/article/articleview/2050/1/1/>.

21. Al Perlman, *A Perfect Match: Wi-Fi Plus Automated Meter Reading (AMR)*, MUNI WIRELESS, Spring 2007, <http://www.muniwireless.com/2007/02/15/a-perfect-match-wi-fi-plus-automated-meter-reading-amr/>.

cost through advanced metering and communications technology.”²² Utility companies in the United States and elsewhere are exploring various approaches for doing so, virtually all of which rely on some sort of wireless sensor technology.

One of the first municipalities to use a municipal Wi-Fi network for AMR was Corpus Christi, Texas. In 2002, Corpus Christi decided to automate its 146,000 gas and water meters supplying a 147-square-mile area. Before automation, human meter readers were having “difficulty accessing a property because of fences or dogs,” and the City received “several complaints per day, every day, from customers who believe[d] their utility statements [were] incorrect.”²³ The new municipal Wi-Fi application, which cost about \$20 million, eliminates these problems and will save the City \$30 million over the next twenty years.²⁴ A similar AMR system in Anderson, IN is expected to save the city \$18 million over fifteen years.²⁵ Likewise, in Northern California, nine million customers of Pacific Gas & Electric Company (PG&E) are being retrofitted with SmartMeters that will report electricity consumption in their homes on an hourly basis. PG&E can alter pricing by season and time of day and provide discounted rates to customers who shift energy usage to off-peak periods.²⁶ Similarly, the Los Angeles Department of Water and Power (LADWP), the nation’s largest municipal utility, has expanded its AMR system.²⁷

Wireless sensor technology has many potential uses beyond AMR. A pilot project in Cambridge, MA, involves over one hundred Wi-Fi enabled environmental sensors mounted on and powered by

22. Energy Policy Act of 2005, Pub. L. No. 109-58, § 1252, 119 Stat. 594, 964 (codified as amended at 16 U.S.C. 2621(d)).

23. TROPOS NETWORKS, CORPUS CHRISTI PIONEERS METRO-WIDE WI-FI MESH 3 (2007), *available at* http://www.tropos.com/pdf/case_studies/tropos_casestudy_corpus_christi.pdf (quoting Leonard Scott, MIS unit manager and program manager); Perlman, *supra* note 21.

24. TROPOS NETWORKS, *supra* note 23, at 4.

25. Carol Ellison, *Wireless Meter Reading Expected to Save \$18.7M*, MUNI WIRELESS, Mar. 9, 2008, <http://www.muniwireless.com/2008/03/09/wireless-meter-reading-expected-to-save-187m/>.

26. Press Release, Pac. Gas & Elec. Co., Pacific Gas and Electric Company’s SmartMeter Proposal Approved by California Public Utilities Commission (July 20, 2006), http://www.pge.com/about/news/mediarelations/newsreleases/q3_2006/060720a.shtml.

27. “LADWP has deployed almost 9,000 SmartSynch SmartMeters, resulting in a reduction in total consumption by over 5%. The system has led to a reduction in peak demand by 240 Megawatts, freeing enough energy for an additional 240,000 homes. Furthermore, the system is estimated to reduce electricity bills by 15% for customers using the technology.” SMARTSYNCH, CASE STUDY: LOS ANGELES DEPARTMENT OF WATER AND POWER’S AUTOMATED METER READING PROJECT 4, *available at* http://www.smartsynch.com/pdf/LADWPcasestudy_000.pdf (last visited Aug. 2, 2008).

streetlamps that will allow researchers to track pollution and weather.²⁸ Wireless sensors could also be used to notify a municipal employee when it is necessary to visit a particular facility or device. A municipal trash receptacle in a remote public park might send a message to the sanitation department when it is ready to be emptied. A Wi-Fi enabled parking meter could send a signal to a local enforcement officer when the meter has expired, or it could be equipped to take a picture of the offending vehicle's license plate. About a dozen cities are considering wireless parking systems that can inform drivers where spaces are available and enable them to pay for a meter remotely via cell phone.²⁹

These sorts of sensor-based applications are not entirely new. For years, industrial processes and critical facilities have used large-scale measurement and control systems known as SCADA (Supervisory Control and Data Acquisition). Used extensively to protect and monitor critical facilities such as power plants, SCADA refers to the ability of sensor-equipped buildings, facilities, or other devices to automatically communicate with a designated person or process upon a particular event.³⁰ For example, if a fire alarm is triggered in a room in a plant, or if a video camera notices motion where there should be none, software can instantly notify a particular chain of command or initiate a public safety response. As SCADA-like concepts and technology are applied at the municipal level—with sensors monitoring manhole covers, hydrants, traffic lights, switches, trashcans, and vehicles—imaginative applications with potentially dramatic benefits to governments and citizens will emerge.

3. Video Camera Systems

Video camera systems, also referred to as closed-circuit TV (CCTV), have been used by governments for a long time and have arguably become an accepted part of the fabric of modern society—at least for the purpose of monitoring high-crime areas, sensitive areas, or critical facilities. The use of video camera systems by governments

28. Ben Ames, *Cambridge Researchers Plan Wireless Sensor Network*, PC WORLD, Apr. 8, 2007, http://www.pcworld.com/article/130493/cambridge_researchers_plan_wireless_sensor_network.html.

29. For example, the City of San Francisco is deploying six thousand small plastic wireless sensors in metered parking spaces to enable drivers to be alerted by street signs or cell phones when and where a spot becomes available. John Markoff, *Can't Find a Parking Spot? Check Smartphone*, N.Y. TIMES, July 12, 2008, at C1.

