MAYER | BROWN

Contracting for Facilities Management Services in the Proptech Era

By Marina G. Aronchik

Technology is transforming the way companies use, manage and maintain their real estate portfolios. Shopping centers are leveraging big data and developing cloud solutions and applications to attract the next generation of shoppers and transforming their ordinary mall visit into an "experience." Large companies are increasingly seeking to monitor, on a real- or close to real-time basis, their facility occupancy rates and optimize their real estate portfolios, based on the analysis of such data. Facilities management providers are implementing and relying on sensors and predictive analytics to detect and remediate issues faster than they could in the past.

Facilities management agreements and related transactions need to reflect the growing transformational role of technology and the risks that technology creates. This article discusses issues in four key areas that clients with real estate portfolios need to consider and negotiate with providers in today's technology-laden facility management deals: data and related compliance obligations, intellectual property rights, new risks and liabilities, post-termination rights and termination charges.

Data Rights and Related Compliance Obligations

DOES THE CLIENT HAVE THE RIGHT TO COLLECT THE DATA IT WANTS?

Technology that is being used to collect data includes cameras, various sensors (water/humidity, heat, smoke, etc.), microphones and badge scanners, to name a few. Cameras, as an example, can be wired or wireless, can be placed in plain view or so small so as to be undetectable. Cameras can be used for security purposes, or, if coupled with facial recognition, they can be used to assist with facility utilization assessments. Thermal imaging cameras can make it easier to identify failing motors or other electrical components, HVAC leaks, deficient ductwork, or leaking roofs. Although we can see significant potential value flowing from the use of cameras within facilities, that does not mean that they can be deployed anywhere and that the information gathered by those cameras can be used for any purpose. This is particularly true when cameras and sensors are gathering data that may be associated with individuals, whether directly or indirectly. For example, sensors that are monitoring the operation of certain equipment may also be providing incidental information about the equipment operator—was the equipment idle at a time when the operator was supposed to be working? Individual privacy rights and laws

must be considered when collecting data through use of technology that is intended to help with facilities management, particularly where individual data collection is not the intended (and approved) use. (See *International Developments in Privacy Laws and Vendor Agreements* on page 27.)

DOES THE CLIENT HAVE THE RIGHT TO PROVIDE DATA (EITHER COLLECTED OR LICENSED FROM A THIRD PARTY) TO THE FACILITIES MANAGEMENT PROVIDER USING THE TECHNOLOGY AT ISSUE?

It is not uncommon for clients to have outsourced different functions to different providers who would benefit from sharing of the data. For example, the facilities management provider could be more effective if it could access data collected by the desktop support provider to determine when and where employees are logged into their computers. Whether that data can be used by the facilities management provider will have to be determined by reviewing the contract between the client and the desktop support provider (and as discussed in the paragraph above, there may be privacy issues to consider). The client may believe that this information belongs to it, but if it did not preserve ownership in that data in the desktop support agreement, it may not have the right to make that information available to its facility management provider.

ARE THERE OTHER LIMITATIONS ON COLLECTING FACILITIES-RELATED DATA?

There are laws in virtually every jurisdiction applicable to the collection and use of personal data. There are various state laws in the United States as well as the existing EU Data Privacy Directive that will be replaced in May 2018 by the more comprehensive and punitive GDPR. Clients need to ensure that their data collection, storage, transmission and usage practices are compliant with all legal requirements as missteps today can be significant public relations issues and costly problems to correct. A client operating in Europe might need to get the assistance of the supplier of technology to conduct a Data Protection Impact Assessment if it is required by the GDPR. There may be significant differences in implementation and compliance costs where data is being transferred internationally or stored in the cloud and this will be an area which will need careful consideration in light of the nature of the data being collected and analyzed. These data issues are not always top of mind in real estate and facilities deals, but they should not be afterthoughts.

Intellectual Property Rights

OWNERSHIP OF INTELLECTUAL PROPERTY

When people think about facility management and maintenance, they traditionally think about snowplows, tools, cleaning carts and cafeterias; they are not typically thinking about intellectual property. Facility maintenance providers may use procedure and maintenance manuals drafted by the provider. These manuals may be important to ongoing facility management functions. Today, some forward-thinking companies are using augmented reality/virtual reality (AR/VR) in place of procedure manuals. A real world example is the use of smart glasses by a maintenance worker to complete complicated assembly processes ensuring that all parts are assembled in the right order without the need to consult hardcopy manuals or other handheld devices. Programming for the collection of data from installed sensors may be similarly important. As technology becomes more complex, the need for documentation regarding not only operation of the facilities but also operation of the technology being used to operate the facilities becomes more important. Whether the client is using hardcopy procedure manuals prepared for it by the provider or

smart glasses to accomplish the same task, the client must give careful thought to the ownership or license rights of intellectual property and other information associated with these solutions so that the client may seamlessly continue services when the contract with the provider ends.

