COVINGTON

Return to Workplace Considerations for Businesses Using AI and IoT Technologies

June 10, 2020

Artificial Intelligence and Internet of Things

The COVID-19 pandemic is accelerating the digital transition and the adoption of artificial intelligence ("AI") tools and Internet of Things ("IoT") devices in many areas of society. While there has been significant focus on leveraging this technology to fight the pandemic, the technology also will have broader and longer-term benefits. As the *New York Times* has explained, "social-distancing directives, which are likely to continue in some form after the crisis subsides, could prompt more industries to accelerate their use of automation."

For businesses proceeding with reopenings over the coming weeks and months, and for sectors that have continued to operate, AI and IoT technologies can greatly improve the way they manage their operations, safely engage with customers, and protect employees during the COVID-19 crisis and beyond. But businesses also should take steps to ensure that their use of AI and IoT technologies complies with the evolving legal requirements that can vary based on several factors, including the industry sector where the technology is deployed and the jurisdiction where it is used. Businesses also will want to have mechanisms in place to help ensure that the technology is used appropriately, including appropriate oversight and workforce training and other measures.

How Businesses are Using AI and IoT in Response to the COVID-19 Crisis

Businesses may want to leverage AI and IoT technologies to support their operations in a number of ways. In connection with reopenings, as discussed previously in this series, many businesses will deploy AI and IoT technologies to protect the health and safety of their employees. New and existing tools are being used for health monitoring, remote interactions, and "contactless" access and security. For example, some businesses are instituting return-to-workplace policies that require temperature scanning or other monitoring of health indicators through wearable AI (i.e., wearable IoT devices powered by AI). Businesses also may use AI and IoT technologies to automate office tasks to enable some employees to continue working from home, to conduct meetings and trainings remotely, or to facilitate social distancing in the workplace by, for example, relying on facial recognition technology in lieu of front-desk security personnel.

Beyond the initial reopening steps, manufacturers and other businesses are considering how expanded use of robotics and automation can increase efficiencies, improve workforce safety, and facilitate "contactless" transport and deliveries. Businesses increasingly also are using AI tools to help improve logistics and supply chain management, provide input for decision making, and to support customer engagement. In some cases, AI and IoT tools are developed by companies for their own use—but increasingly businesses are turning to cloud services providers and other third parties for many of these technologies and services.

Key Questions to Ask Before Deploying AI and IoT Solutions

When businesses are implementing AI and/or IoT technologies, such as robotics, wearable devices, AI supply chain management and human resources management tools, health monitoring equipment and other AI or internet-connected products or services, they should consider the existing and proposed legal obligations and the benefits and risks that may be introduced by use of these tools. Businesses should ask, for example:

- Does the use of this technology create any new benefits or risks to our operations, such as with respect to workplace or public safety, cybersecurity, or quality control? What are the impacts of those benefits and risks on the business and potentially affected individuals and entities? Have we taken appropriate steps to mitigate risks through documentation, contract, processes, oversight, training and insurance? Do the benefits justify the risks?

- Does the technology meet our needs? Is it sufficiently reliable? Can its operations be validated? To the extent relevant, have we considered the NHSX AI in healthcare checklist?

- Does the AI application or IoT device have reasonable security features given its nature and function, and the kind of information it collects, generates, processes or transmits? Are there appropriate response mechanisms in the event of an actual or suspected security breach?

- In the case of AI, what steps are being taken to foster AI trustworthiness (e.g., accuracy, safety, free from unintended bias, explainability, security, reliability and accountability)?

- If the use of the technology would involve monitoring the behavior, activities, or attributes of staff, have we considered applicable law and guidance relevant to staff monitoring? Could use of the technology result in any measures or decisions being taken that could raise concerns under applicable discrimination law?

- Have privacy and data protection obligations and risks, which differ by jurisdiction, been evaluated and managed? Will personal data be collected and used?

- How will we become aware of potential problems with the technology, and how will we respond to those problems? How will problems be prioritized and fixed?

- Have we taken appropriate steps to secure rights to use third party data and other third party proprietary rights and to protect our own data and proprietary rights?

- Are we complying with applicable trade control laws and other applicable laws?

- Do our contracts appropriately address the AI and IoT issues arising in connection with our acquisition, deployment and use of AI and IoT technologies or services? Have we undertaken appropriate due diligence with respect to our third party providers?

- Do we have mechanisms in place to identify and promptly respond to new legal AI and IoT legal developments, particularly given the evolving landscape described below?

- Is the technology solution subject to regulation by the FDA (see more detail below), given that FDA actively regulates some software as a medical device?

The AI/IoT Legal Landscape

Businesses must be mindful of the rapidly evolving legal landscape surrounding AI and IoT technology, and the potential need to comply with new requirements that may vary by industry or jurisdiction. On the AI front, earlier this year, the European Commission solicited comments on an artificial intelligence white paper that describes a proposed AI regulatory framework. The white paper embraces a risk-based and proportionate approach and acknowledges that high-risk AI applications should be regulated differently than lower-risk applications. Among other things, the European Commission white paper proposes a pre-market assessment requirement for “high risk” AI. The European Commission also has proposed changes to the AI liability laws. In the United States, President Trump signed an Executive Order on AI in February 2019, which calls for a coordinated federal AI strategy. In early 2020, the Trump Administration proposed 10 Principles for AI Regulation which takes a lighter touch approach to regulation than the European Commission white paper. Pursuant to the Executive Order, the National Institute of Standards and Technology has submitted a plan for developing AI standards. Meanwhile, in April the Federal Trade Commission provided guidance on the use of AI and algorithms in automated decision making. There also is a variety of pending AI legislation in Congress, and some state and local governments continue their efforts to examine regulation of AI. Several entities are also working to coordinate these types of efforts internationally. More information is available on our Artificial Intelligence Toolkit.