30. techFAQ.com, *What is SCADA?*, <http://www.tech-faq.com/scada.shtml> (last visited Aug. 2, 2008); SETTLES, *supra* note 8, at 8 (quoting Merton Auger, City Administrator for Buffalo, MN).

likely will continue expanding rapidly as the costs of camera equipment, data storage, and video transmission continue to plummet and public safety funding continues to flow.³¹

Municipal broadband video camera systems, particularly those enabled by wireless, introduce even greater efficiency and opportunity for innovative use. In the past, video camera systems would generally be tethered to a wire line infrastructure. For each camera a particular transmission line—often leased from a phone company or other service provider at substantial expense—would provide the means to transmit the image to a given destination, such as a police station or transportation department. With a municipal broadband system, the expense of installing or leasing an individual wireline disappears. As wireless capabilities increase, cameras can be deployed even more cheaply and with greater flexibility and innovation.³² Temporary camera deployments, for special events or as a response to a disaster, become more economical and useful.³³ Eventually, instead of merely receiving video footage, patrol cars themselves might possess cameras that, using a municipal wireless system, could transmit a live feed to a dispatch station or other patrol cars.³⁴ With a municipal broadband system, video cameras become a much more powerful tool, enabling governments to more efficiently monitor the cities for which they are responsible.

The primary motivation for municipal video camera systems is public safety, and placing cameras in high-crime areas can have a deterrent effect. A municipal wireless video camera system in Rockford, IL, operational since 2005, reportedly helped lower crime by twenty percent.³⁵ In Chicago, IL, a computer-operated surveillance system notifies police when people “loiter[] near critical infrastructure locations, park[] vehicles in restricted areas or leav[e] packages unat-

31. Martha T. Moore, *Cities Opening More Video Surveillance Eyes*, USA TODAY, July 18, 2005, at 3A.

32. See Indrajit Basu, *Making the Case for Wireless Video Surveillance*, GOV'T TECH., Jan. 23, 2008, <http://www.govtech.com/dc/articles/253947>.

33. MuniWireless, *MuniWireless 101: Applications: Video Surveillance*, Jan. 1, 2008, <http://www.muniwireless.com/2008/01/01/muniwireless-101-applications-video-surveillance/>.

34. MARK SCHLOSBERG & NICOLE A. OZER, UNDER THE WATCHFUL EYE: THE PROLIFERATION OF VIDEO SURVEILLANCE SYSTEMS IN CALIFORNIA 8 (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.

35. Basu, *supra* note 32 (quoting Paul Hackerson, security director of the Rockford Housing Authority).

tended.”³⁶ Software to automatically read license plates can also be used, as well as a variety of other triggers that depend on wireless sensor technology.

As some municipalities are discovering, the ability to rapidly deploy a camera system, or to repurpose an existing system in response to an event, is a realistic option if there is reliable wireless access. The increased flexibility of a broadband-enabled camera system can be especially helpful in the case of disaster response. As the collapse of the Interstate 35 bridge in Minneapolis on August 1, 2006 demonstrated, “the potential for muni networks in disaster response is tremendous.”³⁷ At the time, the City’s municipal wireless network was only one quarter complete, but the collapsed bridge happened to be in the completed area. When the bridge fell, the Chief Executive Officer (CEO) of the network vendor for the citywide Wi-Fi network, USI Wireless, attempted to call the City to offer assistance but the cellular phone network was jammed. The CEO immediately opened the Wi-Fi network to the general public, allowing crucial channels of communication to remain open.³⁸ The contractor also rapidly installed wireless video cameras around the collapse site. The cameras, working in conjunction with GIS data sent to city crews via the network, proved invaluable in assisting the response.³⁹ These examples illustrate just some of the ways municipal broadband systems can vastly improve the effectiveness of video camera systems.

II.

PRIVACY CONCERNS OF MUNICIPAL BROADBAND APPLICATIONS

While municipal broadband applications have the potential for many beneficial uses, they also raise significant privacy and anonymity concerns. As video camera and wireless sensor networks evolve and there is increasing ability to combine information from various sources—perhaps automatically triggered by an interaction with an embedded wireless sensor device—one can imagine that a number of potentially chilling scenarios can arise. What if, for example, a cam-

36. Thomas J. Nestel, III, *Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse Be Prevented?* 63 (Mar. 2006) (unpublished Master’s thesis, Naval Postgraduate School), available at <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA445554&Location=U2&doc=GetTRDoc.pdf>.

37. CRAIG SETTLES, *WHEN CRISIS HITS THE FAN—MUNI WIRELESS TO THE RESCUE*, add. at 1 (2007), <http://www.successful.com/msp/reports.html> (follow “Snapshot addendum: Minneapolis network meets the challenge” hyperlink).

38. *Id.*

39. *Id.* at 1–2.

era system uses a facial recognition system to identify a person or group of persons milling about a train station or participating in a protest march, and automatically correlates that identification with data about his or her known associations? Or perhaps a wireless sensor system could detect an RFID chip in a driver's license as one approaches an advertising billboard, instantly referencing a database containing that person's electronic profile, including age, gender, income, and buying habits; the advertising billboard then addresses the person by name with a tailored advertising pitch. Many people might find such access to and use of personal information invasive, yet the value of such a system to an advertiser would be enormous and, in an era of cash-strapped public transportation and highway systems, it could be tempting for a government to cooperate in its deployment. This Part explores some of the privacy concerns raised by municipal broadband applications, particularly video surveillance and electronic profiling.

A. *Video Cameras, Privacy, and Anonymity*

According to the American Civil Liberties Union (ACLU) and other privacy advocates, the presence of video cameras presents a palpable example of the progress toward a "surveillance society."⁴⁰ Broadband-enabled video camera systems present a stark example of a potentially privacy-infringing municipal broadband application. While there certainly are valid privacy concerns surrounding the use of video cameras by government entities, few would dispute that a robust, full-motion video surveillance system is entirely appropriate and warranted in at least some cases.⁴¹

On the other hand, leaving aside the question of whether current laws establish an actionable right of privacy that can be used to restrict their deployment, it must be acknowledged that the ubiquitous presence of cameras looming over street corners and other public places would indeed be difficult for some to fathom, at least at the present. But, before making a determination about whether a camera on every