LICENSE OF INTELLECTUAL PROPERTY

As discussed above, the client may be using a number of providers to deliver services. It may be necessary or desirable for a provider to use technology owned or otherwise provided by a third party engaged by the client, or vice versa. In either situation, license rights flowing from one party to the other will be necessary in this situation. As with other technology licensing agreements, clients would be well served to include licensing permissions and use rights for the entire ecosystem of the client's providers who may need to use third-party licensed technology to assist the client in maintaining or managing its facilities and property.

New Risks and Liabilities

The use of technology to provide facility management services can create new risks and potential liabilities for clients.

SECURITY CONCERNS

As devices become connected, security concerns grow. Although there are a number of security issues that we could address, we will focus on two: (i) increasing access points to a client's network and (ii) proprietary systems running on these devices. Years ago, thermostats were mechanical devices (not connected) that controlled heating and cooling in defined areas. Today, many thermostats are connected to a network in addition to the heating and cooling system. This connection to the network is another access point for a hacker. When you add up all of the thermostats in all of the facilities that are networked, those thermostats could constitute hundreds if not thousands of opportunities for hackers to gain access to the client's network. The sheer number of additional network access points that the networked thermostats create results in significant monitoring and intrusion detection challenges for IT administrators.

A SECOND SECURITY ISSUE IS PROPRIETARY SYSTEMS RUNNING ON CONNECTED DEVICES

When it comes to deploying computers into a company's environment, it is not uncommon for there to be approved software images that are loaded onto approved hardware that have been tested as secure configurations that are supported by the company. Many connected products such as sensors and networked thermostats, use proprietary systems that provide little or no ability for customization or security enhancements. In these situations, clients need to balance the productivity improvements and efficiency gains against the security risks associated with using the technology.

DATA AND SECURITY BREACHES

Clients need to recognize that the risk of data and security breaches by facility maintenance providers is as significant, and the consequences as harmful to the client's business, as any other data or security breaches. From published reports about third-party providers who caused or enabled significant data breaches, no third-party provider is immune from the potential to create a security vulnerability or incident.

LIABILITY CONCERNS ASSOCIATED WITH THE USE OF AUTONOMOUS SOLUTIONS

There is still a lot of uncertainty, both under applicable laws and with respect to a "market standard" for contractual provisions, over how liability will be apportioned for autonomous solutions if property is damaged or people are injured. Over time, the law will likely develop in

this area providing more guidance with respect to specific technology (e.g., self driving vehicles used in connection with facility management services). (*See How Smart, Connected Products Are Transforming Business* on page 49.) In the meantime, we expect these issues to be subject to extensive negotiation by the parties, with a range of possible outcomes and compromises depending on a number of factors, including the technology at issue and specific risks (and risk-mitigation strategies) involved.

Post-termination Rights and Licenses and Termination Charges

POST-TERMINATION RIGHTS AND LICENSES

As discussed above, even simple written documents created by the provider can be intellectual property. If the client desires to use third-party or provider-owned software or technology that is used by the provider in the provision of the services, then the client will need post-term license rights to continue to use such software or other IP. If the provider has deployed sensors to detect water leaks, do the sensors stay with the client when the contract ends? Does the software used to monitor the sensors stay with the client? The client should understand the entire landscape of intellectual property used by the provider and the exit strategy that works for the client, including post term license rights where applicable.

TERMINATION CHARGES

Absent some sort of investment by the provider, there typically are no termination charges in facility management contracts. A provider's investment in technology may result in the provider insisting on an early termination fee to help it recoup any stranded costs associated with that investment. If a provider is making such an investment, then those costs should be documented in the contract along with a clear mechanism for calculating any resulting termination fee should the customer terminate the contract early.

Conclusion

Technology is creating significant opportunities for cost savings, process efficiencies, safety enhancements and improved workplace morale. Technology is entwined with data, intellectual property, privacy, and security issues, and continued use of technology (including information about how to operate the technology) may be critical to the continued provision of facilities management services. These issues should be considered and addressed when technology is deployed in a facilities management outsourcing deal or by property owners or managers.