Return-To-Work Tech Brings New Contract Issues

By **William Tanenbaum**


William Tanenbaum

This article outlines the key legal terms to include in agreements to use technology to comply with coronavirus-related return-to-work regulations, such as in the following scenario: A company retains a vendor to provide an app that enables self-screening and then "talks" to turnstiles that allow or prevent office entry.

The company may need to retain multiple vendors to automate as much of COVID-19 compliance as it desires. A company can be an employer or tenant that directly contracts with one or more vendors, or it can be a landlord or building management company that contracts with vendors to provide COVID-19 services to tenants.

Contracts should look beyond the return-to-work period because COVID-19 compliance can accelerate the use of technology and data to improve business operations and reduce costs in ways that will be useful after a vaccine is available.

As a simple example, ceiling-mounted sensors to monitor social distancing can also be used to automate room-specific heating, cooling and lighting, and to provide data for the redesign of corporate office space. Data is an asset that is transforming business, and coronavirus-related technology will collect new sources of data for this transformation. It will enable data analytics that generate proprietary insights for internal use or external monetization.

While much of coronavirus-related regulatory compliance can be automated, the agreements must allow for a human loop. For example, an individual's answers to the screening app's questions may fall in a middle ground, where a medical professional must determine whether medical symptoms indicate the likelihood of a COVID-19 infection or another medical condition that does not pose a danger to the workplace.

This human determination must be fed back into the technology system. It is foreseeable that artificial intelligence will be used to make an assessment or provide information to assist the medical professionals.

The key legal terms addressed below draw on information technology outsourcing, business-process outsourcing, intellectual property management, and so-called internet of things agreements.

Requests for Proposals

It is important to involve the right people from the right company departments in drafting requests for proposals and evaluating vendor responses. In addition to the IT department, the company should involve those responsible for COVID-19 compliance: human resources, facilities management, network security — often the chief information security officer — and data use and analytics — often the chief data officer — because the data generated by technology will be an important resource for COVID-19 and non-COVID-19 uses.

Request for proposals often assign different weights to different factors. This weighting should be determined with care. If the request for proposals assigns 5% out of 100% to

security, then vendors will conclude that security is not a priority and may not provide the information security that the company anticipates. Further, to reduce the time from start to finish of the agreement, it is useful to have the request for proposals' sections map directly to the relevant sections in the agreement.

Proof of Concept

Companies should establish acceptance criteria and require a proof-of-concept phase to test the operation of technology with a trial group before deploying it companywide.

When multiple vendors with different technologies are to provide the technology services to the company, this phase should confirm the ability of technologies from different vendors to work together, and identify any weak links that need improvement. The right combination of a correction phase and the company's right to terminate should be drafted ahead of time.

Service Levels

The service levels each vendor must meet should be set out with specificity in the agreement or the statements of work. In the case of a screening app, the agreement should include a defined time period for the app to provide a cleared, not-cleared or further-medical-assessment-needed status. The time period should be a short period, defined in minutes, from the time the app is opened and ending when the app completes its function.

Because you get what you measure, an illustrative service level agreement, or SLA, would be that the app will provide the accurate status for x number of simultaneous users within y minutes 99.95% of the time. Depending on the circumstances, the time for the medical professional to provide an assessment can be included in this SLA or excluded from it and subject to its own SLA.

Vendors will want SLAs to be contingent upon the company meeting certain requirements, such as providing fast and stable internet access. See the discussion in the "Bring-Your-Own-Device" section below.

Precontract due diligence should confirm that the vendor technology has the capability to handle the number of the company's employees or other users, as well as the aggregate number of those from all of vendor's customers. During the term of the contract, this capability will be rolled up and captured by the SLA discussed above.

A company's remedy for the vendor's failure to meet the SLA is generally the issuance of service credits in dollar amounts tied to the frequency and degree to which the vendor failed to meet the SLA. Determining the service credits, caps, earn-backs and other factors is often subject to intense contract negotiation based on business needs and the capabilities of the technologies.

Another service level is setting the maximum time for the vendor to begin cure of a deficiency in meeting the performance SLA. Different time periods are often used for different severity levels determined by the impact on the business.

Privacy

Vendors should represent, warrant and covenant that they will meet governing laws on privacy and data retention. With respect to personal health information, there may be requirements to delete such information within a short period of time after a screening

session is completed.

Different jurisdictional requirements must be met. For example, New York City has privacy laws that are in addition to and more stringent than New York State law.

Companies will want vendors to provide indemnities against administrative fines and sanctions, and other damages. The caps on and exclusions from indemnification obligations are areas that are likely to be subject to careful negotiation.

Intellectual Property and Combinations Under Indemnification Obligations

New intellectual property rights may arise from the parties' collaborative creation of improved technology. It is advisable for the parties to allocate ownership and license rights by contract because the default rules under the statutes may give rise to unanticipated adverse business results. While joint ownership has business appeal, it can lead to situations where either party can license the jointly developed IP to the other party's competitors.

IP infringement indemnifications often contain exclusions when the vendor's products or services are used in combination with third-party products or services. These exceptions should not cover combinations that are necessary and are contemplated.

For example, screening apps must be used on mobile devices and work with other products and services. For combinations that cannot be specified, the mere fact of a combination should not waive indemnification.

Exclusion can be appropriate where the combination gives rise to infringement but where the vendor's product or service alone would not. A contested area arises when the vendor wants indemnification from the company where the company demands that the vendor use specific products outside of the usual technology ecosystem.

Data as Confidential Information

A company may consider data that is not personally identifiable information to constitute confidential information that is not to be used or disclosed by the vendor. For example, the number of employees working in a specific laboratory may be reverse engineered by a competitor to determine what research and development a company is conducting, and the products that may result.

Data Commercialization

An important issue in allocating rights in the contract is the prohibition of use or the scope of permitted use by a vendor of aggregated data derived from its customers. In some cases, a company may permit certain commercialization in exchange for a lower price. In other cases, a company may not want the vendor to monetize the data collected by the vendor in providing services to the company.

A related issue is whether such customer data can be used by third parties as training data for machine learning. As between the parties, the company should own the data, and licensing is the vehicle to determine the scope of the vendor's rights in data.

Bring-Your-Own-Device Policies

Companies should review and update their policies covering smart phones and similar devices when apps and other technologies are used for COVID-19 regulation compliance and to meet the company's obligations to its vendors. Companies will require employees to use, and avoid compromising, the screening and other apps on which the company relies for COVID-19 compliance

Force Majeure and Disaster Recovery

Vendors should have disaster recovery and business continuity plans in place to allow them to perform during foreseeable events otherwise leading to interruptions in service. The agreement should provide that if an event constitutes both a force majeure event and an event covered by the disaster recovery or business continuity plan, the disaster recovery or business continuity plan will control.

Conclusion

The contract provisions discussed above address key risks faced by companies when retaining vendors to use automation to comply with COVID-19 return-to-work regulations. In addition to having technology that operates according to contractual requirements, data will be increasingly important to companies inside and outside of the return-to-work context, including the role it plays in AI and machine learning.

William A. Tanenbaum is a partner at Moses & Singer LLP.