40. See, e.g., SCHLOSBERG & OZER, *supra* note 34, at 1.

41. For example, an extensive system of full-motion, real-time, full-color, human-controlled cameras surveys Morrow County, Oregon and its Hanford Nuclear Reservation and Umatilla Chemical Weapons Depot. Relying on a seven hundred square mile hybrid Wi-Fi/WiMAX network, the County's Emergency Management Center operates cameras that can be remotely controlled to turn and zoom in on specific critical areas. The camera system also monitors the area highway system and could help the County orchestrate a rapid evacuation in the event of a chemical disaster. CRAIG SETTLES, *WHEN CRISIS HITS THE FAN: MUNI-WIRELESS TO THE RESCUE* 13 (2007), available at <http://www.successful.com/msp/snapshot-5-07.pdf>.

street corner would or should be inevitable, it may be worthwhile to consider how the policies underlying the use of a video camera surveillance infrastructure might exacerbate or ameliorate the privacy concerns. In some instances, the privacy debate has resulted in somewhat arbitrary restrictions on video camera systems' use.⁴²

Policy concerns should be taken into account, for example, when considering broadening the access to video surveillance feeds. Future technology could enable all surveillance cameras to post live feeds on the Internet in real time, accessible to anyone who wishes to view them. With such a system, a suspicious spouse could pull up the feed of a camera to view the comings and goings of a particular drinking establishment or apartment complex, from the comfort of his or her own home. From a strictly legal perspective, it would be difficult to object to the use or deployment of this system: so long as the cameras only view public places, persons in their scope presumably have no reasonable expectation of privacy and no enforceable right to prohibit others from viewing them.⁴³ From a political and public policy perspective, though, proposing such a system would be questionable at the very least.

In a less drastic and more realistic scenario, video cameras may be widespread in public areas, but the general public cannot access the video feed. Rather, the camera feeds are presumably accessible only to certain government and law enforcement personnel, who may be viewing them in real time, possibly with complete control over a camera's direction and focus.⁴⁴ Under such circumstances, a strong inquiry based on privacy and anonymity concerns would be appropriate. There may be no clear, enforceable policies regarding the use of the images, including who may access them and for how long they are archived. Public records laws may or may not allow general public access to recorded images upon request.⁴⁵ Without adequate safeguards, real-time, human-viewable controllable cameras present potential for abuse beyond mere voyeuristic abuses of controllable

42. "San Francisco's cameras aren't monitored in real time, as they are in many other places—and thus can't be turned or zoomed to take a close look at a suspect. Police are barred from watching live footage from Newsom's 70 city cameras in order to satisfy privacy advocates; officers can request tapes only after a crime is reported." Demian Bulwa & Matthew B. Stannard, *Is It Worth the Cost?*, S.F. CHRON., Aug. 17, 2007, at A1.

43. See *infra* Part III.A–B (analyzing the limits of the protections of the Fourth Amendment and discussing the applicability of federal electronic privacy statutes to municipal broadband networks).

44. See generally Nestel, *supra* note 36, at 27–44 (describing several different police camera systems in the United States).

45. See *infra* Part III.C.3.

cameras. The potential for the harassment of citizens and the improper release of images, for example, are real threats to the integrity of video surveillance systems and to organizations that use them.

B. Profiling Through Database Combinations

Privacy concerns also may arise with the possibility of creating and using electronic profiles of persons, perhaps in real time. As broadband connectivity becomes pervasive, distributed data sources can be linked together in various ways. The ability to do so increases the value of the network, enabling users—government personnel, citizens, and devices—to acquire not only information directly experienced (such as a video image of a face or the chemical signal of a biological agent), but also additional knowledge that provides valuable context (such as whether the face corresponds to that of a person on the FBI Most Wanted List, or a person in the market for Nike athletic shoes).

Such tools are already being used by government entities.⁴⁶ In London, for example, counterterrorism specialists use a camera system and automated number plate recognition (ANPR) software to analyze the license plate of every vehicle entering the city.⁴⁷ In the United States, the REAL ID Act of 2005 requires that state-issued driver licenses and identification cards comply with Department of Homeland Security mandates relating to digital readability and biometric identification and requires the standardization of databases in federal and state computer systems.⁴⁸ Further, a government entity or a private entity could potentially operate a network that delivers targeted advertising based on known information about the user. A proposed part of EarthLink's financing of a free municipal network in San Francisco was Google's ability to tailor its advertisements based on a user's location in the city.⁴⁹

46. Non-government entities, particularly advertisers, also use database combinations and profiling extensively. "Project Canoe" is an emerging example of such in the cable television industry. See Todd Spangler, *Project Canoe Not a Joint Venture*, MULTICHANNEL NEWS, Mar. 10, 2008, <http://www.multichannel.com/article/CA6539950.html>.

47. Nestel, *supra* note 36, at 63.

48. Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 6 C.F.R. § 37 (2008).

49. EARTHLINK MUN. NETWORKS & GOOGLE, SAN FRANCISCO TECHCONNECT COMMUNITY WIRELESS BROADBAND INITIATIVE 15 (2006), available at http://www.sf.gov.org/site/uploadedfiles/dtis/tech_connect/EarthLink_SanFrancisco_RFP_2005-19_PUBLIC.pdf.

The prospect of combining various data sources with surveillance tools, such as video cameras and wireless sensors, may present a threat to conventional notions of privacy.⁵⁰ At the same time, such tools may substantially increase the value and improve the effectiveness of many municipal systems, particularly those focused on security-related objectives. Apparently, the technological means exist—or soon will—to identify, locate, and learn a striking amount of information about virtually anyone. But the theoretical possibility of doing so does not necessarily mean that potentially beneficial tools and applications should not be used. Municipalities can easily implement policies and procedures that would adequately protect the privacy of their citizens. Part IV of this Article will suggest some such policies, but first, Part III will discuss relevant legal principles already in place at federal, state, and local levels.

III.

BALANCING PRIVACY: EXISTING LEGAL TOOLS

Part I highlighted several beneficial aspects of various municipal broadband applications, and Part II explored some of the associated privacy concerns. This Part examines existing legal tools available to effectively address privacy concerns while allowing beneficial applications to reach their full potential. The provisions of privacy law most often turned to include the Fourth Amendment, federal statutes such as the Electronic Communications Privacy Act, and the patchwork of state constitutions and statutes.

