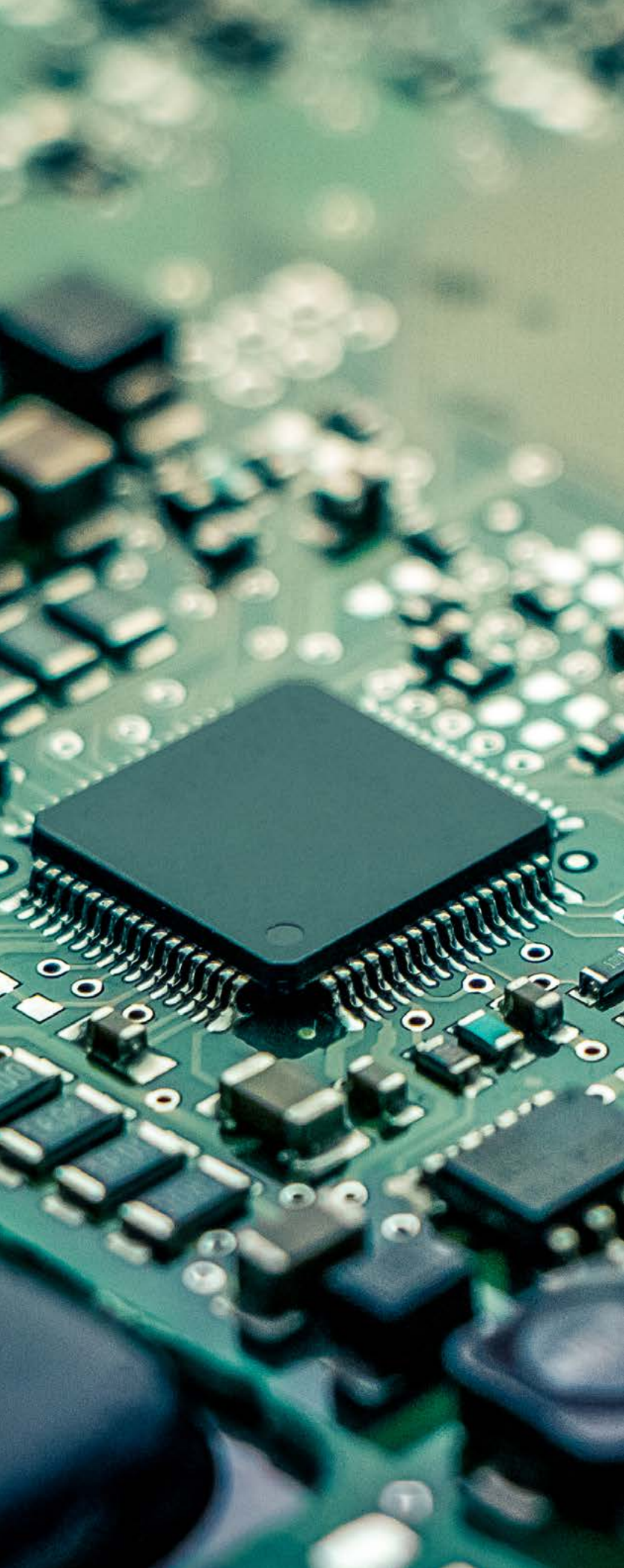




Aerospace & Defense Insights

New technologies come with new litigation risks

Christopher Pickens



Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

Aerospace, defense, and government services (ADG) companies increasingly rely on advanced and interconnected technologies for a wide variety of business-critical efforts. For instance, companies may incorporate Internet of Things (IoT) technology into production lines as well as inventory and fleet management tools, and they may utilize machine learning to develop autonomous drones, autonomous vehicles, or cybersecurity products. As ADG companies increasingly rely on technology to drive their growth, they must also prepare for the litigation risks these technologies present.

Technology-related litigation risk may grow out of cybersecurity vulnerabilities, technology failures, partnerships with technology companies, and alleged biases embedded in AI and machine learning systems. Yet, a recent Hogan Lovells [survey](#) of 550 businesses¹ indicates many companies have not taken steps to examine and mitigate these risks. Of those surveyed, 76% reported they are moderately or very concerned about potential investigations and/or litigation risk that could follow failure of a technology. However, only 46% reported they have done everything they can to mitigate this risk. An even smaller percentage (40%) reported that the C-suite is actively involved in mitigating the regulatory and litigation risk posed by a potential technology failure.

In the following, we examine a few of the key technology-related litigation risks for ADG companies and outline steps companies can take to mitigate them.

1. The survey, entitled "How to prevail when technology fails," is based on 550 interviews with general counsels, data privacy officers, or equivalent of some of the world's largest multinational companies. A full report on the survey can be found [here](#).

Mitigating cybersecurity and data privacy risks

A data breach at an ADG company can result in a safety risk or even a national security or economic security risk. The recent SolarWinds cyberattack, which compromised data of at least nine federal agencies and about 100 private sector companies,² underscores how far-reaching such an incident can be. Companies impacted by a cyber incident may not only suffer significant reputational damage but also may face regulatory investigations by multiple government enforcement agencies and collective and class action lawsuits.

It is important to note that IoT devices that have been deployed to track performance, logistics, unmanned systems, and other important business processes collect vast amounts of data that compounds the cybersecurity-related litigation risk. And, companies that produce consumer products must be aware that consumers are increasingly focused on their privacy rights and many jurisdictions have tightened data privacy regulations in recent years. Failures to comply with fast-changing privacy laws also threaten reputational and financial consequences. Moreover, uses of consumers' data in ways that are not anticipated or beneficial to the consumer, even if legally compliant, could erode consumer trust.

