dentons.com

大成 DENTONS

Dentons' pick of global regulatory trends to watch in 2017

Dentons' team of regulatory lawyers from key jurisdictions around the world weigh in on regulatory trends to watch in 2017 in the US, Europe, the UK, China, Canada and Mexico.

Table of contents

1. Public affairs

Focus on the US 6
Focus on Europe and Brexit 7
Focus on Canada 9

2. Competition/antitrust law

Focus on the US 11
Pharmaceutical pricing 11
Merger enforcement activity and matters to watch 11
The FTC will continue to scrutinize technology industries 11
Stiff criminal fines and jail time against price-fixers will continue 12
Packaged Seafood Cartel 12
Generic drugs 12
An antitrust case to watch 12
Focus on the UK and Brexit 13
What Brexit means for competition enforcement 13
Merger control 13
State aid 14
Focus on Europe 14
Private enforcement of competition law in Europe comes of age 14
The taxing question of state aid 15
E-commerce inquiry by the European Commission 18
Big Data and social media: competition, privacy and consumer protection 20
China 22
Concerted practice under scrutiny 23
Healthcare industry and automobile industry targets of enforcement 23
Competition initiatives: A fair competition review system 24
Merger control: second case adopting “fix it first” approach 24
Revised Anti-Unfair Competition Law 25
Enforcement against anti-competitive loyalty discounts 25
Chinese courts have become more accustomed to SEP and antitrust suits 26
Canada 26
Legislation and enforcement guidance 26

Mergers 27
Cartels....27
Abuse of dominance....27
Litigation 27
Mexico 28
A reinvigorated COFECE 28
Deregulation of the energy sector 29
Cartel-like horizontal agreements under scrutiny 29

3. Foreign investment review and national security

Focus on the US 30
Defense and national security 30
Foreign investment – national security review 31
Focus on China 31
Foreign investment rules and national security review 31
Focus on Canada 32
Background.... 32
Fewer "net benefit" reviews as review thresholds increase.... 32
National security review out of the shadows?.... 32

4. Privacy and data protection

Focus on the US 34
Focus on Europe 34
Legislative reform picks up steam....34
Proposed e-Privacy EU Regulation – more red tape or the necessary alignment with the new EU data protection rules? 35
Germany 35
Focus on China....36
Rapid changes as China moves on cybersecurity and data protection....36
Focus on Canada....38
Eyes on Europe while preparing for mandatory breach reporting 38
Focus on Mexico....38
Focus on Colombia 39
Extended and expanded powers to regulate data processors....39

5. Economic sanctions and trade

Focus on the US ... 41
Trade ... 41
TPP ... 41
NAFTA ... 41
Other trade priorities ... 42
Focus on Canada ... 42
Trade agreements ... 42
Sanctions ... 42
Trade disputes ... 43

6. Anti-corruption

Focus on the US ... 44
A new team takes over at DOJ and the SEC ... 44
The DOJ's Yates Memorandum changed the fundamentals for internal investigations ... 44
The future of the DOJ's FCPA Pilot Program is less clear ... 45
International cooperation on anti-corruption appears to be locked in ... 46
Conclusion ... 47
Focus on the UK ... 47
Conduct of Rolls-Royce ... 47
A distinctive DPA ... 47
Decision to impose a DPA rather than prosecute ... 48
What next? ... 48
Focus on China ... 48
Judicial interpretation on handling criminal cases involving embezzlement and bribery ... 48
Anti-commercial bribery in revised Anti-Unfair Competition Law ... 49
Focus on Canada ... 49
Focus on Mexico ... 50
Contributors ... 53

1. Public affairs

Focus on the US

The first few months of the political calendar in the US will be dynamic and marked by significant policy and regulatory developments as the presidency of Donald Trump and new US Congress take shape. The legislative agenda is likely to be loaded with Republican priorities, chief among them revisions to the US tax code, and repeal or significant modification to health care, specifically Obamacare.

Once Obamacare is addressed, the candidates for legislative action are virtually endless, as what for many years was simply the Congressional Republican wish list, is now squarely within the realm of the possible. It involves such issues as undoing much of Dodd-Frank (financial regulation); reversing the Obama Administration's climate change agenda; making fundamental changes in immigration policy designed to strengthen the border and curb illegal immigration; moving away from global trade deals and toward bilateral agreements; and potentially making profound changes to federal personnel practices to facilitate termination or reassignment of federal workers.

