Baker McKenzie.

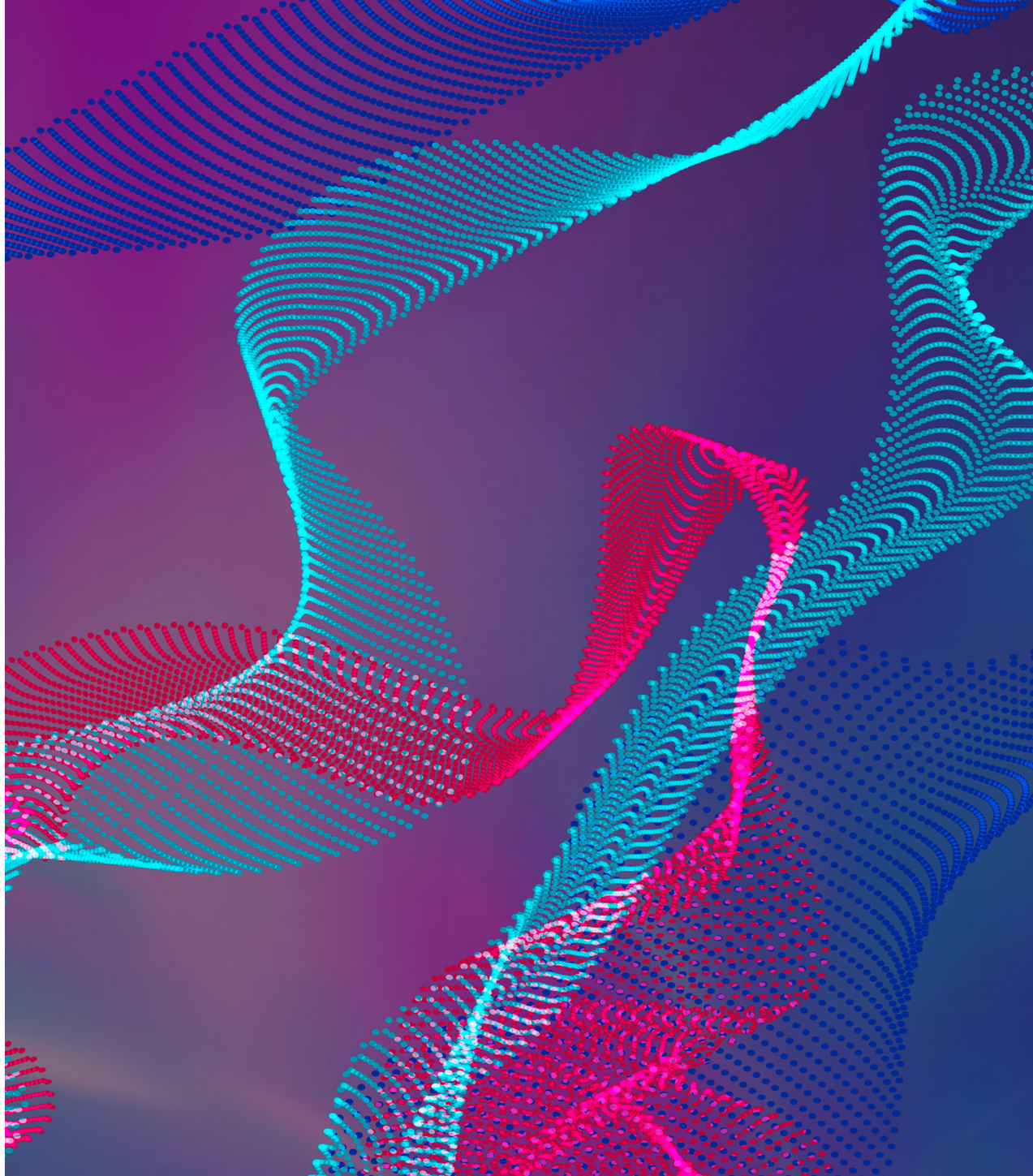
Tech Regulation and Compliance

Report 1

TMT Looking Ahead 2022

Contents

bakermckenzie.com



Foreword

The Technology, Media & Telecommunications (TMT) industry has been crucial in providing the technology, products and services necessary for accelerating digital transformation and helping to enable new ways of working, living and doing business. As the pace of innovation accelerates, new regulatory and compliance questions and considerations will continue to arise.

