

Big Data and Big Brother:

How General Counsel Cope
with Artificial Intelligence
in an Era of Economic
Nationalism



LexMundi
World Ready

Table of Contents

I. About the Report	1
II. Big Data and Big Brother: How General Counsel Cope with Artificial Intelligence in an Era of Economic Nationalism	2
a. AI, Geopolitics, and the Legal Context	2
b. Big Brother and Big Data 1.0	5
c. Conclusions	7
III. “Implementing Economic Sanctions Today and Preparing for Tomorrow in an Uncertain World” – Contributed by John Smith	8
IV. “EU Trade, Investment Controls and Industrial Policy in a Bi-Polar World” – Contributed by David O’Sullivan	10
V. “Antitrust vs. Regulatory Intervention: How Will Global Markets be Kept Open in an Era of Digitization, AI and Big Data?” – Contributed by Alexander Birnstiel	12
VI. Acknowledgments	15
VII. About Lex Mundi	16



2019 Summit Partner

This publication is not intended to represent a comprehensive guide nor legal advice on the matters covered but rather provide a general overview on the subject. It may only be used as an indication, and advice should always be sought from the appropriate Lex Mundi member law firm.

About This Report

The profound impact of artificial intelligence (AI) on human relationships can hardly be overstated. AI cuts to the very foundations of the social contract that underpins legal institutions and is setting in motion a rather precarious “new power balance...between countries, companies, people, and machines.”

This unprecedented technological leap on its own would be enough for corporate legal departments to cope with. Yet, placed in the hands of nationalist-minded governments, AI might supercharge global power blocs and catch companies in a regulatory crossfire.

In what ways might governments harness AI to protect markets, build champions, advance the national interest overseas, or monitor violations of law? China’s Belt and Road Initiative, US trade and sanctions policies, regulatory pressure from EU governments, and populist movements the world over are all manifestations of an ongoing trend toward greater economic nationalism.

AI poses uncharted problems in the areas of compliance, liability, intellectual property, product development, and antitrust. Increasingly General Counsel are called upon to guide boards, C-suites, co-workers, and the public through new ethical and legal complications about targeting customer sets, diligence on supply chain partners, personnel decisions, and risk. AI, and the politics around it, adds new layers of complexity to the very challenging role of the General Counsel.

The 2019 Lex Mundi Summit in Amsterdam brought together thought leaders and recent government officials from the US and EU to consider the challenges that arise from the intersection of AI with economic interventionism. Specifically, they tackled the emerging landscape by analyzing:

- the power shifts resulting from competing national AI strategies;
- the attitudes of US and EU authorities regarding the use of sanctions and trade policies; and
- the convergence of AI and regulatory activism, i.e. when Big Brother gets Big Data.

Lex Mundi extends its thanks and appreciation to senior in-house counsel participants, guest speakers, and Lex Mundi member firm lawyers for their contributions to the Summit programs and this report. Lex Mundi also extends its thanks to Lexis Nexis for its contributions as the 2019 Summit Partner.

To learn more about how to participate in a future Lex Mundi Summit or Lex Mundi’s risk management resources, please contact Eric Staal or Helena Samaha.

Helena Samaha
President
Lex Mundi
hsamaha@lexmundi.com

Eric Staal
Vice President, Business Development
Lex Mundi
estaal@lexmundi.com

This report brings to light three practical areas requiring vigilance from the General Counsel, as even traditional industries become digital players and business models evolve:

1. Governance

- The composition of Boards may need to be adjusted to ensure the right mix of expertise, to avoid conflicts of interest, and to comply with the regulation of data.
- Companies will need to consider having an ethical and governance framework for AI that is cascaded across the business. Never has the “tone from the top” been so important.

2. Compliance

- Companies may stray into new industries and become subject to unexpected regulation.
- AI may be used by authorities to surveil companies, industries and markets, creating unprecedented liability.
- Authorities may expect companies to leverage AI capabilities for compliance monitoring, including third parties, which would render compliance programs built for the “analog-era” inadequate.

3. The Legal Function

- Members of the in-house team will need to be trained on what to look for and get involved in product development, in order to anticipate new regulatory exposure.
- The legal department may require specialists in data science.
- The legal team will lead, or at least be involved in, the development of the company’s legal and ethical framework for AI, including training the business.

Big Data and Big Brother: How General Counsel Cope with Artificial Intelligence in an Era of Economic Nationalism



AI, Geopolitics, and the Legal Context

According to the 2019 Lex Mundi Summit keynote speaker, Professor Olaf Groth, the emerging geopolitical order will not be determined as in the past with hard military assets and occupation of physical territory, but by AI capabilities used to manipulate real world outcomes through cyberspace. Already we are seeing a competition for preponderance of AI capabilities to magnify the influence of competing social-ideological systems. Much is at stake.