President Trump will continue to roll back specific regulatory initiatives of the Obama Administration, and will continue to identify and select key officials to fill senior roles within the administration. But the likelihood of success for all new initiatives remains subject to the politics of the moment, and will be shaped by the new president's relationship with the Republican-dominated Congress. The coin of the realm in Washington remains floor time in the Senate. When one reviews the President's agenda, pairs it with the agenda of the House and Senate leaders, and adds into the mix the left-over appropriations work from the 114th Congress that still must be addressed, one quickly realizes that the 115th Congress is gearing up to be one of the busiest in recent memory.

In the midst of Republican control, the Democratic Senate Minority, particularly those Democratic Senators in states that President Trump carried and who are up for re-election in 2018, will have significant sway over how much of this aggressive agenda finds its way to the President's desk.

It is also critical to consider that not all Republicans, and this is especially true in the Senate, are necessarily in favor of the sweeping agenda the President proposes. This potential divergence has already appeared in the emerging debate over the future of Obamacare, as Republican Party members in both chambers begin to question the necessity for immediately repealing with no replacement bill. Should President Trump offer a significant infrastructure proposal along the lines of the approach he discussed during the presidential campaign, it could create an early test of whether the conservative core of the House Republican conference views the Trump spending proposals as a bridge too far.

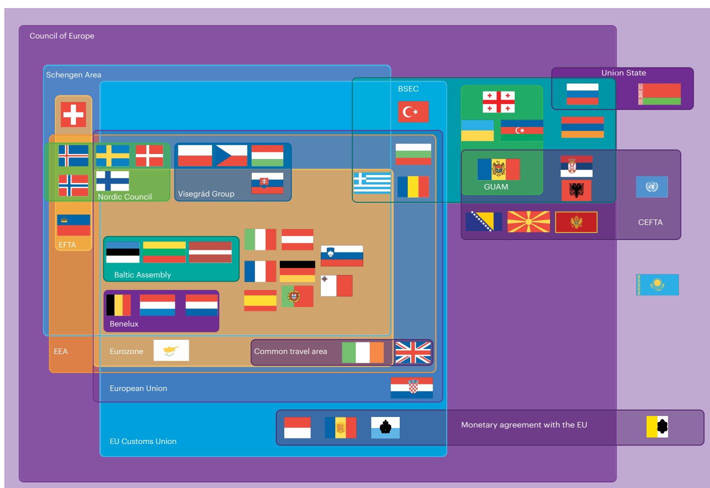
Focus on Europe

Brexit: What happens now?

Six months on from the EU referendum result, the UK Government is no closer to articulating where it wishes to go and how it proposes to get there. The vote is now spoken of in the same breath as the election of Donald Trump and the "No" vote in the Italian constitutional referendum, and is referred to as the beginning of the "populist wave" of "anti-establishment" votes.

The referendum question put to British voters was: "Should the United Kingdom remain a member of the European Union or leave the European Union?" with "Remain a member of the European Union" and "Leave the European Union" as the only options. The referendum was silent on the UK's membership of other international agreements entered into by European countries, which (for the most part) layer themselves around the EU like an onion.

A diagram showing these arrangements is below:



Within the EU, at the core, is the Eurozone and the Schengen Agreement (the latter, confusingly, also contains non-EU members), though the UK has never been a part of either of these. The EU itself sits within the EU Customs Union and the European Economic Area (EEA), the latter of which is also referred to as the Single Market.

The lack of clarity on the UK's future relationship with these other bodies in the original referendum question has caused a logjam in the UK political process, exacerbated in part by the narrowness of the result (52 percent voted to Leave, 48 percent to Remain: there was no "supermajority" threshold). Supporters of what has become known as "hard Brexit" suggest that the Leave vote has also created a mandate for the UK to extricate itself from the entire "onion" and join Kosovo, Kazakhstan and Belarus as the only European countries outside the network of agreements centred on the EU (or alternatively, as some "hard Brexit" advocates suggest, create a series of completely new but as yet undefined bilateral agreements). Supporters of what has become known as "soft Brexit" (who consist primarily of Remain voters) advocate keeping the UK in a similar place to where it is now, but for its EU membership. Under a soft Brexit, the UK would move out a layer and come to rest either alongside Norway (which is in the EEA but not the EU Customs Union) or Turkey (which is in the EU Customs Union but not the EEA). Others still would like a second referendum on whatever arrangement the UK enters into for the most part because they believe that enough Leave voters will have changed their minds to tip the balance in favor of Remain in the event of a rematch.