In 2022, the TMT industry can expect to see the following developments in regulation and compliance:

- Heightened regulatory activity and continued scrutiny of the industry.
- Proactive and increasingly connected regulators working across jurisdictions, proposing new laws and regulations, and sharing information on compliance and enforcement activities.
- Further innovation in areas including autonomous vehicles, virtual and augmented reality, blockchain and digital health, and a renewed focus on how best to protect this IP.
- No slowdown in the pace and complexity of laws regulating data, and continued regulatory enforcement in light of the significant increase in cyber attacks in 2021.

Carolina Pardo
Partner, Bogotá

This report, the first in a five-part series, explores the following key areas:

Artificial Intelligence (AI) — more specifically, machine learning algorithms and software — is one key area of regulatory activity predicted in 2022. The global race to innovate and protect the resulting IP in this space will continue. We look at AI and trade secrets and what is next, with a focus on the US and China.

Read more about AI and trade secrets trends in the US and China in **Section 1**.

Data, the lifeblood of the digital economy, is already a focus area for regulation and compliance activity. We share our data-focused predictions for 2022, with an eye on jurisdictions and technologies to watch in terms of privacy laws and the latest in data transfers and cookies.

Read more about our data and privacy outlook for 2022 in **Section 2**.

As regulators ensure continued, effective detection and enforcement of anti-competitive behavior online, revisiting **antitrust preparedness**, especially within the context of the remote/hybrid working environment, will be crucial for companies working in this space.

Read more about the latest developments in antitrust in **Section 3.**

Cybersecurity has become a key board agenda item in light of the significant increase in the number and severity of cyber attacks, as well as their sophistication. These attacks, coupled with privacy regulations worldwide, raise the spectre of increasing disputes. Examples include class actions (on the back of private rights of action in many privacy laws) and data controllers passing on costs/liabilities to processors or vendors.

Read more about disputes in privacy, cyber and emerging technology in 2022 in **Section 4**.

Look at the **wider compliance and investigations activity** in the TMT sector and where there are likely to be increased compliance activities and further developments around whistleblowing.

Read more about tech regulation and compliance for TMT companies in **Section 5**.

1 AI and Trade Secrets — What's Next in the US and China?

*Authored by **Bradford Newman**, Partner, Palo Alto & **Zheng Zhou**, Partner, FenXun (Baker McKenzie's Joint Operation platform partner in China), Shanghai*[1]

This year promises to be an important one for global AI development. While AI continues to proliferate in Canada (speech recognition use cases), Latin America (healthcare), the European Union (EU) (AI privacy regulation) and various other jurisdictions, the United States (US) and China[2] currently remain as world leaders in AI innovation and deployment. The US and China approach AI from different cultural, political and legal lenses. The breadth and pace of their respective AI innovation and use cases make this an important trend area of focus.

United States:

In the US, there will be increased regulation and enforcement around AI fairness, transparency and explainability — especially in consumer-focused industries.

A notable example is AI hiring tools. The Equal Employment Opportunity Commission (EEOC) has announced a new initiative to investigate these tools. Baker McKenzie experts have been in direct contact with an EEOC Commissioner to understand the EEOC's precise focus. New York City enacted a law which goes into effect in 2023 that, among other requirements, bans the use of automated employment decision tools in hiring unless a bias audit is conducted before that tool is used. Employers that don't disclose their use of algorithm-based technology are subject to a USD 1,500 fine. California is considering similar legislation.