A. *Privacy Guarantees of the Fourth Amendment*⁵¹

The protection against unreasonable searches and seizures in the Fourth Amendment of the U.S. Constitution is, historically, the most obvious federal safeguard against invasive conduct by government entities.⁵² However, it proves to be of limited utility with regard to the

50. See, e.g., SCHLOSBERG & OZER, *supra* note 34, at 5.

51. Given all the potential ways a government could employ video camera systems or other municipal broadband applications, a number of constitutional considerations could conceivably come into play. For example, if a camera system were used to intentionally discriminate against a suspect class of persons, the Equal Protection Clause might be invoked. Or if it were found to chill freedom of speech or of association, First Amendment questions would be raised. However, this Article focuses its discussion on the constitutional provision most directly implicated by government use of municipal broadband applications: the Fourth Amendment.

52. The Fourth Amendment provides the following guarantee: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

core issues discussed in this Article, particularly video surveillance. While the Supreme Court held in *Griswold v. Connecticut* that a right to privacy is implicit in the First, Third, Fourth, Fifth, and Ninth Amendments,⁵³ two years later in *Katz v. United States* the Court clarified that the Fourth Amendment does not confer a general constitutional “right to privacy.”⁵⁴ The Fourth Amendment “protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.”⁵⁵ Furthermore, while some provisions of the Constitution protect privacy from other types of governmental invasion, “the protection of a person’s *general* right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.”⁵⁶

Katz and subsequent case law interpreting the Fourth Amendment’s prohibition against unreasonable searches and seizures has produced the doctrine that no protection against a government “search” is afforded unless the subject possesses a “reasonable expectation of privacy.”⁵⁷ Whether an expectation of privacy is “reasonable” involves both a subjective and objective inquiry: did the person invoking Fourth Amendment protection have an actual expectation of privacy, and would society agree that the individual’s actual belief was in fact reasonable?⁵⁸ *Katz* also established the proposition that a person’s right to privacy does not depend entirely on where he or she may be: “the Fourth Amendment protects people, not places.”⁵⁹ A person can be in a public place and still have a reasonable expectation that some aspects of his or her life are not open to public inspection. In *Katz*, the Court held that a person standing in a public phone booth may reasonably expect to conduct a private phone conversation, but the reasonable expectation of privacy would not extend to the fact that the person was in the phone booth nor to the physical identification of the person,

probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.

53. *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

54. *Katz v. United States*, 389 U.S. 347, 350 (1967).

55. *Id.*

56. *Id.* at 350–51.

57. *See, e.g., Rakas v. Illinois*, 439 U.S. 128, 148 (1978) (holding that petitioners had no “legitimate expectation of privacy” in “the glove compartment or area under the seat of a car in which they were merely passengers”); *Smith v. Maryland*, 442 U.S. 735, 741–43 (1979) (holding that no reasonable expectation of privacy exists for phone numbers dialed from a person’s phone).

58. *Smith*, 442 U.S. at 740.

59. *Katz*, 389 U.S. at 351.

because “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”⁶⁰

Since *Katz*, case law interpreting the Fourth Amendment’s prohibition against unreasonable searches and seizures has resulted in the general assumption that no reasonable expectation of privacy exists regarding conduct occurring in a public place.⁶¹ Accordingly, the use of video cameras to monitor a public area, for example, would not be a “search” under the Fourth Amendment. The same principle generally is true with regard to physical facts observable from public places, assuming that there is no reasonable expectation that facts exposed to the public will remain private, even if the subject has taken steps to restrict the public’s view.⁶² However, in 2001, the Supreme Court articulated its concern that new technologies may be used to circumvent the Fourth Amendment and held that the use of a thermal imaging device to view, from a public vantage point, heat signatures inside a home was an impermissible search for which a warrant was required.⁶³ Yet, the Court proceeded to imply in dictum that using a device “in general public use” to see inside a home might not be a search if the government only views what a naked eye might discern through a window.⁶⁴

Given the current Supreme Court doctrine, it is difficult to see how the Fourth Amendment would be an effective tool to stave off a surveillance society presented by the municipal broadband applications, particularly video surveillance and wireless sensor networks, discussed in this Article. Because there is no reasonable expectation of privacy on a public street, the mere fact of a camera looming over every street corner would not violate the Fourth Amendment. And if a camera was deemed a device “in general public use” or analogous to

60. *Id.*

61. *See* *United States v. Knotts*, 460 U.S. 276, 281–82, 285 (1983) (holding that the use of a radio transmitter to track an automobile on public streets is neither a “search” nor a “seizure” under the Fourth Amendment because a person does not have a reasonable expectation of privacy regarding movements on public streets and highways).

62. *See* *California v. Ciraolo*, 476 U.S. 207, 209, 213–14 (1986) (holding that the Fourth Amendment does not require police to obtain a warrant before making observations from an airplane, traveling one thousand feet off the ground in public airspace, into a private backyard surrounded by a ten foot tall fence); *Florida v. Riley*, 488 U.S. 445, 450–51 (1989) (holding that police in a helicopter four hundred feet off the ground do not need a warrant to observe into a person’s greenhouse because there is no reasonable expectation of privacy where the sides and roof of a greenhouse are partially open); *Dow Chemical Co. v. United States*, 476 U.S. 227, 234–39 (1986) (holding that the aerial observations from navigable airspace of an industrial complex is not a search prohibited by the Fourth Amendment).

63. *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

64. *Id.*

what could be seen with the naked eye, there might not even be a Fourth Amendment protection against a government camera peering inside a home. As surveillance becomes increasingly ubiquitous, people may be less likely to have a reasonable expectation of privacy; however, it is difficult to accurately predict how the doctrine will be applied in a world of evolving technological sophistication. Lastly, attempting to address the difficult and competing concerns surrounding municipal broadband applications through Supreme Court interpretations of the Fourth Amendment seems to be a needlessly inflexible and unpredictable approach for municipalities who are seeking to deploy innovative and controversial technologies.