The questions for the UK include:

- Where in the "European onion" it wants to end up; and
- Where the UK will be allowed to go by the co-signatories to the agreements that will need to be amended to accommodate a non-EU UK.

The UK may take up a position beside Turkey and remain in the EU Customs Union (a "soft Brexit" position occasionally espoused by the opposition Labour Party) as a permanent or temporary measure post-Brexit.

Turkey has supposedly been moving towards EU membership since 1963, when the Ankara Agreement was signed between Turkey and what was then the European Economic Community. But, in the intervening 53 years, Turkey's progress towards EU membership has stalled. Turkey has managed to enter the EU Customs Union, meaning that it benefits both from free trade with the EU and from its exports to the EU not being held up by customs checks. Turkey does not, however, enjoy the regulatory harmony or free movement of its workers to the EU that comes from Single Market membership. The barriers to Turkey joining the EU, known as "accession", (not least the political barriers) appear intractable.

The UK's current customs infrastructure is designed for an environment where around half the UK's imports do not require customs clearance (coming from elsewhere in the EU Customs Union). Without a dramatic expansion, the UK's customs infrastructure would be overwhelmed by the need for additional checks on goods imported from the EU. Multinational supply chains, which rely on an absence of customs checks between the UK and the other EU Customs Union countries, would also have to make allowances for the additional waiting time for products to clear customs when entering the UK from another EU Customs Union country and vice versa. The UK's supermarkets, which rely on "just in time" deliveries of food (half of which is imported into the UK) would also need to adapt their highly complex supply chains. The UK remaining in the Customs Union (at least on a transitional basis) would be the simplest way of avoiding these issues.

The UK Prime Minister, Theresa May, who was appointed to succeed David Cameron, has made it clear in a speech made on January 17, 2017, that she does not see a future for the UK in the Single Market. Although she has not made it clear, it appears likely that she also wishes to exit the EU Customs Union. However, while on the one hand suggesting a complete extrication from the "onion", she has also said that she would like this to be accompanied by a comprehensive free trade agreement with the EU. The points made in May's speech were reiterated in a "White Paper" (a UK Government policy document) published on February 2, 2017. Although the White Paper was hailed as a "plan" for Brexit, it contains very little new information on the UK Government's intentions and appears to have been written in a hurry in order to satisfy demands for a White Paper, rather than to address the mechanics of Brexit in any detail. Crucial issues remain unresolved by the White Paper. For example there is, as yet, no detailed UK Government proposal for the management of the border between Northern Ireland and the Republic of Ireland (which is and will remain an EU Member State) upon Brexit. This is a highly contentious issue given the troubled history of Anglo-Irish relations and the likely problems a "hard" border will create for the peace process. Around the same time, her government suggested repealing the Human Rights Act, which would likely require exiting the Council of Europe (although this plan has apparently since been shelved: not for the first time). The closest country to the UK's eventual position in the diagram, were these things to come to pass, is UN-administered Kosovo which, although outside all multilateral agreements surrounding the EU, has a number of bilateral agreements with the EU. Ironically, Kosovo's position on the outside of the "onion" is a result of its self-declared independent status and not a matter of choice: it is actively seeking EU membership.

May's plans for the UK are no longer necessarily the UK's plans. The UK's Supreme Court ruled on January 24, 2017 in *R* (on the application of Miller and Dos Santos) *v. Secretary of State for Exiting the European Union*, holding that the triggering of Article 50 of the Treaty of European Union (TEU) (a recently-inserted exit mechanism in the EU treaties) could not be triggered by the UK Government without primary legislation by Parliament authorizing it to do so. The UK Government has responded by publishing a very short Bill which would do just that; however, Members of Parliament are proposing amendments which either try to specify "softer" Brexit terms (e.g. retention of the Single Market) or the ability to approve/reject a deal (with rejection resulting in remaining in the EU).

Adding further uncertainty is the ambiguity on the reversibility of the triggering of Article 50. A key reason the UK Government lost in *Miller* was because of its concession for the purposes of the case that Article 50 was irreversible. It did so in order to avoid *Miller* being decided ultimately by the European Court, which has the final say on the interpretation of TEU. An EU court telling the UK how it could leave the EU would have been extremely contentious politically. A case has been launched with the support of "crowdfunding" to bring the question of the reversibility of Article 50 before the European Court via a reference from the Irish courts (the Irish Case).