The Plaintiff's Bar is also becoming more familiar with AI use cases in various industries, and an increase in lawsuits is expected in several sectors, including in healthcare and mortgage and other lending. These issues necessarily implicate trade secret protections for algorithms and training data sets. Whether in the context of a government inquiry or litigation, third parties will invoke discovery processes (including subpoenas) specifically aimed at requiring disclosure and production of algorithms, testing protocols and results, internal communications regarding developments and gaps, and many other forms of confidential and valuable information.

China:

China is actively utilizing its advantages in market size, population and national focus to become a world leader in AI development and use cases. China's leaders have made AI a top priority and are encouraging the Chinese tech industry to define standards and norms for global AI practices.

Chinese AI companies, including those in sectors such as gaming, ecommerce, search engines and social media, are clearly at the forefront of AI research, and their products and services are integrating AI into daily life in China and the rest of the world.

On 10 September 2020, the PRC Supreme People's Court released the judicial interpretation titled "Provisions of the Supreme Court on Several Issues Concerning the Application of Laws in the Trial of Civil Cases of Infringement of Trade Secrets." The core elements of AI, such as algorithms and data, are explicitly entitled to trade secret protection under this judicial interpretation. In fact, there have been positive developments for trade secret protection in China, and legislation on trade secret issues has also been significantly accelerated.

[1] Zheng Zhou is a Partner of FenXun Partners, which is a premier Chinese law firm. FenXun established a joint operation office with Baker McKenzie in China as Baker McKenzie FenXun, which was approved by the Shanghai Justice Bureau in 2015.
[2] Throughout this report, "China" refers to Mainland China.

2 Privacy — 2022 Predictions and What to Prepare for

*Authored by **Lothar Determann**, Partner, Palo Alto & **Michaela Nebel**, Partner, Frankfurt*

Countries around the world will continue updating and supplementing data protection laws to restrict data processing and sharing, and to address new technologies and threats to privacy, including facial recognition and artificial intelligence.

To stay ahead of these changes, companies need to develop, regularly update and review privacy compliance measures, risk profiles, tools and governance models[3].

Relatively recent GDPR-like privacy laws in Brazil and the People's Republic of China are being implemented and are expected to be enforced and interpreted by authorities and courts soon. In California, the California Privacy Protection Agency has begun an expansive rule-making process; it is the United States' first such agency, established by the California Privacy Rights Act, that Californian voters passed at the general election of 2020.

Cross-border data transfer restrictions and data residency requirements will continue to present obstacles to global economic cooperation.

Cross-border Transfers

By December 2022, companies must complete the implementation of the revised EU Standard Contractual Clauses (EU SCC), which the European Commission published in June 2021. Some data protection authorities outside of the EU will likely also accept the EU SCC as a transfer vehicle under their non-EU data protection laws, but others may promulgate their own national standard clauses, increasing the compliance burden on multinationals. Meanwhile, companies will continue to struggle with documenting cross-border data transfer impact assessments to address requirements from the Schrems II judgment of the Court of Justice of the European Union for "essentially equivalent levels of data protection" that few non-EU countries (and likely not even many EU member states) can realistically meet. Baker McKenzie foreshadowed these trends in last year's TMT Looking Ahead report **here**.

Cookies

EU and UK data protection authorities continue their acute focus on cookies and similar web-based tracking technologies, and have recently imposed remarkably high fines. Publishers struggle to respond to contractual restrictions on tracking imposed by platform gatekeepers, highly prescriptive and ever-shifting rules for "cookie banners" in the EU, and "do not sell my information" restrictions under US state laws. Nevertheless, many adtech providers, data brokers and industry associations seem intent on staying the course — with the potential for conflicts.

Enforcement

More generally, we expect to see EU data protection authorities continuing to step up enforcement with audits, investigations and high fines. At the same time, companies are likely to challenge fines and injunctions issued by data protection authorities. Law firms will also continue to increase private lawsuits, and press forward with initiatives to establish class action-like litigation in Europe.

