INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION



Work Session: Monday, October 29th -- NCC 209-210

Title: Contract, Regulate or Be Regulated: New Technology Contracts and New Roles for Local Governments

by

Presenter: Gail A. Karish

Presenter's Title: Attorney

Presenter's Office: Miller & Van Eaton, P.L.L.C.

© 2007 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2007 Annual Conference, held October 28-31, 2007 in Nashville, Tennessee. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Contract, Regulate or Be Regulated:
New Technology Contracts and New Roles for Local Governments

Local governments have long been vital participants in the development and expansion of communications infrastructure. They participate in a wide variety of ways. They own or control access to public rights-of-way where the bulk of communications infrastructure is deployed. Some operate their own institutional networks for internal government, emergency responders, educational, and community service uses. Others, who found their citizens were underserved by the private sector, built their own systems to offer "commercial" services such as broadband.

In recent years, there has been a proliferation of new communications technologies and new business opportunities. Some – like municipal Wi-Fi – have gained a lot of attention ---good and bad---in the national press. All of them bring new opportunities and new challenges for local governments.

This paper has two purposes. First, it describes some of the key legal considerations that should accompany the review of any new communications infrastructure project. Second, it offers some practical advice on how to ensure that legal issues do not become an impediment to the successful development of communications infrastructure.

Key Legal Considerations

A. Contract Structure Issues

A first point to consider is that the new communications technology contracts can be structured in an infinite variety of ways, depending on the technology to be deployed, the type of service being offered, the role/contribution of the local government, and the wishes of the parties involved.

Often the project will require the simultaneous preparation of multiple contracts to cover all the different legal arrangements being entered into. For example, our firm has represented several cities in the negotiation of WiFi projects with Earthlink. The Houston project involved the negotiation of a variety of documents including the following:

- Wireless Broadband Network License Agreement – permitting Earthlink to build out its system in the City and provide WiFi service.
- Site Master License Agreement – covering the terms and conditions for use of specific City property for installation of the system.
- Service Level Agreement – defining the minimum standards for the WiFi service offering.
- Wireless Service Agreement – providing WiFi services to the City as anchor tenant for the project.

As this brief description indicates, in this project the local government took on a number of roles – from regulator to lessor to subscriber – all concurrently, and each with its own complex set of legal issues to consider.

B. Federal Law Issues

Beyond the standard contract review considerations, when evaluating new communications technology projects, it is important to bear in mind that there are various federal laws that might apply that the local government may not have had to consider previously. Some of the most important ones are discussed below.

1. Communications Assistance for Law Enforcement Act of 1994 (CALEA)

CALEA is an example of a law enforcement program that has grown exponentially in scope with the growth of new communications technologies. As a result, it can apply to a wide variety of communications networks and functions.

In 1994, Congress enacted CALEA "to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities." [1] In 2004, at the urging of the Justice Department, the FCC issued a Notice of Proposed Rulemaking ("NPRM") to consider extending CALEA to new communications technologies. The FCC issued two orders as a result of that proceeding -- one in which it concluded that all broadband Internet access services and interconnected VoIP services were covered by CALEA. *First CALEA Order* at ¶ 8, and a second which addressed issues related to the implementation of the new requirements. Second Report and Order and Memorandum Opinion and Order, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, FCC 06-56, released May 12, 2006) ("*Second CALEA Order*").

The first question you might ask yourself is – does this legislation apply to facilities owned or used by my local government? As with most legal issues, the two ends of the spectrum are clear, but the vast middle is subject to considerable uncertainty. The definition of "telecommunication carrier" in the legislation is different than that found in the Communications Act, and the FCC's definition varies from both. Nonetheless, it is clear that CALEA applies to traditional telephone companies and other

[1] First Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, FCC 05-153, ¶ 4, released Sept. 23. 2005 ("*First CALEA Order").*

entities that offer telecommunications services to the public.[2] At the other end of the spectrum it is also clear that purely private networks are to be exempt.[3]

The difficulty is in determining whether networks that do not fit squarely in one or the other category must comply with CALEA. The answer can turn on subtle differences in the network architecture. Not only should existing government networks be evaluated. As new technology projects are presented, the potential CALEA implications of those projects must be considered carefully.

For example, based simply on a plain reading of the term "private network," it would seem that the exemption ought to apply to an I-Net, because I-Nets are internal communications networks used by the government entity for its own purposes and, unlike the networks operated by telecommunications and cable companies, they generally do not offer service to the public. The *First CALEA Order* completely excludes private networks (except to the extent they are interconnected, as discussed below), but does not define them.

The only written guidance the FCC has offered is the following statement, referring to certain education, library and research networks, which allow members to communicate with each other and retrieve information from shared databases, and which are not open to the public:

> We therefore make clear that providers of these networks are not included as "telecommunications carriers" under the SRP with respect to these networks. To the extent, however, that these private networks are interconnected with a public network, either the PSTN or the Internet, providers of the facilities that support the connection of the private network to a public network are subject to CALEA under the SRP.