Yet another ambiguity is whether or not the exit of the UK from the EU also means its exit from the Single Market. As noted above, the Single Market is also known as the EEA, which is held together by the EEA Agreement. This agreement has its own exit clause (Article 127 EEA). It has been suggested that the exit of an EU Member State from the EU would trigger its automatic exit from the EEA; however, a separate mechanism for exit in the EEA Agreement implies otherwise. It is not clear whether Article 127 is intended for use by a former (or soon to be former) EU Member State. In part, this question arises because the EEA Agreement uses the term "Contracting Parties", which is defined inconsistently with respect to the EU and its Member States. Sometimes it means the EU itself, sometimes it means the Member States themselves and sometimes it means both of them. The meaning each time is meant to be "deduced" (to quote Article 2 of the EEA Agreement) from the context in which it is being used and the competencies of the EU and its Member States. The Irish Case is also seeking to resolve the ambiguity around Article 127.

If the UK enters a transitional deal, it is possible, like Turkey's accession process, its exit from the layers of the European "onion" will stall. The UK has an immense bureaucratic task ahead of it in extricating itself from the EU, one which many have suggested it is simply not capable of achieving. The UK's civil service has been shrinking for many years and decades of having the European Commission negotiate international trade agreements on its behalf have left the UK short of the expertise it needs to negotiate its own deals. Additionally, the UK's negotiating partners in the rest of Europe have indicated that they will take a hard line in negotiations. It is therefore unlikely that, this time next year, a clear road map to the UK's final destination will have been made.

Focus on Canada

The election of Donald Trump was, without question, the most important global event to happen in 2016. But Canada's political, business and public policy leaders must not treat the election as just a uniquely ugly campaign with a surprise outcome that can be looked past. It was a historic event that should shift everyone's thinking about the forces of resentment that resulted in the outcome, and what it means for the years ahead. This isn't the first time a tectonic shift in thinking has been thrust upon us.

On November 27, 2000, Prime Minister Jean Chrétien was elected to his third of three majority governments and his final term as Canada's Prime Minister. The Official Opposition—Canada's conservative movement—was directionless and in disarray. In Québec, the separatist parties, the Bloc Québecois and Parti Québecois, lost support for their cause following their defeat in the 1995

Referendum and passage of the federal *Clarity Act* in 2000. The separatist leader, Lucien Bouchard, resigned as Premier of Québec in 2001. The result was a wide open field for Prime Minister Chrétien to move forward on any domestic or foreign policy agenda he wished to pursue.

Once 9/11 happened, everything changed. Prime Minister Chrétien's third mandate was set: the Afghanistan mission, establishing the Department of Public Safety, passing anti-terrorism legislation, creating the Canadian Air Transport Security Authority (CATSA), and eventually saying no to the war in Iraq. Mr. Chrétien experienced the Macmillan principle.

British Prime Minister Harold Macmillan was once asked by a young journalist what he feared most in office, and he famously responded, "Events, dear boy, events." 9/11 was, for Mr. Chrétien, one of those "events". For Prime Minister Stephen Harper, the global recession of 2008-2009 was his. For Prime Minister Justin Trudeau, the election of Donald Trump is his, and 2017 will be dominated by this event—the biggest event—of 2016.

In 2015, after his cabinet was sworn in, the government made public the mandate letters of Prime Minister Trudeau's cabinet ministers. Those mandate letters all likely have an addendum now: regardless of portfolio, all ministers must have a comprehensive engagement plan with the United States for the life of this mandate.

The range of policy anxieties that are now clear and present to Prime Minister Trudeau's government are broad. A few examples:

- Auto sector: Canada's auto sector is the eight largest in the world, integrated through North America, globally competitive and employs more than half a million Canadians. The Canadian auto industry depends heavily on access to the American market, with $135 billion in two-way trade, with America absorbing roughly two-thirds of Canada's parts production and 85 percent of Canada's vehicle output. With President Trump directly criticizing business decisions by auto firms to invest in Mexico, the Canadian sector is rightfully concerned.