Data security threats, ransomware attacks and phishing will also continue to increase. Companies that fall victim to cyber attacks can expect little help or protection from governments against cybercrime waves and need instead brace for additional punishments imposed by governments for insufficient security measures. Individual data subjects will increasingly assert claims and sue for damages, which has been greatly simplified by the statutory damages provisions in the California Consumer Privacy Act. Companies need to prepare or update their incident response plan and systematically upgrade and document their technical, administrative and organizational data security measures (TOMs), ideally directed by legal counsel under attorney client privilege.

Decentralized information technology ecosystems (such as blockchains) will provide new questions and challenges concerning controller/processor models of responsibility. This will therefore create exposure for individual participants, product architects and gatekeepers. Privacy-by-design principles will have to be considered at a early stage[3].

[3] For practical guidance, see Determann's Field Guide to Data Privacy Law, 5th Ed. (2022) and Feiler/Forgó/Nebel, The EU General Data Protection Regulation (GDPR): A Commentary, 2nd Ed. (2021).

3 Antitrust Investigations and Digital Compliance

*Authored by **Jeffrey Martino**, Partner, New York & **Mara Ghiorghies**, Senior Associate, London*

In a world where business is increasingly carried out over a wide range of digital platforms, antitrust regulators have had to reassess their existing investigation tools to ensure continued, effective detection and enforcement of anti-competitive behavior occurring online and/or on ephemeral media. It is therefore essential that in-house legal and compliance teams continue to keep up with these developments and address the compliance and internal auditing challenges that these latest practices reveal.

Spotlight on Digital Dawn Raids

Regulators are adjusting their dawn raid practices[4] and detection procedures to accommodate new working models for businesses, including remote/hybrid environments and new methods of communication.

Our experience across global Baker McKenzie offices indicates a proliferation of the different technologies used by authorities to conduct dawn raids remotely: from using virtual data rooms for an initial triage of documents or conducting unannounced remote interviews with key business personnel, in some cases, surprising companies by accessing company data virtually via video conference facilities without any prior notice. Online tools have been used in certain countries where the enforcement authority has been known to directly contact an employee via video conference without notice, or to have "invited" companies to virtual meetings, then surprising these companies during the meeting by requesting them to provide remote access to employees' laptops so that inspectors from the authority could access specific data on those laptops.

In these virtual or "digital" dawn raids, enforcers are requesting company personnel to immediately provide inspectors with "control" rights to the employees' laptops, without any prior notice, including searches of data stored on their own personal devices at home.

Spotlight on Cartel Detection

A number of regulators have also prioritized their focus to invest in technology around cartel detection tools beyond the tools usually used in dawn raids. For example, using collusion data analytics to identify suspicious bid patterns or resale price maintenance.

Regulators need to analyze vast quantities of complex data and many have taken steps to increase their capacity and ability to analyze new and complex information, investing resources into a wide range of areas, from establishing dedicated units and upskilling in-house, to creating internal working groups and working with external experts (see the G7 report here).

Authorities around the world now have dedicated teams of technical specialists such as data engineers, data scientists, digital forensics and behavioral scientists, who play an important role in monitoring and detecting competition issues as well as analyzing data.

Handling unannounced inspections by authorities in this new remote working reality poses unique challenges that most existing guidelines and training do not address. Yet, access to data and employees during an inspection remains a priority. The penalties for obstructing an investigation remain extremely high, and antitrust authorities are showing very little sympathy for excuses. See the following key recommendations:

- Dawn raid preparedness should be re-visited as a matter of priority and core consideration for companies in this new online environment.
- Companies should ensure that their internal policies are adapted to the latest dawn raid practice and that their employees are re-trained to handle "remote" raids or raids taking place at their homes.
- Technology and internal dawn raid procedures should be tested to ensure they are effective and work in practice in this new hybrid work reality.

[4] The United States Department of Justice executes "search warrants" (not "dawn raids"), however, in this publication we will use "dawn raids"' to describe the overall act from the local authority of executing an unannounced inspection if the authority suspects that an infringement of the local competition law(s) occurred.