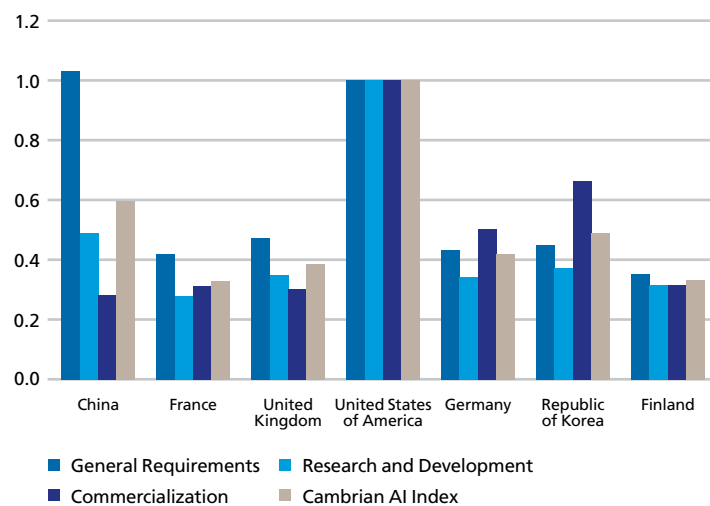
Vladimir Putin and US officials share similar views. The Russian President stated boldly, “the one who becomes the leader in this sphere (AI) will be the ruler of the world.”¹ Robert Silvers, former assistant secretary for cyber policy at the Department of Homeland Security, agreed: “these kinds of technologies are so transformative that the country that gets the lead is going to have not just an economic or tech advantage but also a national security advantage.”²

A look at investment in AI technologies shows two countries head and shoulders above the rest, namely the US and China.³ As representatives of competing systems, many, including US Administration officials, see the emergence of a new Cold War. The Cold War metaphor for US-China rivalry has an important warning for the rest of the world: be careful not to get left behind or squeezed between the two superpowers, owing to a lack of homegrown champions and adequate investment.

Undoubtedly, Chinese policy is intent on creating an alternative to the existing order through significant global undertakings such as the *Belt and Road Initiative* (“BRI”) and *Made in China 2025*.

Cambrian AI Index

Base indicators incorporate a country’s AI preconditions, the research and development environment and degree of AI commercialization.



<https://www.kas.de/documents/252038/4521287/Comparison+of+National+Strategies+to+Promote+Artificial+Intelligence+Part+1.pdf/397fb700-0c6f-88b6-46be-2d50d7942b83?version=1.1&t=1560500570070>

Source: Dr. Olaf J. Groth, Dr. Mark Nitzberg and Dan Zehr, *Cambrian.ai*

¹ “Putin: Leader in artificial intelligence will rule the world,” AP, September 1, 2017, <https://apnews.com/bb5628f2a7424a10b3e38b07f4eb90d4>.

² Louise Lucas and Richard Waters, “China and the US compete to dominate big data,” *Financial Times*, April 30, 2018, <https://www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd>.





³ Dr. Olaf J. Groth, Dr. Mark Nitzberg, and Dan Zehr, “Comparison of National Strategies to Promote Artificial Intelligence,” Konrad Adenauer Stiftung, 2019.

Lesser known is that the China Development Bank (CDB) and the Export-Import Bank of China provide as much financing to developing countries as the World Bank — and this is not to mention the Asian Infrastructure Investment Bank (AIIB) launched in Beijing in 2014. These and other foreign policy initiatives have set President Xi Jinping apart from his predecessors,⁴ offering an unprecedented injection of finance to foreign countries but, crucially, without the same level of Western political meddling.

Underlying the BRI is the expansion of China’s technology and digitization reach. Following the second BRI Forum in April 2019, participants released a statement stating that they ‘aim to enhance connectivity among financial markets and encourage the development of digital infrastructure.’⁵ With over two-thirds of the world’s population covered by BRI, this is a massive step forward in the battle for tech dominance.

Professor Groth cautions against the self-fulfilling prophecy of AI inexorably giving way to a bipolar Cold War 2.0, but he recognizes the potential for it to happen.⁶ Meanwhile, he points out that what the EU does have going for it is a unique model and values that protect the individual, which is more synchronous with the American value system and rule of law — certainly by comparison to China. He sees various competing models of AI globalization with four main ones depicted below and researched thoroughly in a report by AI consultancy Cambrian for Germany’s Konrad Adenauer Stiftung.

Four Approaches to Fostering AI

			
<ul style="list-style-type: none"> • Market (corporate) scale driven: Frontier research. • Breakthrough focus: Ecosystem. • Simultaneous efforts by public and private sector. • Globalized approach. 	<ul style="list-style-type: none"> • “Chinese dream”: The greatest good for the greatest number. • Application focused, techno-Confucianism. • Public-private integration. • Domestic & BRI. 	<ul style="list-style-type: none"> • Individual protection. • Basic research & industry 4.0 focus. • High degree of (market) fragmentation. • Foundation in globalized industries. 	<ul style="list-style-type: none"> • From competition to strategic collaboration. • National specific strengths & weaknesses.

Source: Dr. Olaf J. Groth, Cambrian.ai

Multinational companies can also get caught in the grinding wheels of big power blocks and they are already facing a very tough dilemma as the US confronts the Chinese model. As one Summit participant clearly explained, “What we’re seeing is that we may end up being caught between a rock and a hard place. We can choose between Iran and the US; it’s much more difficult to choose between China and the US.”