- Regulatory cooperation: In 2011, the Canada-US Regulatory Cooperation Council and the Beyond the Border Initiative were put in place to spur greater economic integration. With the North American Free Trade Agreement (NAFTA) having been the subject of a withering attack by President Trump, Senator Bernie Sanders, and emboldened players in both the Republican and Democratic Parties, it is unclear where this integration initiative will now end up.

- Border management: While President Trump's commitment to "build a wall" along America's southern border is well known, what is less well known are his thoughts on the northern border. More than 400,000 people cross the Canada-US border each day, as does an average of US$1.7 billion in commercial activity. Efficiency of infrastructure, data sharing, supply chain realities are all dependent on a cooperative and collaborative policy approach.

- Mutual defense: Canada and the United States have shared interests in the defense and security of the North American continent. From policing the Canada-US shared border to participation in joint operations through NORAD and NATO, Canada and the US share a deep commitment to mutual defense. Initiatives like the Shiprider program that allows Canadian and American enforcement officials to move in tandem to protect the waterways along the border demonstrate the interconnectedness of their security interests. The Permanent Joint Board on Defense also remains an important tool for the Canadian and American militaries to have frank discussions, and exchange views and information regarding joint security.

With one in five Canadian jobs dependent on trade with the United States, and those jobs at risk in export dependent industries from the auto sector to agriculture to forestry and more, Donald Trump's Presidency must now be at the center of Canada's policy planning. In every region, in every aspect of the Canadian economy, it is all at stake, and Canada will need to engage with America anew. While the Canada-US relationship has been a most prosperous two-way economic relationship, the election of President Trump presents a challenge to Canada and Canada needs to be ready, engaged and persistent in protecting our interests. This responsibility lies not only with Ottawa, but also with the provincial governments, big city mayors, business leaders, and others who must shoulder responsibility for engagement with a more distrusting and cynical leadership in the US.

2. Competition/antitrust law

Focus on the US

In the wake of the 2016 elections, we now await the decision as to who will be the "antitrust guard" at the top of the US Department of Justice (DOJ) and the Federal Trade Commission (FTC). At the time of writing, President Trump had not yet named any members of his team to run the Antitrust Division or announced who will be named to the several openings as Commissioners of the FTC. With these significant appointments not yet known, a Republican (at least in name) controlling the Executive Branch, and a worldwide shift towards nationalism instead of globalization, we anticipate the following significant antitrust enforcement issues in 2017:

Pharmaceutical pricing

Pharmaceutical pricing and marketing will be under heavy fire in 2017, as investigations by both the DOJ and FTC, and private lawsuits in this area have exploded and will continue to explode. The attack on the industry is bipartisan, as price increases in the industry are considered to be unjustified by members of both parties at all levels and continue to be attacked. While unilateral pricing behavior is not usually the subject of antitrust challenges, the agencies are likely to push the envelope here. The DOJ's ongoing probes of generic drug pricing include virtually the entire industry. The FTC, state attorneys general, and private plaintiffs are all expected to continue to aggressively pursue conduct by pharmaceutical companies, particularly at the expiration of patent life. "Reverse payment" challenges based on the US Supreme Court's *FTC v. Actavis* decision and on the lower court decisions (particularly antitrust challenges concerning forms of consideration other than cash payments), will continue to encourage government and private suits.

Merger enforcement activity and matters to watch

Big wins in recent years should encourage the staff at the DOJ and FTC to continue to focus on mergers and to bring enforcement actions based on narrow market definitions—unless the new administration has different ideas and appoints leadership with a different agenda. Investigations have resulted in parties abandoning or being enjoined from consummating major acquisitions. Time will tell if companies will test the new administration on merger enforcement. The DOJ and the FTC actively sought to block or reshape combinations in 2016, and our "crystal ball" does not see much significant change in 2017. Among the most notable matters in 2016 were the DOJ's Antitrust Division decisions to attempt to stop the two proposed mergers of the largest health insurance companies, and the FTC hospital merger challenges across the country.

Among the merger reviews and challenges that are already on the docket and worth watching are the *Anthem/Cigna* and *Aetna/Humana* transactions. In July 2016, the DOJ sued to block both Anthem Inc.'s US$54.2 billion bid for Cigna Corp. and Aetna Inc.'s US$37 billion bid for Humana. These merger challenges will be decided by district court judges in Washington, DC, likely in early 2017, with a strong possibility that the losers in those cases will appeal. The two deals raise different competition issues. The DOJ contends that the Anthem/Cigna deal will harm or even eliminate competition to sell insurance plans to large, nationwide employers or those who need large regional networks, and increase the bargaining power the combined entity will have with providers. In the Aetna-Humana deal, meanwhile, the DOJ worried that seniors who rely on Medicare Advantage plans would lose out on the benefits of competition. The DOJ has also claimed the merger would limit competition for individual plans sold on Affordable Care Act public exchanges, though Aetna has said it decided to leave those exchanges as a result of how poorly the business had done as opposed to the merger review. The Aetna/Humana deal raises issues as to whether competition will be harmed in the Medicare Advantage market.