Given these risks, it is essential that ADG companies ensure their cybersecurity practices comply with all applicable regulations, that they have an up-to-date cyber incident response plan, and that they periodically conduct a cybersecurity response simulation exercise. It also is increasingly important that the board of directors, if applicable, play an active role in overseeing management of cyber risks because major strategic business decisions, such as investing in new technology, can expand these risks, and regulators increasingly expect boards of directors to be actively overseeing them.

Finally, the role of suppliers is of the utmost importance. ADG companies can have extremely complex supply chains and a cyber vulnerability

anywhere in that chain can undermine the company's own cybersecurity defenses. Companies must therefore confirm suppliers have adequate cybersecurity practices in place and should take steps to add privacy and cybersecurity specialists to their product development teams to avoid developing products that unknowingly raise consumer privacy issues.

Mitigating the risk of technology failures

A failure in a critical technology can also expose companies to costly products liability lawsuits and other claims. The first step to mitigating such risks is to identify business-critical technologies. Yet the Hogan Lovells survey found that 35% of companies surveyed indicated they have not identified all of their business-critical technologies.

After business-critical technologies have been identified, companies need policies and procedures to follow if one of them fails. A "crisis-management playbook" helps companies to mitigate risks, identify gaps in defenses, and deal efficiently with issues as they arise. Producing such a playbook needs to be a collaborative effort. As with cyber incident response plans, multiple parties will have to be involved, including management, technology, and legal teams. Such a plan should include:

- Information defining circumstances that trigger contacting the in-house legal team.
- Escalation procedures that outline when senior management should be informed and consulted.
- Information identifying circumstances that require a report to regulators and detailed information about regulators in each jurisdiction in which your business operates.

Teams must, of course, also be trained to act on this information and respond effectively to a major technology failure event. One of the best ways to reinforce that training is to simulate the response through tabletop exercises.

2. See Jon Porter, *White House now says 100 companies hit by SolarWinds hack, but more may be impacted* (Feb 18, 2021), <https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies>.

Legal teams should be involved in any technology partnerships at the ground floor

The drive to get access to innovative technologies can understandably lead to entering into transactions with companies – many of them start-ups – in new or emerging markets. Thus, some ADG companies are partnering with technology companies through joint ventures (JVs), mergers and acquisitions, and by outsourcing key business functions. These ventures frequently must navigate regulatory regimes that may not have been designed with the current technology in mind. To mitigate the litigation risk raised by such deals, legal counsel should be involved in shaping the transaction from the outset.

Counsel should work closely with technical teams throughout the entire lifecycle of a transaction. It is particularly important to identify any potential issues raised by the technology that may not be covered by generic representations and warranties and to craft specific language in the deal documents to address these issues. The legal team should also consider the extent of the company's right to seek compensation from a JV partner, as well as the extent of protection afforded to the directors of an acquired company if there is a problem.

In the United States, the Committee on Foreign Investment in the United States (CFIUS) has become active in scrutinizing deals involving Chinese companies' investments into technology businesses, therefore it is essential to clarify what party bears the risk of CFIUS intervention and how a conflict will be resolved if one party believes the other has not made every effort to obtain CFIUS approval. ADG companies should also confirm how intellectual property will be shared when entering into JVs with counterparties in other jurisdictions.

Check your artificial intelligence technologies for bias

Most improvements in artificial intelligence (AI) systems are made because of advances in machine learning. However, algorithms underlying machine learning often reflect unwanted biases found within the data on which they are trained. Even as military leaders express hope that AI can give their forces the edge on the battlefield, they have also recognized that algorithms can potentially introduce unintended biases into military systems. Lt. Gen. Mary O'Brien, deputy chief of staff for intelligence, surveillance, reconnaissance, and cyber effects operations, explained during a 17 November 2020 virtual presentation that "If that automated processes that we create are limited in scope or scale or rely on bad sets of data, then we're introducing bias to that limited perspective."³ For instance, an algorithmic bias embedded in a medical simulation program that is used to train medical professionals could lead to better treatment for some patient populations relative to others. Or, as Lt. Gen. O'Brien explained, voice-recognition software that relies on AI may work better for men and for individuals for whom English is their first language. Finally, ADG companies must also be on the lookout for algorithmic biases in business operations tools such as resume screening software employed by human resource departments.

To mitigate the risk of algorithmic bias, companies should catalog what datasets are underlying AI and machine learning technologies they employ and move to eliminate any bias in those datasets. In addition, companies should seek warranties and assurances that any software they procure from a third party does not contain biases, and conduct due diligence to confirm this fact.

3. Mark Pomerleau, *Top intel official warns of bias in military algorithms* (Nov. 18, 2020), <https://www.c4ismet.com/artificial-intelligence/2020/11/18/top-intel-official-warns-of-bias-in-military-algorithms/>.

Key takeaways

Aerospace, defense, and government services companies rely heavily on technology to drive growth. Their C-suites should therefore prioritize risk mitigation and consider the following actions:

- Taking steps to enhance board oversight of technology risk by increasing the time the board spends discussing these risks, adding new technology roles to the board, and creating a technology risk board committee where relevant.
- Reviewing cyber incident response plans to ensure they have adequate input from the legal team, are up-to-date, and are regularly practiced through appropriate simulation exercises.
- Taking steps to ensure suppliers have adequate cybersecurity practices in place.
- Adding privacy and cybersecurity specialists to your product development teams.
- Identifying business-critical technologies and developing “crisis-management playbooks” to mitigate risks associated with these technologies.
- Involving the legal team in the entire lifecycle of transactions that relate to technology acquisitions.
- Taking steps to eliminate bias in AI and machine learning technologies – both those technologies that are developed in-house and those procured from a third party.



Christopher Pickens

Partner | Northern Virginia

T: +1 703 610 6194

E: christopher.pickens@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2021. All rights reserved. 06651