One of the main cross-border battlegrounds is over the deployment of 5G with China moving ahead fastest. The network will also enable a lead in factory automation, robotics, and autonomous driving. “5G is a foundation and catalyst for reinventing industries. The fundamental benefit of being the first mover is that you can build business models on the back of that and export them to other countries.”⁷ But that is not all. 5G will expand massively the capabilities of the AI-driven, data-based cognitive economy, which profiles every citizen and can be misused for surveillance capitalism and/or the surveillance state.

⁴ “China’s Massive Belt and Road Initiative,” Council on Foreign Relations, last updated May 21, 2019, <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>.

⁵ Evelyn Cheng, “China expands global ambitions with a new phase of Xi’s signature program,” *CNBC*, April 29, 2019, <https://www.cnbc.com/2019/04/29/belt-and-road-china-expands-global-ambitions-with-new-program-phase.html>.

⁶ Olaf Groth and Mark Nitzberg, “Technology in midst of ‘Cold War 2.0’ between America and China,” *The Hill*, March 21, 2019, <https://thehill.com/opinion/international/435146-technology-in-midst-of-cold-war-20-between-america-and-china?amp>.

⁷ Sheryl Tian Tong Lee, “China Races Ahead of the U.S. in the Battle for 5G Supremacy,” *Bloomberg*, August 1, 2019, <https://www.bloomberg.com/news/articles/2019-08-01/china-bets-on-5g-socialism-in-push-to-lead-global-tech-race>.

In addition to the nightmare reality of ZTE providing tech-enablement for Venezuela's repressive regime, there are obviously also concerns about state and corporate espionage. It was highly coincidental that on the opening day of the 2019 Lex Mundi Summit in Amsterdam, Dutch daily *Volkskrant* published an article alleging that their national authorities had found Huawei likely to have a hidden back door to unspecified "customer data" in the Netherlands.⁸

In recent years the US Administration imposed tariffs on billions of dollars of Chinese imports, blocked a \$1.2 billion bid by Ant Financial to buy MoneyGram, and banned sales of Huawei products in the US. A next move may be to withdraw the favorable conditions for Chinese companies to access US capital markets, which have been exempted from the same level of Dodd-Frank and other Public Company Accounting Oversight Board (PCAOB) requirements that other companies face.

National security concerns are a significant driver in the US-China confrontation, including China's ability to obtain proprietary information and user data through company acquisitions. However, measures against Huawei may impede the development of the US 5G network and inhibit future competitiveness. The EU shares similar concerns and has "urged the US to join forces in countering Chinese attempts to define the technologies of the future, saying a transatlantic alliance is needed to influence global standards for sectors such as telecoms and the internet of things."⁹ Recently, however, the openness to cooperate over technology and commerce appears to depend on whether the EU generally supports American geopolitical objectives such as Iranian sanctions and whether the US supports EU objectives of individual agency and privacy protection.

For General Counsel, the geopolitics of AI have significant implications that will not only drive corporate decisions but also strategies for navigating the legal terrain when it comes to launching products and services, dealing with regulations, and handling negotiations.

Shifting power balances matter for asset valuations, future compliance requirements, enforcement mechanisms and risk in the value chain. How long before it becomes an expectation for parties to use AI in due diligence exercises, not for document review, but for things like identifying successor liability with respect to corruption, third party suppliers, use of data, etc.? The General Counsel has a role in determining appropriate business hygiene regarding the use of AI, including the ethical approach to how AI is incorporated into products and operations.

Groth concluded with "six key components of corporate strategy for the cognitive era," which decision makers should consider as they seek to protect the company's mission critical functions (see box).

As suggested, the crossover between data science, corporate strategy, and legal will only get stronger. It is not too early for General Counsel to think about adding skills and competence to the legal team, both through hiring specialists and training lawyers on staff to identify data issues.

Furthermore, some Summit participants even suggested the need to have a cyber expert on the company board, given the level of AI-related risk companies will increasingly face. Compliance and risk management starts at the top and an individual with cyber expertise can be a valuable ally to a General Counsel.

Corporate Strategy Components for the Cognitive Era

- 1 Form networks to pool anonymized and clean data.
- 2 Acquire data scientists (ensure diversity) and learn to speak the language.
- 3 Define your competitive advantage as hybrid physical-digital players.
- 4 Integrate AI to support your business strategy system.
- 5 Establish safeguards to ensure that everything your AI does is human centered.
- 6 Develop, nurture, and harvest an engagement with the broader ecosystem.

For General Counsel, the geopolitics of AI have significant implications.

⁸ Arnout Brouwers, "Europe cannot escape a choice between America and China", *deVolkskrant*, May 19, 2019, <https://www.volkskrant.nl/columns-opinie/europa-ontkomt-niet-aan-een-keuze-tussen-amerika-en-china-b4b81266/>.

⁹ Jim Brunsten, "EU urges alliance with US to counter Chinese tech dominance," *Financial Times*, July 25, 2019, <https://www.ft.com/content/aabd515e-aed5-11e9-8030-530adfa879c2>.

Big Brother and Big Data 1.0

There are some early examples of the use of AI in investigations and enforcement actions. Summit participants mentioned claims by the Brazilian antitrust authority to use AI to identify cartel activity, or the role of AI in financial services to monitor transactions and clients. In the US, the Securities and Exchange Commission (SEC) uses algorithms to drive surveillance programs and innovate their market risk assessment initiatives.¹⁰ The Australian Securities and Investment Commission also uses AI to detect misconduct and improve regulation.¹¹ AI provides a faster and more comprehensive tool for governments to identify violations, sometimes even before the company has done so. The question becomes how companies keep up with regulators, in order to know both what big brother knows and what big brother expects them to know.