The FTC will continue to scrutinize technology industries

Given the Russian, Chinese and other "hacking" allegations and certainties, scrutiny of technology industries by both the competition and consumer protection bureaus of the

FTC will continue with vigor and there will be a continued focus on privacy, big data and data security.

Stiff criminal fines and jail time against price-fixers will continue

The DOJ continues to seek and obtain large criminal penalties for cartel activities. Billions of dollars in fines sought and obtained against companies and significant jail time for the individuals involved continued in 2016, and there is no reason to think there will be a change in worldwide cooperation or enforcement in 2017. No industry is immune, with the advertising industry being the most recent in the DOJ's crosshairs. Any company without a vigorous antitrust compliance program that is not only in effect, but also regularly updated and enforced, is playing with fire.

Packaged Seafood Cartel

In December 2016, the DOJ announced its Packed Seafood Cartel investigation snared its first victim when Walter Scott Cameron, a vice president of Bumble Bee Foods, pled guilty to allegations that he participated in a conspiracy to fix seafood prices in the US. A second Bumble Bee Foods vice president, Kenneth Worsham, agreed to a guilty plea shortly thereafter. In 2015, Thai Union Frozen Products publicly disclosed the DOJ's investigation into the packaged seafood industry when it announced a planned acquisition of Bumble Bee Foods would not go forward given the government's competition concerns. The investigation has also sparked lawsuits by private parties, including Wal-Mart's antitrust suit in an Arkansas federal court that accuses Bumble Bee Foods, StarKist and Tri-Union Seafoods of conspiring to fix prices for packaged tuna.

Generic drugs

In December 2016, the DOJ accused two former top Heritage Pharmaceuticals executives of plotting to fix prices for antibiotics and diabetes treatments. A Philadelphia district court unsealed a pair of two-count felony charges against Jeffrey Glazer, the former CEO of Heritage Pharmaceuticals, and Jason Malek, the firm's former president, for conspiring to fix prices, rig bids and

divide up customers for doxycycline hyclate, an antibiotic used to treat respiratory tract infections (among other conditions), and glyburide, an oral diabetes medication. The next day, 20 states announced a lawsuit against Heritage Pharmaceuticals, Mylan and four other generics makers, alleging the companies conspired to fix prices and constrain competition for the two drugs. The lawsuits arise out of a DOJ investigation into the generics sector and are a direct result of an industry under heavy scrutiny for high prices. More suits are likely to follow.

An antitrust case to watch

The DOJ and the State of North Carolina sued Carolina's HealthCare System (System), claiming that the System used its dominant market power to prevent Aetna, Cigna and other major health insurers from steering patients to lower-cost hospitals. This is the DOJ's first in the healthcare arena on anti-steering issues. The complaint alleges that the System has rules that include prohibitions on (a) narrow insurance networks of only the System's competitors; and (b) tiered networks placing competing hospitals into the same top tier as System hospitals.

Focus on the UK and Brexit

What Brexit means for competition enforcement

The UK has its own national competition law, prohibiting anti-competitive agreements and abuses of dominance, which affect trade in any part of the UK. These prohibitions are identical to the EU prohibitions (except that the latter apply to trade between Member States), and domestic and EU law both ensure that the UK's primary competition authority, the Competition and Markets Authority (CMA), draws the same conclusions on matters of law and fact as the European Commission (Commission). Eurosceptics should note that the UK voluntarily yoked itself to Commission precedent before it was compulsory to do so, in order to help ensure legal certainty on matters of competition law.

EU competition law has become a model for much of the world and it is highly unlikely that the CMA would want to forge its own path with regard to the vast majority of this jurisprudence. With one exception, that is: vertical restraints.