B. Federal Statutory Law

There are numerous federal statutes that pertain to electronic privacy,⁶⁵ but only a few provide means to address the privacy concerns raised in this Article. Of most immediate relevance to this discussion are the federal Wiretap Act⁶⁶ and the Stored Communications Act.⁶⁷

The Wiretap Act establishes the procedures and standards⁶⁸ for obtaining the necessary warrants to conduct “electronic surveillance.”⁶⁹ However, the language of the Wiretap Act does not specifi-

65. These include but are not limited to the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); the Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified as amended in scattered sections of 47 U.S.C.) (establishing privacy safeguards for cable television); the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in scattered sections of 47 U.S.C.) (establishing privacy safeguards for telecommunications customers); the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.) (establishing a special subpoena power enabling identification of alleged copyright infringers); the Privacy Act of 1974, 5 U.S.C. § 552a (creating record keeping rules for the federal government); the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C.) (imposing a duty on telecommunications carriers to cooperate with the government for law enforcement purposes); the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.); and the Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified in pertinent part, as amended, at 50 U.S.C. §§ 1801–1811 (2006)) (authorizing electronic surveillance for foreign intelligence purposes).

66. Wiretap Act, 18 U.S.C.A. §§ 2510–2522 (West 2000 & Supp. 2008).

67. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2001 & Supp. 2007).

68. Wiretap Act §§ 2516, 2518.

69. For purposes of the Wiretap Act, the term “electronic surveillance” is defined, in relevant part, as “the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a

cally mention video surveillance, prompting four Circuit Courts of Appeals to hold that, while video surveillance may in some instances implicate the Fourth Amendment and require a warrant, it is not itself regulated by the Wiretap Act.⁷⁰ The Ninth Circuit, on the other hand, has held that video surveillance—more precisely, video surveillance for which a warrant is required—is regulated by the Wiretap Act.⁷¹ Either way, the Wiretap Act would seem to have little bearing on the use of CCTV systems in public places by local governments, because, as noted in Part III.A, the use of cameras in public places is generally unlikely to require a warrant under the Fourth Amendment. Therefore, even in the Ninth Circuit, video surveillance seemingly would not fall within the definition of “electronic surveillance” applicable to the Wiretap Act’s warrant procedures. But, while the Wiretap Act likely does not apply to CCTV visual images, the Act’s general prohibition against the non-consensual interception of electronic, wire, or oral communication, should prevent both government and private CCTV systems from monitoring aural conversations as a matter of course.⁷²

The Stored Communications Act addresses the disposition of user records and content maintained by providers of a “electronic communication service”⁷³ or “remote computing service.”⁷⁴ In the context of municipal broadband applications and services, the Stored Communications Act most readily applies to those entities that go beyond using broadband solely for government services by offering free or subscription-based services. A citywide Wi-Fi service provider that makes service available to the public, as a provider of “electronic

reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(f)(4) (West 2003 & Supp. 2008) (defining “electronic surveillance”); Wiretap Act § 2511(2)(f) (authorizing the conducting of “electronic surveillance” exclusively under the procedures of the Wiretap Act and FISA, and indicating that “electronic surveillance” is defined according to 50 U.S.C. § 1801).

70. *United States v. Mesa-Rincon*, 911 F.2d 1433, 1436–38 (10th Cir. 1990); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504, 508 (2d Cir. 1986); *United States v. Torres*, 751 F.2d 875, 885–86 (7th Cir. 1984).

71. *United States v. Koyomejian*, 946 F.2d 1450, 1454 (9th Cir. 1991) (“[T]he legislative history provides ample evidence that Congress intended through Title III to provide strict regulation of *all* highly intrusive forms of surveillance.”)

72. Wiretap Act § 2511.

73. “Electronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” Wiretap Act § 2510(15); Stored Communications Act, 18 U.S.C. § 2711(1) (2001 & Supp. 2007) (adopting the definitions of § 2510 of the Wiretap Act).

74. Stored Communications Act § 2711(2).

communication service,” would be subject to the same privacy obligations under the Stored Communications Act as any private provider of such services. For example, a municipal broadband provider could not “knowingly divulge a record or other information pertaining to a subscriber or customer of such service,”⁷⁵ subject to a variety of exceptions.⁷⁶

Federal statutory law provides a basic level of privacy protection; however, like constitutional jurisprudence, it is not sufficiently flexible to regulate municipal wireless applications while enabling them to develop.

C. State Law

Virtually all states have various provisions that may be relevant to a privacy debate concerning municipal broadband applications. However, state privacy laws and regulations are not consistent among states⁷⁷ and are often described as a “patchwork.”⁷⁸ Some are very general, while others directly address some of the applications discussed in this Article, including Internet Service Providers (ISP),⁷⁹ video camera systems,⁸⁰ and RFID usage.⁸¹ This Section examines the varying privacy provisions in state constitutions, privacy statutes,

75. Stored Communications Act § 2702(a)(3).

76. Among these exceptions are the consent of the user, Stored Communications Act § 2702(b)(3), and as otherwise authorized by a warrant, court order, or other sufficient instrument pursuant to a law enforcement investigation, Stored Communications Act § 2702(b)(2).

77. See generally Electronic Privacy Information Center, Privacy Laws by State, <http://epic.org/privacy/consumer/states.html> (last visited Aug. 4, 2008) (summarizing the topics covered by each of the state privacy laws).

78. Kristin Gallina Lovejoy, *Beyond the Patchwork of Privacy Regulations*, NEWSFACTOR.COM, Dec. 8, 2005, http://www.newsfactor.com/story.xhtml?story_id=39958; Sandra Swanson, *State Internet Laws: Help or Hindrance to Privacy Efforts?*, INFORMATIONWEEK, Apr. 11, 2002, http://www.informationweek.com/news/security/privacy/showArticle.jhtml;jsessionid=KOSJWM03B2C52QSNLPSKH0CJUNN2JVN?articleID=6502088&_requestid=289166.