First CALEA Order, ¶ 36, fn 100. This statement leaves open the status of I-Nets that provide additional or different functionalities, such as access to the Internet for library patrons, or VoIP-based voice communications for government employees. The statement also does not clarify what the FCC believes is meant by "support the connection of the private network to a public network."

---

[2] *Communications Assistance for Law Enforcement Act*, Second Report and Order, 15 F.C.C.R. 7105 (2000) at 7110, ¶ 9. In the *First CALEA Order* the agency noted further that "to the extent that any facilities-based broadband Internet access service provider chooses to offer such service on a common carrier basis, that provider is subject to CALEA pursuant to section 102(8)(A), the Common Carrier Provision." *First CALEA Order* ¶ 24.

[3] Section 1002(b)(2)(B), which excludes from the requirements of Section 1002(a): "equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers."

In its brief in *American Council on Education v. FCC*, 451 F.3d 226 (D.C. Cir. 2006), the FCC stated that:

> The best reading of the statute is that the interconnection point between the private network and the public network must be CALEA-compliant because at that connection point the network ceases to be private. At the same time, Petitioners are wrong to read the *Order* as requiring any private network that connects to the Internet to comply with CALEA even as to its private components. What the Commission determined was that a private network connecting to the Internet must comply with CALEA at that connection point, and that connection point alone.

In other words, if a law enforcement agency can obtain access to transmissions over the I-Net at its point of interconnection with the Internet, either through facilities controlled by the County, or facilities controlled by a third party, this may be sufficient.

Recent conversations between our office and the FCC staff suggest that the FCC's position is that if an entity provides a connection to the Internet, *even if the actual connection to the Internet is provided by a third party carrier*, the entity is subject to CALEA if it engages in any routing or soft-switching on its side of the connection.

Answering the question correctly – for existing networks and new projects – is not just a theoretical exercise; it can have serious financial implications. If CALEA applies, the network architecture must take into account CALEA capability requirements (to enable the law enforcement surveillance). Compliance can be expensive even if incorporated into the original plan; having to retrofit compliance would generate added costs. In addition, non-compliance can lead to fines and civil penalties of up to $10,000 per day. *See* 47 C.F.R. § 200008, 47 C.F.R. § 1.80, 47 U.S.C. § 503(b)(2)(C).

2. Wireless Projects -- Over-the-Air-Reception-Devices (OTARD) Rules & Radio Frequency Interference (RFI) Regulation

For wireless projects, or projects with wireless components, special attention should be paid to two areas of FCC regulation---OTARD and RFI.

The FCC's Over-the-Air Reception Devices ("OTARD") Rule, 47 C.F.R. § 1.4000 preempts local zoning that limits the placement on private property of not only direct broadcast satellite antennas, but also of fixed wireless facilities which include Wi-Fi antennas. The rule applies to facilities installed on property under the "exclusive use or control" of the antenna user, including leased property. In addition, the rule may also apply to preempt an agreement between the local government and the wireless provider, to the extent that the local government has granted the provider the exclusive right to use space on poles or rooftops. Agreements must be carefully drafted to guard against preemption. For example, the wireless provider should waive the application of OTARD and should explicitly state that no exclusive rights are being granted.

Radio Frequency Interference (RFI) poses another set of potential compliance and liability issues, as well as public safety concerns. Generally unlicensed frequencies are used for Wi-Fi networks. These networks may interfere with other unlicensed networks, including the local government's existing public safety systems, and they may also interfere with FCC licensed users. An FCC licensed user may seek redress from the FCC if it experiences harmful interference from others. However, unlicensed users do not have the same FCC protection. In addition to determining who will bear responsibility for interference claims, the local government should insist on a contractual mechanism for resolving these disputes.

Practical Considerations

1. *Perform specialized legal review early on* in project planning, and most definitely in advance of issuing a request for proposals. Instead of reacting to proposals brought by the private sector, get ahead of the issues. Know what you can and can't do legally and what types of legal risks you would and would not be willing to take on. Are you missing out on opportunities to maximize the value of your existing communications infrastructure assets? Does your infrastructure planning consider legal issues in its risk/reward analysis? Legal uncertainty and complexity should not cause local governments to pass on projects. But without a clear understanding of the potential legal issues at stake in a project, it is impossible to make an accurate evaluation of its attractiveness or to negotiate a deal that adequately protects the community from the downside risks, while allowing residents to enjoy the benefits of new communications technologies.

2. *Be sure to continuously monitor legal developments*. The law is playing catch-up with the new technologies and the new opportunities for local governments. Constant monitoring of the Federal Communications Commission, your state Public Service Commission, Congress, and state legislatures is imperative.