wiley

NEWSLETTER

Smart Cities: A Look at Risks and Opportunities for Technology Companies

February 2017

Government Contracts Issue Update

Smart Cities transformation is one of the next major municipal infrastructure investments. The federal government's grant investments in Smart Cities technologies will create dynamic opportunities for both emerging and established technology companies. But companies need to enter this market with their eyes open, and consider the unique compliance obligations that come with federal grant funding. This article explores just a few of the unique privacy concerns and contract-related compliance issues that companies developing and deploying Smart Cities technologies could face, which may be foreign to commercial technology companies who do not have experience performing work under public contracts or grants, and which highlight the need for a multi-disciplinary approach and counsel.

What is a Smart City?

A "Smart City" employs information and communications technology to enhance its livability, workability, and sustainability. Smart Cities is a facet of the "Internet of Things," a ubiquitous interconnected network of computing devices, software, smart sensors, and "big data" analytics. According to the Smart Cities Council, "in simplest terms, there are three parts to that job: collecting, communicating and crunching." First, interconnected devices and sensors are used to collect information. Next, that information is communicated in real time using wired or wireless networks. Third, the Smart City "crunches" or analyzes that data to understand what's happening now and what's likely to happen next.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

George E. Petel
Partner
202.719.3759
gpetel@wiley.law

Practice Areas

Government Contracts

Privacy, Cyber & Data Governance

Examples of Smart City solutions are already being proposed. Smart meters can measure utilities usage for planning and maintenance purposes. Smart traffic sensors can report road conditions and traffic congestion to direct traffic control resources, snow plowing, and first responders where they are needed. Smart GPS gear can pinpoint the exact locations of the city's buses and develop metrics to optimize routes based on demand, or to enable greater tactical visibility for police and firefighting activities. In addition to these types of sensors, citizens' mobile devices can be used to collect data on population movements, positions, speeds, where people gather at different times of the day, and the environmental conditions around them. All of this data can be used to more readily target local challenges and improve city services.

In September 2015, the Obama Administration announced its "Smart Cities" initiative, including federal research grants for Smart Cities solutions to municipal problems. Federal agencies including the Departments of Transportation and Homeland Security have announced grant programs focused on Smart Cities. The federal effort is designed to promote research and development via collaborative "test beds." Meanwhile, state and local governments have begun exploring the possibilities of existing and emerging Smart Cities solutions. Although there has been a great deal of effort and excitement on the technical aspects of Smart Cities, including a National Institute of Standards and Technology (NIST) International Technical Working Group on IoT-Enabled Smart City Framework, little attention has been paid to the legal implications for both cities and solution-providers.

Companies Supporting Smart Cities May Confront Unique Privacy Issues

There are many unique issues a Smart City project will face. One is privacy. Collecting and analyzing vast amounts of data is at the heart of Smart Cities, and companies should be aware of the unique privacy issues and obligations that may be implicated. To understand these privacy concerns, Smart City providers can look to the experiences of technology companies, like Google, Apple, and Facebook, who have faced a host of privacy challenges over the past decade based on their collection and use of personal data through social media, email services, and smart phones. Privacy concerns exist—and may be amplified—in the context of Smart Cities. Cities and service providers may have access to, handle and manage a variety of data: some truly aggregated and de-identified, some personally-identifiable, and some in a gray area.

For example, many Smart City solutions rely on location monitoring. In order for a Smart City solution to direct you to the last free parking space near your doctor's office, for example, it will need to know where you are and where you are headed. While nothing prohibits the Government or any private individual from observing people in public, analysis of continuous location monitoring data over a longer period of time can reveal private patterns: where people live and work, who their friends are, what medical issues they face, or what their hobbies may be, for example. Courts and regulators like the Federal Trade Commission (FTC) have become increasingly sensitive to the privacy implications of continuous location monitoring technology that will be central to Smart City solutions. Current user consent models may be tested by novel and ubiquitous deployments that depend on location information and interact with devices and users.

Future Smart City models may push boundaries. Smart Cities are designed to facilitate communication in a given area by increasing connectivity between city government, devices, and people on the street. There could easily expand to include local businesses. For example, a future Smart City could detect a user in a particular area at a certain time (like the lunch hour) and send content to that user's smart phone about specials at the sandwich shop on the corner. Facilitating that communication may implicate certain privacy laws and the FTC's sensibilities.