Discrepancies across jurisdictions are starkest when dealing with sanctions, particularly with respect to Iran, Venezuela, Cuba, Russia, and others. Huawei provides an excellent example. While the US, Australia, New Zealand and Japan have enacted some degree of banning Huawei technology, some major European countries did not follow suit.

During Summit discussions, frustrations were apparent over how companies doing business with a blacklisted vendor should proceed globally. Investment regulations are also being pursued aggressively by the US and increasingly the EU, both focused on China. The extent of the sanction reach has gone far beyond a direct relationship to Chinese companies as seen with the blocking of Broadcom's \$142 billion bid for US chipmaker Qualcomm on the basis that it would give China another edge in 5G.¹²

John Smith, long serving director of Office of Foreign Assets Control (OFAC) in the US Treasury Department, shares his views about sanctions compliance based on the five main principles of the OFAC compliance framework.

Summit discussions also highlighted the importance of so-called secondary sanctions, which one participant raised as a "fog of uncertainty" that undermines the ability of General Counsel to give "go-no-go" decisions to the business.

As geopolitical considerations factor more into compliance and regulation, the use of AI may exacerbate differences over sanctions policy and the prosecution of violations by authorities.

Some participants felt that sanctions are an area in which interacting with regulators is fraught with more uncertainty compared to others. While there is little reliability of getting "clear guidance," the company may become subject to greater scrutiny by notifying potential exposure.

More than ever it is imperative to pay close attention to third party exposure beyond normal due diligence exercises on direct counterparties. Companies should be especially careful when undertaking M&A as it is one of the most significant ways to fall afoul of sanctions. It can be very difficult to stop a deal if an issue is identified, but the failure to do so creates very real exposure.



¹⁰ Scott W. Bauguess, "The Role of Big Data, Machine Learning and AI in Assessing Risks: a Regulatory Perspective," (keynote address, New York, New York, June 21, 2017), 19th Annual Operational Risk North America Conference, <https://www.sec.gov/news/speech/bauguess-big-data-ai>.

¹¹ Jamie Smyth, "Australian regulators cautiously embrace AI to boost compliance," *Financial Times*, April 8, 2019, <https://www.ft.com/content/33eb5934-4519-11e9-b168-96a37d002cd3>.

¹² John Thornhill, "Formulating values for AI is hard when humans do not agree," *Financial Times*, July 22, 2019, <https://www.ft.com/content/6c8854de-ac59-11e9-8030-530adfa879c2>.

¹³ Margrethe Vestager, "Check Against Delivery" (speech, Brussels, September 29, 2016), EDPS-BEUC Conference on Big Data, https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/big-data-and-competition_en.

Even where sanctions are not in play, the general lack of consistency in regulatory approaches is a challenge. The EU's approach to considering control of data as part of merger reviews is a prime example.¹³ The US, so far, has taken a much more hands-off approach by not entertaining big data arguments at all. At the time of the Summit, however, neither the EU nor the US had rejected a merger on the basis of big data creating an unfair advantage.¹⁴

Alexander Birnstiel, Partner with Noerr LLP, the Lex Mundi member firm for Germany, shares his analysis at the end of this report regarding what companies should bear in mind as they go digital. Digitization means that for every company, the competitor set and space is changing. The EU is leading the way for taking digitization into account in antitrust matters with other countries following its lead over the US laissez-faire approach. In this context, companies are well advised both to update their antitrust compliance programs as well as to consider how their new business models may encounter regulation. Additionally, companies may need to look at who is on the company board and involved in governance, because as business digitizes you can start to run into problems regarding the exchange of data and sensitive information. Product development and operations teams do not necessarily anticipate the impact of innovation on corporate governance and compliance, but the General Counsel is in a unique position to spot potential issues.

With the embedding of AI into a company's operating platform comes a host of liabilities, most obviously data privacy. The Equifax data breach yielded \$700 million in fines. Both Marriott and British Airways have also suffered massive fines under the EU's General Data Protection Regulation (GDPR) for cybersecurity breaches they suffered in late 2018, \$123 million and \$229 million respectively. UK Information

Commissioner Elizabeth Denham explains the burden on multijurisdictional companies with respect to personal data in her statement regarding the Marriott fine, "...organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected."¹⁵

The use of AI can also open companies up to liability for discrimination on all levels, including suppliers, customers, employees, etc. "AI is only as good as the data it's fed, so if the information is biased, the AI's decisions will reflect this as well."¹⁶ What happens when risk profiling systems reject people for a job, a loan, insurance coverage, or other services based on data? What happens when algorithms create new classes of society that previously were not protected?¹⁷

When it comes to compliance investigations some timeless lessons and truths continue to hold. Kees van Ophem, Executive Vice President and General Counsel of Fresenius Medical Care, shared the riveting experience of negotiating a FCPA settlement amounting to over \$200 million dollars with the US Department of Justice. As ever, cooperation and training are key factors to reducing current and future liabilities.