On the IoT side, while Congress is considering legislation, states are increasingly active as well. For example, both the California and Oregon IoT security laws came into effect in 2020. California is also currently considering a bill regarding trip mobility data collected from autonomous vehicles and other mobile applications. The bill would require the operators of autonomous vehicles to share aggregated and de-identified trip data for transportation planning and safety purposes, including in response to the COVID-19 pandemic. Standards continue to evolve outside the United States as well. For example, the United Kingdom has been active in providing guidance regarding the security of consumer IoT devices. In October 2018, the Department for Digital, Culture, Media and Sport, published a Code of Practice for Consumer IoT Security, and in March 2020, the National Cyber Security Centre issued guidance about using smart security cameras safely in the home.

Privacy and Security Concerns Presented by AI and IoT

Businesses should proactively manage privacy-related legal matters arising from the use of AI and IoT technologies. In order to function, many of these tools must collect significant amounts of personal data from individuals. For example, wearable AI devices that can be used for health monitoring may collect geolocation information, data about an individual’s physical movements, heartrate and blood pressure indicators, biometric information such as fingerprints and facial features, and other personal information. Some of these devices also may collect and store more data than they actually use, or retain data for lengthy periods of time. These devices, when used with AI, also may create new personal data about an individual, such as the likelihood an individual may experience severe COVID-19 symptoms based on pre-existing conditions.

Any solution that involves the collection, generation or use of personal information should have adequate privacy and data security safeguards in place. Businesses should have privacy policies in place and should comply with such policies as well as applicable law. Heightened privacy requirements may apply if the information being collected is particularly sensitive in nature. For example, the collection of biometric and health information may be subject to federal laws regulating the use of medical information, such as the Health Information Portability and Accountability Act ("HIPAA") or the Americans with Disabilities Act ("ADA"), and state laws regulating the collection of biometric information, such as the Illinois Biometric Information Privacy Act, or medical confidentiality. Similarly, automated technologies that record audio or video data could implicate state wiretap laws if that collection occurs without the consent of the individuals being recorded.

FDA Regulatory Issues

Some AI and IoT technologies are regulated by FDA. For example, digital health screening tools may ask employees about risks for exposure to COVID-19 (e.g., COVID-19 status of individuals in the employee's household, COVID-19 testing history, social distancing practices) or about the individual's symptoms (such as those identified by the U.S. Centers for Disease Control and Prevention ("CDC")). Some technologies may simply transmit that information to a medical professional for assessment, while other tools may utilize AI and IoT technologies to provide an assessment of the individual's exposure risk directly to the individual and/or the employer.

Depending on the functionality and intended use of the technology, it may be subject to regulation as a medical device. FDA generally does not regulate tools that match user-specific information (e.g., symptoms) to established reference information (e.g., CDC guidelines). Likewise, tools intended to help a patient document their health and communicate health information with a healthcare professional are not regulated as devices. On the other hand, FDA would likely regulate as a medical device an AI and IoT technology that provides patients recommendations on COVID-19 diagnosis if it does more than automate health authority guidelines.

While companies utilizing technologies developed by third parties will generally not be subject to FDA regulation, firms that develop their own technologies could be subject to regulation as a device manufacturer, depending on the functionality of the product. Companies developing tools, including those contracting out certain elements of the development, should carefully consider whether FDA or other regulators will actively regulate the technology.

Employee and Workforce Issues

Although some technology solutions are likely to be temporary, in many cases businesses are simply accelerating the adoption of permanent changes to how they operate. It is therefore important to consider the impact that these technologies may have on the workforce in both the immediate and long term.

Automation and robotics can protect employees from virus-related health dangers, but they may require their own safety precautions. While the Department of Labor's Occupational Safety and Health Administration ("OSHA") has not issued regulations on the use of robotics in the workplace, it has issued guidance explaining how existing workplace safety regulations can affect robotics and a guide for best practices regarding robotics safety. These guidelines explain how to think about worker training, hazard assessment, and safeguarding the workplace in the context of workplace robotics. In the future, workplace health and safety is an area that is likely to be subject to additional regulation relating to AI and robotics, and businesses should pay close attention to those developments as they evolve.

Employers also should be mindful of the need for workforce training. To help ensure that AI and IoT are deployed properly, employees may need to be trained on its use. For example, businesses using health monitoring systems in connection with returning to the workplace may need to train some personnel on the proper use of such systems. In addition, as businesses continue with their digital transitions, they may need to devote more employee attention to data management, and they may be better able to optimize employee time.

Of course, businesses should also keep in mind broader employment law concerns when implementing AI and IoT technology solutions, including potential issues related to bias, medical confidentiality, recordkeeping, employee monitoring, wage and hour requirements, protections for legal off-duty conduct, and labor law protections.

For more information, we invite you to visit our new **Covington Artificial Intelligence Toolkit** and our **Internet of Things website**.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our AI, IoT, Medical Device, and Employment teams:

Jennifer Johnson	+1 202 662 5552	jjohnson@cov.com
Lee Tiedrich	+1 202 662 5403	ltiedrich@cov.com
Scott Danzis	+1 202 662 5209	sdanzis@cov.com
Carolyn Rashby	+1 415 591 7095	crashby@cov.com
Danielle Kehl	+1 415 591 7076	dkehl@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.