79. Minnesota and Nevada require Internet Service Providers to keep private certain customer information, unless the customer authorizes its disclosure. MINN. STAT. ANN. § 325M.01–09 (West 2008); NEV. REV. STAT. § 205.498 (2007). Laws of this type go beyond the federal Stored Communications Act, which specifically permits ISPs to share customer record information with any party, so long as the party is not a “government entity.” Stored Communications Act § 2702(c)(6). This begs the question, what if the ISP is a government entity?

80. Twenty-one states have some form of photo or video surveillance law. National Conference of State Legislatures, Electronic Surveillance Laws, <http://www.ncsl.org/programs/lis/cip/surveillance.htm> (last visited Aug. 4, 2008).

81. CAL. CIV. CODE § 52.7 (West 2008) (prohibiting coerced or compelled subcutaneous implantation of RFID devices); 2008 Wash. Legis. Serv. ch. 138 (West) (prohibiting the intentional remote scanning of another person’s RFID device, without

and sunshine laws, and concludes that the most effective and flexible way to immediately address the concerns of privacy advocates is through state and local sunshine and privacy laws.

1. *State Constitutions*

According to the National Conference of State Legislatures, ten states contain some form of explicit privacy protection within their state constitutions.⁸² In California, for example, voters in 1972 approved an amendment to the state constitution that included a right to privacy within the “inalienable rights” of all people.⁸³ The Supreme Court of California noted that part of the motivation for passing the privacy amendment was the fear of “government snooping” and the looming ability, with computerization, to create “cradle-to-grave profiles” of citizens.⁸⁴ However, California courts have produced a privacy test that is arguably more difficult to satisfy than that called for by the Fourth Amendment. To find a violation of California’s constitutional privacy clause, courts must make a preliminary finding of “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct . . . constituting a serious invasion of that privacy.”⁸⁵ Once that preliminary finding is made, the court then applies a balancing test, weighing the value of the conduct in question against the severity of the intrusion.⁸⁶ Even though California is arguably the most aggressive state in terms of statutory privacy protections,⁸⁷ it is not at all clear how or whether California’s constitutional privacy provision provides the means to

that person’s prior knowledge or consent, for an illegal purpose, such as fraud or identity theft).

82. National Conference of State Legislatures, *Privacy Protections in State Constitutions*, <http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm> (last visited Aug. 4, 2008). The ten states are: Alaska, ALASKA CONST. art. I, § 22; Arizona, ARIZ. CONST. art. II, § 8; California, CAL. CONST. art. I, § 1; Florida, FLA. CONST. art. I, §§ 12, 23; Hawaii, HAW. CONST. art. I, §§ 6–7; Illinois, ILL. CONST. art. I, §§ 6, 12; Louisiana, LA. CONST. art. I, § 5; Montana, MONT. CONST. art. II, § 10; South Carolina, S.C. CONST. art. I, § 10; and Washington, WASH. CONST. art. I, § 7.

83. CAL. CONST. art. I, § 1; *White v. Davis*, 533 P.2d 222, 233 (Cal. 1975).

84. *White*, 533 P.2d at 233.

85. *Hill v. Nat’l Collegiate Athletic Ass’n*, 865 P.2d 633, 657 (Cal. 1994).

86. *Loder v. City of Glendale*, 927 P.2d 1200, 1230–31 (Cal. 1997).

87. California has enacted more than forty different privacy laws since 1999, and was the first in the nation to have an agency specifically dedicated to promoting and protecting the privacy rights of consumers. Joanne McNabb, *Stitching Together the Legislative Patchwork*, TRUSTE, http://www.truste.org/articles/legislative_patch.php (last visited Aug. 4, 2008); California Office of Privacy Protection, *Welcome to the Office of Privacy Protection*, http://www.oispp.ca.gov/consumer_privacy/default.asp (last visited Aug. 4, 2008).

reasonably address the privacy issues raised in this Article, while permitting the reasonable development and deployment of the technology. The same is true of the other nine states that have constitutional provisions explicitly addressing privacy, the terms of which, naturally, are very general. Case law interpreting state constitutional privacy clauses provides very little, if any, specific guidance for those considering the implementation of privacy-sensitive municipal broadband applications.

2. *State Privacy Acts*

Virtually all states have statutory provisions that impose duties on state government agencies and political subdivisions with regard to the collection, maintenance, accuracy, use, and disclosure of personal information. In some states, the laws are part of an overarching statutory scheme analogous to the federal Privacy Act of 1974⁸⁸ and address the government's use of "personal information" or "personal records," while other states attend to such issues in piecemeal fashion with context-specific laws, such as ones that focus on the government's use of tax and school records and regulatory filings.

Existing state privacy laws of this type could play an important role as governments employ increasingly powerful means of gathering, compiling, and using information about its citizens. To the extent a municipal broadband system or application uses or produces a qualifying "personal record" under such statutes, the municipality may have an obligation to clearly inform citizens of its practices. However, even when states have privacy statutes, many questions remain. For example, is a new "record" created—and thus subject to disclosure under sunshine laws—every time a particular application (a video facial recognition system, perhaps) compiles information from various databases? Is this "personal information" protected under the state privacy laws? Questions such as these are ripe for consideration, and state privacy laws may function as a starting point from which local governments must address privacy concerns.