Companies do not have the ability to know all that big brother knows or will know, but a code of conduct and training procedures can help establish the commitment to avoid violations and comply with regulations. In the Fresenius Medical Care case, the lessons learned were integrated into training and supported by the company leadership.

Fresenius Medical Care FCPA Negotiation

Following a whistleblower disclosure, the company launched an internal investigation which was disclosed to the US Department of Justice (DOJ) and Security and Exchange Commission (SEC). The consistent pattern of communication and cooperation with the US government assisted in building credibility and improving negotiations, which led to the ability to lock in a specific timeline for issue discovery purposes. In addition, the company agreed to "enhance its compliance program, implement rigorous internal controls, and retain an independent corporate compliance monitor for at least two years" in lieu of prosecution. At the time of the Summit, additional prosecutions were still pending in other jurisdictions.

¹⁴ Daniel S. Bitton, "United States – E-commerce and Big Data: Merger Control" Global Competition Review, E-Commerce Competition Enforcement Guide, December 7, 2018, <https://globalcompetitionreview.com/insight/e-commerce-competition-enforcement-guide/1177730/united-states-%E2%80%93-e-commerce-and-big-data-merger-control>.

¹⁵ Kate O'Flaherty, "Marriott Faces \$123 Million Fine For 2018 Mega-Breach," Forbes, July 9, 2019, <https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#409f3d914525>.

¹⁶ Kori Hale, "IBM's Unbiased Approach to AI Discrimination," Forbes, September 25, 2018, <https://www.forbes.com/sites/korihale/2018/09/25/ibms-unbiased-approach-to-ai-discrimination/#c715b4071185>.

¹⁷ Professor Frederik Zuiderveen Borgesius, "Discrimination, artificial intelligence, and algorithmic decision-making," Council of Europe, 2018, <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>.

Some early warning signs include companies that have decentralized and weaker compliance functions but strong local managers able to circumvent policies and controls. It is also worth being on the lookout for how sales incentives and targets might influence individual behavior, for example when they are linked to margins and cash flows. Van Ophem also stresses that the General Counsel and local legal heads should get involved in hiring decisions to ensure that leadership and management have the right values.

Conclusions

As if the global web of regulatory activism were not enough to deal with already, it is only a matter of time before the AI-enablement of national authorities fortifies that web. AI is changing the power balance and fueling the rise of new social-ideological blocks with the US and China leading the way. Companies will inevitably be caught in the enforcement crossfire as legal institutions evolve to accommodate this new technological reality. It is worth looking at where these trends are taking us and what it means for compliance and risk management.

There is an upside for companies and General Counsel. AI can also be leveraged for greater transparency and oversight of business practices in ways that lead to greater adherence to the company's ethical standards and values. In time, perhaps issues can be spotted sooner, and the damage mitigated. First, however, General Counsel will need to get a grip on how AI is transforming their companies inside-out and what new areas of regulation will be encountered.

More and more, analog-era compliance indicia such as leadership commitment, a rigorous code, training and other measures will become mere table stakes. Similar to financial services today, more companies will need AI systems and capabilities to self-monitor compliance. Even if governments do not yet impose expectations of AI capabilities, it will be important to keep up with what governments know about the business, in order to head off risks and liabilities.

Proactive General Counsel will also take on a role for ensuring effective AI-hygiene to preempt new areas of risk. As General Counsel cope with AI – on the regulatory front and in the business – they will need to assemble a program of AI training for both legal and management teams. General Counsel may also need to hire in expertise on data management issues to keep up with rapidly changing AI applications.

Beyond the legal department itself, General Counsel should keep an eye on governance as the business model evolves, and assess whether the company is straying into new markets and becoming subject to additional regulation.

As if the global web of regulatory activism was not enough for General Counsel to deal with already, it is only a matter of time before the AI-enablement of national authorities fortifies that web.





Implementing Economic Sanctions Today and Preparing for Tomorrow in an Uncertain World

Contributed by: **John E. Smith**, Partner, Morrison & Foerster (Lex Mundi member firm for USA, California), and Former Director of the US Treasury Department's Office of Foreign Assets Control (OFAC)

Economic sanctions have become among the most powerful tools governments deploy in our modern age — and among the most pressing and complex concerns that global corporations face. Boardrooms, chief executives, compliance chiefs, and General Counsel not only are expected to adhere to the intricacies of today's sanctions rules and requirements, but also to use their crystal balls to accurately forecast the evolving geopolitical landscape as the Trump Administration battles China, the U.S. Congress takes on Russia, the situation in Venezuela continues to deteriorate, and the Iran nuclear deal hangs by a thread amid tensions between Iran and both the United States and Europe.

Amid the political, military, and diplomatic strife in the world, what are global corporations expected to do to stay in compliance with the sanction rules and out of the cross hairs of governments? As the venerable Boy Scout motto commands, "Be prepared."

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) recently issued a Framework for Compliance Commitments.¹⁸ These five general principles provide a useful starting ground for global companies to prepare themselves to manage today's rules and tomorrow's risks.