4 Disputes in Privacy, Cyber and Emerging Technology in 2022

*Authored by **Paul Glass**, Partner, London & **Stephen Reynolds**, Partner, Chicago*

2021 saw a significant increase in the number and severity of cyber attacks, along with related litigation and regulatory action. In addition, new regulation and government guidance across the globe on both data privacy and cybersecurity, often giving private rights of action to data subjects, mean that the data-related risk continues to increase in 2022.

Class Action Lawsuits for Misuse of Data

In Europe, the filing of class actions for misuse of data, many of them quantified at more than EUR 1 billion, is continuing apace.

This is a relatively new area, so many issues relating to class membership and commonality of harm are still to be determined, although the Supreme Court in England has recently provided some clarity in favor of data controllers. In the United States, ransomware attacks have increasingly led to litigation — both from allegedly impacted individuals and businesses.

Civil Claims Related to Data Transfers

The very strict approach that EU data protection regulators are taking to data transfers after the Schrems II ruling is likely to result in civil claims, on a class basis where permitted, on the basis that the transfers are a breach of GDPR.

These claims are likely to be driven by privacy activists such as NOYB and similar bodies, or litigation funders. However, quantifying damages remains a fundamental issue on which more clarity is needed.

NFTs and Related IP Issues

NFT (non-fungible tokens, unique digital certificates stored on blockchains and conferring certain rights) was one of the buzzwords of 2021; 2021 also saw the first significant reports of NFT theft.

As the market develops at breakneck speed and more businesses see opportunities to expand into this area, we expect to see more disputes over ownership of NFTs and related IP issues. In addition, there are already the first signs of cyber issues relating to some NFTs.

Disputes and Claims Against Vendors

As the cost of responding to and regulatory risk arising from serious cyber incidents increase, we expect to also see an increase in disputes following cyber attacks.

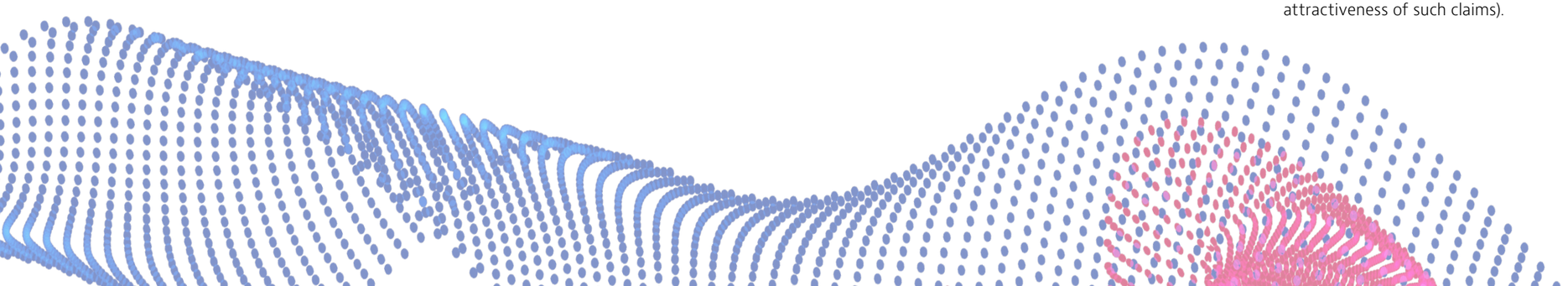
Data controllers may seek to pass on costs or liability to processors or vendors, where the controller considers that those entities were actually responsible for or substantially contributed to a breach.

As supply chain attacks continue, claims against vendors whose software or technology is the conduit for an attack are likely to rise (although limitations on liability will continue to restrict the attractiveness of such claims).

Sanctions as Deterrents to Ransomware Attacks

As the value of personal data to criminals has decreased (due to the sheer availability of stolen data), ransomware attacks continue to increase in regularity, sophistication and the amount of ransom demanded. Threat actors continue to take whatever steps they can to increase their chances of successfully deploying malware (such as paying departing employees to click on links or open documents) and to incentivize payment (for example, deleting backups before activating ransomware).