3. *Sunshine Laws*

In addition to federal and state privacy guarantees, most state agencies and local governments are subject to state and local open meeting laws and open records laws—sometimes collectively referred to as "sunshine laws"—that are designed to ensure government transparency. Open meeting laws impose an obligation to make poli-

88. Privacy Act of 1974, 5 U.S.C. § 552a.

cymaking activities open and available to the public, subject to certain exceptions. Open records laws, some of which are based on the federal Freedom of Information Act (FOIA)⁸⁹ (and many of which predate it) generally permit persons to access records and writings produced and maintained by government entities. Sunshine laws vary substantially among localities. For example, Vermont, Florida and Ohio strongly favor openness and access, while Pennsylvania and Washington, D.C. have much more restrictive policies for access to records and meetings.⁹⁰

The state sunshine laws vary widely in how they define a “meeting,” “public record,” or “public writing” that is subject to openness. Many states statutorily define what constitutes a “meeting,”⁹¹ and requirements often include such factors as the presence of a minimum number of government policymakers, whether the meeting is solely of an advisory group, whether the purpose of the meeting is “fact-finding” or “policymaking,” and whether “informal sessions or conferences” are covered. Similarly, some states’ open record laws define “public records” or “public writings” quite broadly to include even drafts and memorializations of conversations.⁹² Records can take many different forms, including electronic versions such as email.⁹³ In most states, the requester need not be a citizen of the state to invoke a records production.⁹⁴

While sunshine laws can ensure accountability and create confidence in the process and procedures adopted,⁹⁵ these general “good

89. Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2006 & Supp. 2008).

90. THE REPORTERS COMM. FOR FREEDOM OF THE PRESS, *Introduction to OPEN GOVERNMENT GUIDE* (Gregg Leslie & Corinna Zarek eds, 5th ed. 2006), available at <http://www.rcfp.org/ogg/item.php?pg=intro>.

91. See, e.g., ALASKA STAT. § 44.62.310(h)(2) (2006); CAL. GOV'T CODE § 11122.5 (West 2005).

92. See, e.g., ALASKA STAT. § 40.25.220(3).

93. See, e.g., TEX. GOV'T CODE ANN. § 552.002 (Vernon 2004); W. VA. CODE § 29B-1-2(4) to (5) (LexisNexis 2002); MASS. GEN. LAWS ANN. ch. 4, § 7 (West 2006); KAN. STAT. ANN. 45-217(f). See generally OPEN GOVERNMENT GUIDE, *supra* note 90.

94. Among states that *do* require requesters to be citizens of the state are Alabama, ALA. CODE § 36-12-40 (LexisNexis 2001); Arkansas, ARK. CODE ANN. § 25-19-105(a)(1) (2002); and Georgia, GA. CODE ANN. § 50-18-70(b) (2006).

95. The City of San Francisco is considering an amendment to the City's sunshine ordinance that would employ advancements in video and Internet technology to provide “complete transparency” of government functions. Under the new law, live audio and video streaming of public meetings held at City Hall would be posted on the Internet within seventy-two hours and would be archived for two years. Joshua Sabatini, *Smile, City Government, You're on Webcast Camera*, EXAMINER.COM, Apr. 4, 2008, http://www.examiner.com/a-1320069~Smile_city_government_you_re_on_webcast_camera.html.

government” statutes also present potential privacy concerns in the context of municipal broadband applications. For example, open records laws in some states, where the definition of “public record” is broadly defined and includes electronic records, could potentially enable a private citizen (including a corporation) to obtain information about, or produced by, a municipal broadband application or surveillance system, such as a stored video feed from a surveillance camera. Under the California Public Records Act, for instance, video camera content may be accessible to district attorneys.⁹⁶ On the other hand, some states have sought to protect this information. For example, the Philadelphia Parking Authority “successfully convinced [the] state legislature to create a statute protecting video images from release.”⁹⁷

Local and state sunshine laws exist precisely to ensure that government functions are reasonably transparent and accessible to the public, and that the government may be held accountable by the public. Similarly, privacy concerns relating to municipal broadband applications (and non-municipal broadband applications, for that matter) tend to disappear so long as the entity operating the system is subject to sufficient obligations relating to transparency and accountability. Accordingly, for municipal broadband projects in particular, local and state sunshine laws can play an important role in ensuring public confidence in the system. Governments should not only ensure that they remain compliant with existing sunshine laws as they consider proposed broadband applications, they should also consider how and whether such laws might need to be amended to reasonably balance the sometimes-competing tensions between privacy, openness, and government effectiveness.

IV.

POLICY CONSIDERATIONS

In Part III, this Article suggested that current federal and state privacy guarantees are not the most effective means of addressing the potential power imbalance that some privacy advocates fear could lead to a “surveillance society.” Section A of this Part will argue that the best solution is for local governments to tailor policies that effectively deploy municipal broadband applications while protecting the privacy of its citizens. Section B concludes with policy recommendations to address the unique privacy concerns presented by municipal broadband applications.

96. CAL. GOV'T CODE §§ 6262–6263.

97. Nestel, *supra* note 36, at 66–67.

A. *Local Governments Are Better Positioned to Develop Effective Protections and Build Public Confidence and Support*

As Part III demonstrated, the provisions of privacy law most often turned to, including the Fourth Amendment and federal statutory law, like the Electronic Communications Privacy Act, do not adequately address the privacy concerns related to the desire to use technology to revolutionize government services.⁹⁸ Indeed, the Supreme Court has stated that “the protection of a person’s *general* right to privacy . . . is . . . left largely to the law of the individual States.”⁹⁹ While the patchwork of state constitutions and statutes provide more flexibility than federal law, they still have significant problems.¹⁰⁰ Instead, complex issues of municipal wireless infrastructure and the use of information are best addressed at the local level. Local governments may well be the most effective entity to manage potentially sensitive privacy issues, because they provide the most accessible venue for public input into the deliberative process; they can adopt policies and procedures that work for their particularized environment; and their citizens can more easily hold local governments accountable than either state or federal governments.

Furthermore, the future use of innovative and beneficial municipal broadband applications will depend on maintaining public support for them. The best way to maintain public support and confidence over the long term is to adopt thorough, well-reasoned policies *at the local level* that address the privacy concerns that stem from the use of such applications. Local open meeting laws enable citizens to directly participate in the formulation of policies, and open record laws could empower citizens and advocates to restrain overreach by local governments. Lastly, municipalities can and should invite privacy advocacy organizations and the public at large to participate in the debate.

B. *Formal Policy Recommendations to Govern the Use of Municipal Broadband Applications*

Consistent with the open deliberation, transparent decision-making, and accountability of local sunshine laws, citizens and local government policymakers should insist on the adoption of formal policies and procedures governing the deployment and operation of major municipal broadband applications. One set of often-cited, privacy-centric recommendations concerning electronic information systems in gen-

98. See *supra* Part III.A–B.

99. *Katz v. United States*, 389 U.S. 347, 350–51 (1967).