The first of those principles — management commitment — means that management must commit themselves and their organizations to creating and fostering a culture of compliance. But what does that actually mean? In my view, it means hiring the best — the best compliance and legal teams, just as companies compete for the brightest stars across all their business lines. It means spending the resources now to equip the company to weather the storms ahead. If your IT resources are not up to par to managing compliance across the organization, for example, then you leave yourself exposed to sanctions violations and the resulting possibility of years-long government investigations, reputational damage, significant monetary penalties or settlements, and astronomical legal fees.

¹⁸ A Framework for OFAC Compliance Commitments, The United States Department of Treasury, https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.



If your IT resources are not up to par to managing compliance across the organization ... you leave yourself exposed.

The second compliance commitment — risk assessments — should be a daily guiding principle for every employee across an organization. What are the risks of particular business lines, products, and geographies? Risk assessments are particularly important, and particularly tricky, because inherently they look to the future — what is the sanctions risk of doing business in China, Russia, or Venezuela today and how is that likely to change tomorrow? Balancing potential risk with potential reward is an essential component of every business line and applies equally in the sanctions compliance realm.

The third compliance commitment — internal controls — is the flip side to risk assessments. It means that global corporations should ensure that they have the appropriate policies and procedures in place to manage risks that are identified today and in the future. If a business line or corporate office identifies a potential sanctions violation, or an area of legal or reputational sanctions risk, are there procedures in place that ensure that appropriate personnel swoop in to examine the risk and manage or neutralize it?

Like its predecessor, the fourth compliance commitment — testing and auditing — follows from the one before. Testing and auditing is where the rubber meets the compliance road. Companies with the most comprehensive, well-designed, and up-to-date compliance programs regularly can be hit with bracing doses of reality when internal or external testing and auditing discovers that personnel spread across the geographic and business lines of a company are not following, and sometimes are not even fully aware of, global sanctions compliance policies.

The final compliance commitment — training — is the one most easily understood and, ironically, perhaps the one most frequently failed. To be fair, it is difficult to ensure that every employee of a global corporation receives a sufficient level of sanctions training. Ensuring that your compliance and legal teams are sanctions whizzes generally will be far less challenging than spreading the appropriate level of training both to the boardrooms above and the business lines throughout a global company. An equally daunting task is making employees recognize that their own futures, along with those of their employer, hinge on their ability to understand and implement the sanctions training they receive.

Testing and auditing is where the rubber meets the compliance road.



EU Trade, Investment Controls and Industrial Policy in a Bi-Polar World

Contributed by: **David O'Sullivan**, Former European Union Ambassador to the United States and Chief Operating Office, European External Action Service (EEAS)

The European Union and the United States are each other's most important trade and investment partner, trading over USD 1.1 trillion annually. That is over \$300 billion a day. However, the policies and practices of the current administrations are calling this partnership into question and increasing tensions globally.

The Trump Administration has adopted a strong preoccupation with bilateral trade balances in goods alone, despite disagreement among economists on whether this practice is a key indicator of economic strength. However, the US trade deficit stems mainly from macroeconomic factors.

Furthermore, the administration has taken a number of protectionist measures, which are not compatible with World Trade Organizations (WTO) rules. Specifically, the US placed tariffs on EU exports of steel and aluminum as a result of an unsubstantiated use of the national security exemption. These types of tariffs threatened to extend to the auto sector as well.

The agreement reached by President Juncker and President Trump on July 25, 2018, called for a standstill on all new tariffs of any kind. Moving forward, they also agreed to work jointly on trade issues of mutual concern.

Yet, transatlantic political and economic tensions continue to increase with the US reimposition of sanctions on Iran and new sanctions related to Cuba, the increasingly contentious debate over defense costs burden sharing, and the WTO panel outcomes in the Boeing vs Airbus cases.

The EU is already at the center of the largest free trade network the world has ever seen.

In contrast to the US approach, the EU continues to pursue an aggressive policy of trade opening via free trade agreements ("FTA"). Landmark deals with Canada, Mexico and Japan have been followed by deals with Singapore, Vietnam and, most recently, Mercosur. Talks are beginning as well with Chile (to update an existing FTA), Australia, and New Zealand. Taking into account existing trade deals (for example, South Korea), the EU is already at the center of the largest free trade network the world has ever seen.



Furthermore, 2019 will also be a year of institutional transition for the EU. After the recent European Parliament (“EP”) elections, agreements must be reached on appointments to the key positions of President of the Commission, President of the European Council, President of the European Parliament, The High Representative for foreign policy and the President of the European Central Bank. These nominations will be followed by the process of establishing the new European Commission, which will take office in early November after a confirmatory vote of the EP.

The EU faces a number of key challenges including climate change and environmental sustainability, growth and jobs (especially Eurozone reform), democracy and fundamental rights, security (in particular border control and migration management), neighborhood policy and enlargement, and external relations, especially with the US, Russia, China, and Africa. Brexit also looks likely to be part of the political and economic agenda for many years to come.

Important though transatlantic relations and EU developments are, we must not lose sight of the bigger global picture and, in particular, the political and economic challenges posed by the rise of China, which will be THE geo-strategic issue of the coming period.