At the same time, increasing activity by the US Department of the Treasury's Office of Foreign Assets Control means that victims of ransomware attacks are facing additional risk on two fronts concurrently: more sophisticated attacks and increasing regulatory risk. There is a clear direction of travel towards increased sanctions activity to push back against ransomware groups, although how effective that is in practice remains to be seen.



5 Future Spotlights in Tech Compliance and Investigations

*Authored by **Yindi Gesinde**, Partner, London & **Jess Nall**, Partner, Palo Alto*

Compliance and investigations activity in the technology sector is expected to rise considerably this year, due to a number of external factors.

Whistleblowers

The United States Strategy on Countering Corruption highlighted the importance of the US and its international partners creating an environment that facilitates whistleblowing and protects whistleblowers. 2021 saw a great deal of publicity in the US for high-profile whistleblowers, raising issues of not only corporate legal non-compliance but non-compliance with public commitments of a more Environmental, Social and Governance (ESG) nature. Though not all of the ESG complaints alleged are breaches of law, many still rise to the level of a corporate crisis, requiring immediate remediation through updated compliance and controls. This trend is expected to continue throughout 2022.

As the US SEC's whistleblower reward program enters its 10th year, we expect the most whistleblower activity to be in the US.

In the EU, notwithstanding that the EU Whistleblowing Directive's implementation is overdue in the majority of member states at the time of writing, we can expect the emergence of more whistleblowers globally as they are emboldened to come forward and benefit from greater protection.

Compliance Teams and Functions

Compliance teams are likely to see their roles and remits expand with the ongoing proliferation of regulation. This year, we expect to see developments in the regulation of cyber security and data use by AI software as companies embed AI into their products and systems.

This increased regulation will require the creation of new — or the expansion of existing — compliance functions. For example, in November 2021, the European Parliament's Internal Market and Consumer Protection Committee adopted its position on the proposed Digital Markets Act (DMA), envisaging that affected companies would establish a compliance function independent from the company's operational functions and with sufficient authority, stature, resources and access to management to monitor the company's compliance with the DMA.

Given the consequences of non-compliance with the DMA, the stakes in respect of compliance are higher than ever and compliance functions will be expected to bear the brunt. Similarly, in the US, cyber security regulations continue to proliferate, including new Office of Foreign Assets Control guidance on reporting ransomware attacks. Businesses with operations in California will also need to pay increasing attention to the revised provisions of the California Consumer Privacy Act as its imposition of GDPR-like privacy protections is set to go into full effect on 1 January 2023, alongside the enforcement mechanisms embedded in the California Privacy Rights Act.

A Hybrid Future

The future of work is now hybrid (at least for some of the time). Remote work, once the preserve of the few, is now the reality for many. Organizations' compliance processes and programs were originally created around a traditional office-based environment and many compliance teams have worked hard to evolve these processes consistently with today's modified working practices.

It will remain important for compliance teams to ensure that compliance processes and programs continue to adapt and that they, and senior leadership, continue to find innovative ways to monitor compliance, effectively manage audits, investigations and non-compliance remediation remotely, and embed company principles and values in the culture of the distributed workforce.

More Investigations

Due to the expected increase in regulation, many TMT companies expect a corresponding increase in investigations. As we explained in our report The Year Ahead: Global Disputes Forecast 2022, 83% of the 600 senior lawyers at large global organizations surveyed stated that they were concerned about regulatory or law enforcement investigations. Similarly, we expect that companies' handling of data breaches, as well as their reporting regarding such incidents and potentially the failure to prevent them is likely to increasingly lead to enforcement action.

Greater International Collaboration

Regulators and agencies worldwide continue to cooperate, share information and deploy new technology to drive compliance. The recently-published United States Strategy on Countering Corruption (the US Strategy) emphasized the importance of international collaboration, and we expect this trend to continue.