100. See *supra* Part III.C.

eral is the Code of Fair Information Practices, initially drafted in the 1970s by the U.S. Department of Health, Education and Welfare.¹⁰¹ The Code sets forth the following five principles:

There must be no personal data record keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for an individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.¹⁰²

In short, the five points of the Code provide a good basis for aggressively evaluating the privacy implications of proposed broadband applications and systems.

Take, for example, video camera systems. According to one estimate, seventy percent of municipal jurisdictions with video camera systems in the United States do not have any policies or regulations concerning their use, and many of the places that do have polices do not punish violations of them.¹⁰³ However, in light of the five points listed above, it is possible to design a policy for a video camera system that addresses most potential privacy and anonymity objections up

101. Electronic Privacy Information Center, The Code of Fair Information Practices, http://epic.org/privacy/consumer/code_fair_info.html (last visited Aug. 18, 2008).

102. U.S. DEP'T OF HEALTH, EDUC. AND WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *available at* <http://aspe.hhs.gov/DATACNCL/1973privacy/tocpreface/members.htm> (follow "Summary and Recommendations" hyperlink).

103. Chris Slobogin, Steven C. O'Connell Chair, Frederick G. Levin Coll. of Law, Univ. of Fla., Public Workshop CCTV: Developing Privacy Best Practices, Remarks at the Department of Homeland Security Privacy Office 6 (Dec. 18, 2007) (transcript available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Legal_and_Policy_Perspectives_Panel.pdf). While U.S. municipalities have failed to develop adequate policies for video surveillance, advisory boards and governments in other countries have. In 2000, the British Data Commissioner produced a "CCTV Code of Practice," with "data protection rules for the gathering, storage and protection of CCTV images." Every system was required to register with the government by 2003. Nestel, *supra* note 36, at 17. In the United States, guidelines for video surveillance systems have been issued by the American Bar Association and the Commission on Accreditation for Law Enforcement Agencies (CALEA). *Id.* at 21-22.

front. Such a policy would include the mandate that the use of information obtained by a municipal camera system be restricted: camera images would not be viewable in real-time by a human being, except by law enforcement as part of ongoing criminal investigations, in instances involving immediate danger, or for specific pre-designated purposes, such as traffic management cameras. All real-time views by humans (even if routed to a particular police cruiser) could be automatically logged, tracked, or flagged, and such logs could be made open to public inspection upon request. If camera images are recorded, retrieval of those images from an archive could be restricted only to law enforcement in the above scenarios or to a private party who obtains a court order, and would also be tracked appropriately.¹⁰⁴ Violations would result in punishment. Audio should not be recorded. The purposes for which the video images are used would be made known to the public. There may be a periodic compliance audit. If these or other similar restrictions were established, publicized,¹⁰⁵ and enforced, the general public might be more amenable to the prospect of ubiquitous video surveillance cameras, or at least relatively limited systems.

Many of the same underlying principles may hold true for the deployment of other systems, such as those involving wireless sensors or a combination of data sources, for which the public may harbor a sense of invasiveness. For example, an entity deploying a public broadband Internet access service that is supported by location-based or behavioral advertising should adopt and publicize exactly what user data is collected, how it is collected, with whom it may be shared, and how long it is maintained.

In addition to the general principles suggested by the Code of Fair Information Practices, local governments might consider some other practical policy approaches. These include appointing a point person, board or committee responsible for safeguarding privacy principles; adopting basic principles or codes of conduct applicable to all users and for all uses of the network; reviewing applicable open records laws and identifying areas of potential change, as suggested in Part III.C; and assessing families of applications making use of the municipal broadband network. For each type of application used in

104. As discussed in Part III, local and state government officials should be mindful of privacy issues presented by public records laws. Amendments to such laws may be necessary to ensure that the burgeoning volume of electronic data about the public is accessible to the public upon reasonable terms.

105. To educate the public about the policy restrictions on the use of information collected from municipal cameras, information could be posted, for example, on a small sign under every camera.

conjunction with a municipal broadband network, local governments should identify technical capabilities and requirements, the expense and efficiencies related to the applications, and the role of contractors, if any, in providing the municipal broadband application. More importantly, governments should address how the information they collect is used, by adopting written, enforceable policies and procedures concerning the type of information gathered; the purpose for which information is gathered; whether information is “personal” or “sensitive” in nature; how information is reviewed, such as in real-time, by a person or computer; what form the information takes, such as audio, video, or data; and how long information is retained. Governments must ensure sufficient recourse to enforce these policies, by providing citizens with the ability to verify compliance, permitting periodic privacy audits, and allowing civil or criminal action for violations by city personnel, if necessary.

These policy recommendations will help ensure that the privacy of citizens is respected, and will permit governments to have maximum flexibility in the use of their municipal broadband for governmental functions. Providing privacy-sensitive safeguards at every step, and making known what those safeguards are, will ensure transparency, accountability, and continued public support for municipal broadband applications.

CONCLUSION

George Orwell’s *Nineteen Eighty-Four* provides an extreme example of the privacy implications of government surveillance. At a fundamental level, *Nineteen Eighty-Four* explores the imbalance of power between an individual, who has no meaningful recourse, and a “Big Brother” state, Oceania, which has complete control over the individual’s life. Many privacy advocates raise the specter of a “Big Brother” surveillance society as an inexorable result of the technological means to do so. While technology enables a government like the omniscient, totalitarian government of Oceania to utterly invade the privacy of its citizens, as discussed in Part II, it also can enable dramatic advances in government efficiency, accountability, public safety, and citizen interaction, as outlined in Part I. Local governments in particular have an important role to play in addressing the tension between citizen privacy concerns and beneficial technology-enabled services of the sort discussed in this Article and should adopt well-considered policies ensuring accountability and transparency for the use of such tools. In Oceania, after all, there were no sunshine laws.