The key question facing both the US and EU is how to deal with China’s reemergence as a global heavyweight. Do we see this as a zero-sum game in which China’s growth can only come at the West’s expense (as some around President Trump clearly believe)? Or is there a win-win outcome possible? European business has become much disillusioned with Chinese unfair practices, and the BRI initiative has also made a number of governments wary of what lies behind China’s investment plans. The growing dominance of companies like Huawei in the IT sector has raised concerns about national security, which in turn raises the bigger issue of the huge changes that technological developments, such as AI, bring to our political, social and economic landscape. It remains that the US, as the current global superpower, probably feels more existentially threatened by China than is the case for Europe.

The political and economic challenges posed by the rise of China ... will be THE geo-strategic issue of the coming period.



Antitrust vs. Regulatory Intervention: How Will Global Markets be Kept Open in an Era of Digitization, AI and Big Data?

Contributed by: **Alexander Birnstiel, L.L.M.**, Partner, Noerr LLP, Lex Mundi member firm for Germany

“How to keep global digital markets open” is not only a question for competition authorities and regulators, but also for companies and their legal teams.

Digital technologies are dramatically disrupting the economic and operating principles that have guided industries for decades. A McKinsey survey revealed that only eight percent of the companies interviewed believe their current business model still would be economically viable if their industry continues to digitalize at its current course and pace.¹⁹

The examples of companies that are digitizing products, services and business models are numerous and spread across countless businesses and industries. Not all of them realize that in doing so they become “digital market players,” which need to comply with a rapidly evolving competition law and regulatory environment especially designed for digital businesses and aiming at keeping global digital markets open.

Legislators, regulators and competition authorities across the globe are responding to digitization, Artificial Intelligence (“AI”) and Big Data in innovative and increasingly different ways. For instance, the European Union has been adopting a more “interventionist” approach to digital matters involving heavy antitrust enforcement as well as new regulatory approaches. In the US, a more “laissez-faire” approach can be seen – despite attention in the political world – whereas other jurisdictions gravitate around these two poles with very different approaches.

Against that background, companies and their in-house legal teams must navigate an environment characterized by a patchwork of new competition enforcement initiatives and regulatory rules across jurisdictions whenever they engage in digital business.

¹⁹ Jacques Bughin, Tanguy Catlin, Martin Hirt and Paul Willmott, “Why digital strategies fail,” McKinsey Quarterly, January 2018, <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-digital-strategies-fail>.



Nowadays when companies are developing new digital business models and are entering new digital markets, their in-house legal teams should be very closely involved to avoid wide-ranging, digital-business focused, antitrust enforcement actions, as well as digital regulatory intervention and overregulation. This is not only important to satisfy their usual legal risk management functions. It is also of utmost importance from a company's perspective, in order to keep its current and future markets open, i.e. free – to the extent possible – from burdensome and costly competition enforcement action and regulatory intervention.

No matter whether in-house legal teams have to deal with mergers, agreements, cooperation, the exchange of information or with designing and implementing commercial policies in a digital context, they face extra challenges:

- 1** They need to understand more than ever before the technical side and technology behind a certain (new) business model;
- 2** They need to understand and define rapidly changing digital markets;
- 3** They need to understand and anticipate rapidly evolving digital competition and regulatory policies;
- 4** They need to understand the role of data and innovation as a relevant competition parameter; and
- 5** They need to make competition authorities and regulators understand the business model they want to defend and how competition works on a given digital market.

Successfully dealing with these challenges, however, will help in-house legal teams cement their role as trusted business advisers in the new digital reality. It will also help in-house legal teams to keep their companies' digital business activities and markets less vulnerable to competition and regulatory intervention in an era of digitization, AI and Big Data.

Some practical takeaways for in-house legal teams moving forward are:

- 1 Develop and establish a “digital competition strategy”:
 - Update competition compliance programs to the digital reality
 - Closely monitor new technologies and digital business models
 - Make competition compliance part of digital business development
 - Participate at an early stage in development and implementation of new technologies and digital business models. Do not leave it to tech and IT teams only.
- 2 Look beyond usual competitors, customers and suppliers.
- 3 Consider the market effects of new technologies and digital business models.
- 4 Think of early cooperation with antitrust authorities and regulators.
- 5 Play an active role in legislative and regulatory initiatives in your company’s key markets and team up with regulatory and governmental affairs teams.



Acknowledgments

Lex Mundi wishes to thank the following:

Alexander Birnstiel, Partner, Noerr LLP, Lex Mundi member firm for Germany

Dr. Olaf J. Groth, Global Professor of Strategy, Innovation & Economics & Program Director for Disruption Futures at Hult International Business School, CEO of Cambrian.ai, Author with Mark Nitzberg, *Solomon's Code: Humanity in a World of Thinking Machines*

David O'Sullivan, Former European Union Ambassador to the United States, and Chief Operating Officer, European External Action Service (EEAS)

John E. Smith, Partner, Morrison & Foerster (Lex Mundi member firm for USA, California), and Former Director of the US Treasury Department's Office of Foreign Assets Control (OFAC)

Cornelis van Ophem, Global General Counsel and Executive Vice President, Fresenius Medical Care

Joanna Weller, Global Legal & Regulatory Compliance Counsel, LexisNexis

Jane Catherine Collins and **Eric Staal** for their work on the Summit program and contribution to this report.