6 Key Takeaways

We have seen the importance of preparing for new regulations, heightened regulatory scrutiny, and ever-increasing data risks. Investing in strategic compliance programs to meet these challenges — and ensuring they use the latest technology and review and update such programs regularly — is more important than ever.

Below are some crucial takeaways with practical tips on key trends:

Global Risk Profiles and Governance Models
Regularly review your global risk profiles, approaches, governance models and priorities.

Data Security Measures
Invest in technical and organizational data security measures and documentation. Individual architects and participants in decentralized IT ecosystems are well advised to consider privacy by design principles at the planning stage.

Regulatory Risks and Ransomware
Litigation and regulatory risk is increasing globally in the context of data breaches, notably including ransomware events. Understanding and documenting data flows as well as your financial risk appetite for ransomware is vital. Analysis of risk and justification of payments will become even more important.

Whistleblower Protocols
Revisit your whistleblower/speak-up programs to ensure they are compliant and fit for purpose. Consider how they deal with potential whistleblowing on ESG-related topics and what controls are in place around related sensitive information.

AI and Trade Secret Protections
Expect increased regulation, litigation and M&A activity around all things AI in the US. China is intensely focused on innovation in this area as it continues its aspiration of being self-reliant. Importantly, core elements of AI, including algorithms and data, are subject to trade secret protection in both jurisdictions.

Dawn Raid Policies
Revisit dawn raid policies and adapt them to current regulatory practice, including training employees on remote raids or raids located at their homes. Regular testing of these policies and company technology is recommended to ensure they are effective in practice in the new hybrid working reality.

Compliance Programs
Adjust your compliance programs to account for increased use of business collaboration platforms and the risks they entail. In addition, adjust the scope of and tools used for conducting internal audits as a key priority — consider using forensic and analytical tools to spot check communications in collaboration platforms and other online tools including instant messaging and chatrooms.

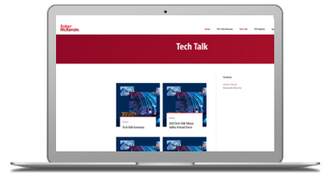
Explore Additional Resources

TMT Talk Podcast
The TMT-focused podcast features insights from top legal advisers in key markets—experts break down the issues and their impacts on businesses and society.

Click here to listen

Tech Talk Events
Tech Talk events offer succinct, practical and timely analyses about the most important global legal developments impacting TMT companies.

Click here to view



TMT Hub
Stay ahead of the curve with Baker McKenzie's Global TMT Hub, which provides a wealth of information around the Technology, Media & Telecoms industry.

Click here to view

7 Key Contacts

Carolina Pardo
Partner

Bogotá
+ 57 60 1 634 1559
carolina.pardo@bakermckenzie.com

Bradford Newman
Partner

Palo Alto
+ 1 650 856 5509
bradford.newman@bakermckenzie.com

Zheng Zhou
Partner, Baker McKenzie FenXun

Beijing / Shanghai
+ 86 10 6535 3878 / + 86 21 6105 8554
zhouzheng@fenxunlaw.com

Lothar Determann
Partner

Palo Alto
+ 1 650 856 5533
lothar.determann@bakermckenzie.com

Michaela Nebel
Partner

Frankfurt
+ 49 69 2 99 08 368
michaele.nebel@bakermckenzie.com

Jeffrey Martino
Partner

New York
+ 1 212 626 4203
jeffrey.martino@bakermckenzie.com

Mara Ghiorghies
Senior Associate

London
+ 44 20 7919 1516
maria.ghiorghies@bakermckenzie.com

Paul Glass
Partner

London
+ 44 20 7919 1288
paul.glass@bakermckenzie.com

Stephen Reynolds
Partner

Chicago
+ 1 312 861 2895
stephen.reynolds@bakermckenzie.com

Yindi Gesinde
Partner

London
+ 44 20 7919 1057
yindi.gesinde@bakermckenzie.com

Jessica Nall
Partner

San Francisco
+ 1 415 984 3822
jessica.nall@bakermckenzie.com

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

bakermckenzie.com