Social media companies that have collected and used user data have often addressed these privacy concerns by obtaining the consent of their users at the same time users opt in to the application or service. Consent in a Smart City environment may not be as straightforward, however, since the environment will be more dynamic and a person walking down the street may not have any direct or solicited interaction with particular entities' websites or apps—be it traffic light operations assessing foot traffic, a parking lot operator alerting drivers to nearby spots, or a business that seeks to interact with nearby potential patrons. Creative thinking will be needed if a Smart City solution wants to obtain consent to enable interactive communications and the offering of services.

There are also privacy implications for how law enforcement will be able to access data collected by Smart Cities to solve crime and protect national security. Smart Cities may have the capability, for example, to use facial recognition software and location monitoring to track in real time a robbery suspect as he flees or to passively monitor people in a given area in order to look for fugitives. These sorts of scenarios are far from fanciful. But they raise hard questions that companies need to consider, and which current municipal and state managers may not be ready to address.

Who will "own" data collected in Smart City deployments? Will cities have the capability to set appropriate policies and expectations for contractors, vendors, and users? How will companies manage and store information they process and collect? How will they respond to law enforcement requests to collect this data? And what assurances will companies provide to the public about the safeguarding of their data? These questions are at the cutting edge of how we interact with our government in an era of increasingly powerful technology. Resolution may be driven by, or influence, contractual vehicles and compliance challenges.

Companies Using Federal Funds to Develop and Deploy Smart Cities Technologies Face Unique Compliance Risks

Government contracting at the federal, state, and local level involves competing in a regulated marketplace and creates compliance obligations and potential liabilities that generally do not exist in the commercial technology marketplace. The source of Smart Cities' funding—often federal grants administered by state and local governments, who in turn typically issue contracts using those funds—establishes regulatory and contractual obligations that will require companies to establish appropriate compliance mechanisms. These compliance programs should be tailored to the size of the company, the scope of the company's government business, and the specifics of the contractual or grant requirements.

Many state and local governments model their procurement processes on the federal marketplace, although there are nuances and distinctions among the states. Some state and local governments have highly developed procurement processes and policies, while others rely on generalized statutory authority, internal agency guidelines, and the courts. Companies interested in selling Smart Cities technology and solutions must be aware of these processes and policies and how they may differ from one state or locality to the next. There will likely be significant differences between the business development and capture process in the state and local government market versus the commercial marketplace for technologies, which can include limits on customer communication and interaction; price justification and audits; unique intellectual property rules; and potential criminalization of business disputes. Contractors will also likely have to navigate socioeconomic requirements that require contractors to utilize small and historically disadvantaged companies to perform a material portion of the work; and, under some state and municipal rules, contractors may need to utilize local companies.

During performance, a contractor's costs may be subject to audit pursuant to guidelines in the Uniform Grant Guidance that governs federal grant funds. Such an audit can result in a recovery of costs by the Government if the contractor's costs are found to be unreasonable, unallowable, or insufficiently supported.

With regard to intellectual property, contractors must diligently protect their intellectual property rights in technical data and computer software, and this will be a unique concern in a technology-driven field like Smart Cities development. Under the federal rules, contractors must comply with stringent mandatory markings or risk losing some of those rights to the Government. Many states lack robust regulations or guidance in this area, and contractors need to protect themselves through careful contract negotiations, including diligent reviews of both solicitations and contract documents.

Lastly, and perhaps most importantly, Smart Cities contractors need to be aware of the threat of the criminalization of contract disputes with the Government. State and local governments across the county have adopted false claims act laws, many modeled off the federal Act, and have begun applying those laws to government procurement (traditionally states focused on the healthcare industry). Adopting the federal government's increased use of the False Claims Act and False Statements Act to fight purported contractor fraud and collect large judgements for the Treasury, there is always the risk that business disputes arising from differing interpretations of contract requirements or contract negotiation tactics may generate either or both criminal and civil investigations and steep monetary penalties. Even if the outcome is ultimately favorable to the contractor, investigations are inherently negative and unpleasant and are often very costly to defend.

Conclusion

Providing Smart Cities solutions to governments can have many benefits. Special socio-economic preferences afford opportunities to new and small business contractors that do not exist in the commercial marketplace and the comfort of dealing with a generally reliable customer. But there also exist many potential pitfalls that do not generally exist in the commercial realm, including the Government's right to terminate the contract at its convenience and the possible criminalization of business disputes. Partnering with the Government in cutting edge, complex endeavors like Smart Cities will be exciting and challenging. It will present novel issues,

such as the foregoing privacy and security challenges, some of which add layers to already-complex commercial relationships. In sum, while there are many promising opportunities in contracting with the Government, a company must do its homework to ensure that it knows, and complies with, the myriad unique rules that apply in this environment.