Participating Lex Mundi member firms:

Arendt & Medernach SA (member firm for Luxembourg)
Asters (member firm for Ukraine)
Basham, Ringe y Correa, S.C. (member firm for Mexico)
Burness Paull LLP (member firm for Scotland)
Chiomenti (member firm for Italy)
Day Pitney LLP (member firm for USA, New Jersey)
Demarest Advogados (member firm for Brazil)
Egorov Puginsky Afanasiev & Partners (member firm for Russia)
Gide Loyrette Nouel A.A.R.P.I. (member firm for France)
Houthoff (member firm for Netherlands)
Jenner & Block LLP (member firm for USA, Illinois)
Lee & Ko (member firm for Korea)
Liedekerke Wolters Waelbroeck Kirkpatrick (member firm for Belgium)
Morrison & Foerster LLP (member firm for USA, California)
Noerr LLP (member firm for Germany)
Pestalozzi (member firm for Switzerland)
Steptoe & Johnson LLP (member firm for USA, District of Columbia)
Uría Menéndez (member firm for Spain)

Participating corporate counsel:

ABN AMRO Bank
AB Volvo
Air France
Alfred Kaercher SE & Co. KG
British American Tobacco (BAT)
BT Group plc
Celanese
Ceratizit
Chassis Brakes
ClearView Strategic Partners Inc.
Dana, Inc.
Diageo
Fresenius Medical Care AG & Co. KGaA
Hudson Advisors
Katoen Natie International
LexisNexis
MoneyGram International
NBK Capital
Panasonic
Polynt S.P.A.
Proximus
Rijk Zwaan Zaadteelt en Zaadhandel B.V.
Skyscanner
Suzano Holding SA
WiseTech Global

Lex Mundi also thanks its 2019 Summit Partner, Lexis Nexis



About Lex Mundi

Lex Mundi is the world's leading network of independent law firms with in-depth experience in 100+ countries.

Lex Mundi member firms offer clients preferred access to more than 21,000 lawyers worldwide – a global resource of unmatched breadth and depth. Each member firm is selected on the basis of its leadership in – and continued commitment to – its local market. The Lex Mundi principle is one independent firm for each jurisdiction. Firms must maintain their level of excellence to retain membership within Lex Mundi.

Through close collaboration, information-sharing, training and inter-firm initiatives, the Lex Mundi network is an assurance of connected, on-the-ground expertise in every market in which a client needs to operate. Through our global service platform, Lex Mundi member firms are able to seamlessly coordinate their clients' most challenging cross-border transactions and disputes.

Lex Mundi member firms are located throughout Europe, the Middle East, Africa, Asia and the Pacific, Latin America and the Caribbean, and North America. Through our nonprofit affiliate, the Lex Mundi Pro Bono Foundation, members also provide pro bono legal assistance to social entrepreneurs around the globe.



Lex Mundi

The World's Leading Network of Independent Law Firms

2100 West Loop South, Suite 1000

Houston, Texas USA 77027

1.713.626.9393

www.lexmundi.com

Get critical intelligence
with help from
Nexis Diligence™



Nexis Diligence™ can help you mitigate business risk by making it easier to vet clients, agents, partners, suppliers, investments, and other third parties against global content in a quick and comprehensive manner.

With Nexis Diligence, you can:

- ✓ Perform a background check on a company or person
- ✓ Uncover indicators of beneficial ownership
- ✓ Conduct a check of negative news
- ✓ Check sanctions watchlists, blacklists and politically-exposed persons (PEPs)
- ✓ Review a subject's U.S. public records* and litigation history
- ✓ Learn about a company's business and management structure, financial health, and M&A activity
- ✓ Scan negative news for a baseline assessment of the risk of doing business in a particular country
- ✓ Predict potential risks with financial vitals such as Experian® business data and risk scores

Here's how you can use it:

- Perform a search on a company or an individual according to your company's due diligence approach. Default preferences can be set at an organizational level to ensure process consistency across all users.
- Search across multiple databases to get comprehensive, relevant matches quickly against news and business information, sanctions and PEPs, litigation history, and more.
- View the results and decide which items you want to save, print, or add to the Report Builder, including any searches that generated no results for your audit.
- Customize reports by prioritizing the information as required. You can also add your own annotations to the report to summarize key points.
- Monitor ongoing activity by creating Alerts in crucial sources, such as Negative News and Sanctions & Watchlists.
- Download a complete History of your search activity when you need to maintain an audit trail.

See Nexis Diligence in action with a personalized demo: [LexisNexis.com/Lexis-Diligence](https://www.lexisnexis.com/Lexis-Diligence) | 800-628-3612



Nexis® Solutions

* Access to U.S. Public Records content is subject to credentialing. Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Using public records for direct marketing activities such as direct mail or telemarketing is prohibited.

LexisNexis, Nexis and the Knowledge Burst logo are registered trademarks and Nexis Diligence is a trademark of RELX Inc. Experian is a registered trademark of Experian Information Solutions, Inc. Other products or services may be trademarks or registered trademarks of their respective companies.

©2019 LexisNexis. All rights reserved. US-EDDM-Diligence-LexMundi-GC-Report-Ad 1119

LexMundi World Ready

2100 West Loop South
Suite 1000
Houston, Texas USA 77027

www.lexmundi.com

Lex Mundi is the world's leading network of independent law firms with in-depth experience in 100+ countries worldwide.