Much EU competition law on vertical restraints, i.e. restrictions to competition agreed between parties at different levels of the distribution chain, has been driven by the Commission's mission to bring about the Single Market. Practices such as dictating the price, or territory where a distributor is allowed to make sales are permissible in other jurisdictions with competition law, but not the EU. The Commission has done this in part to help create the Single Market: ensuring that distributors are able to sell freely from one Member State into another.

The Commission has extended its case law in this area to the point where restrictions of intra-brand competition (e.g. between two distributors of Nike trainers) are regarded as being as serious as restrictions of competition across entire markets (e.g. across all brands of trainers). The zeal of Member States' authorities in enforcing this interpretation of competition law has also made it very difficult for suppliers to apply different conditions to online and offline selling: a practice which allows suppliers to recognize the additional costs borne by traditional "bricks and mortar" retailers and the additional benefits conferred to the supplier of its goods being put on display. Many have argued that this has been a step too far. Brexit offers an opportunity for the UK's Competition and Markets Authority to step back from enforcement in this area and focus instead on violations of competition law that have more demonstrable effects.

Merger control

The Commission is a "one stop shop" for evaluating and clearing mergers in 31 countries where the merging parties reach the relevant EU and worldwide turnover thresholds. Once it is notified of a transaction, the Commission takes

over evaluation of the merger and its effects, not just for the EU Member States, but for the whole EEA (i.e. the 28 current EU Member States, plus Norway, Iceland and Liechtenstein).

Brexit will mean that UK turnover will no longer count towards the EU turnover thresholds, so the number of transactions notified to the Commission will fall slightly. As with competition enforcement, should the UK remain in the EEA or enjoy an equivalent relationship with the remaining 27 Member States, the Commission will probably continue to evaluate the effect of the merger within the UK, negating the need for a separate UK filing. Our expectation, however, is that parallel notifications will be needed in the UK and EU.

The CMA already operates its own system of merger control, for transactions which meet the UK's domestic thresholds but not the EU's thresholds. A merger notification is, in theory, voluntary, but since the CMA can intervene and require divestments post-completion, merging parties are likely to make a notification if there is a potential impact on competition. According to the Law Society of England and Wales, based on the mergers filed with the EU in 2015, a further 50-75 cases will come under the jurisdiction of the CMA absent the Commission's one-stop-shop. Were all of these notified, this would increase the CMA's total merger control caseload by roughly 50 percent, which it would be unable to cope with at its current levels of staffing. Unlike the Commission, the CMA charges merger filing fees, of up to £160,000.

State aid

EU State aid law prohibits subsidies to businesses which distort the Single Market. The State aid rules have their origin in one of the EU's predecessor bodies, the European Coal and Steel Community, and have not been widely adopted outside the EU. Does this mean that a post-Brexit UK will dispense with State aid law? Probably not.

While there was much talk about a post-Brexit UK providing a low-tax refuge for companies, any tariff barriers between the UK and the Single Market would likely negate any corporate tax advantage gained by shifting a business' profit-making activities in Europe to a low tax, State aid-free UK. For most businesses, a comprehensive trade agreement would be needed in order for the UK to be a profitable hub to do business into the rest of Europe. However, historically, where the Member States of the Single Market have (via the EU) entered into comprehensive trade agreements with other countries, these agreements have generally included State aid-type obligations, with similar prohibitions on subsidies to businesses. For example, the Accession Agreements between the EU and the Balkan States effectively require the latter to set up domestic authorities that mirror the Commission's State aid enforcement role, while the Free Trade Agreement and Air Transport Agreement between the EU and Switzerland both contain State aid-type rules for Switzerland to follow.

The notable exception to the EU's "no comprehensive trade deal without State aid" rule is Canada's Comprehensive Economic and Trade Agreement (CETA) with the EU, which does not contain any specific state aid provisions.

Focus on Europe

Private enforcement of competition law in Europe comes of age

Private enforcement of competition law in the EU has historically been weak, with plaintiffs preferring to make complaints to the competition authorities (on the rare occasions that they took any action in the face of violations of competition law). However, in the UK over the last six months, the trend towards private enforcement has begun to gather pace.

The UK supermarket, Sainsbury's, successfully claimed last summer that the interchange fees charged by the MasterCard credit card scheme amounted to an anticompetitive agreement by effect. The Competition Appeal Tribunal (CAT), the forum where the Sainsbury's claim was heard, was only given the right to hear "standalone" competition damages actions (i.e. those not

following on directly from the decision of a competition authority) in October 2015.

The verdict turned what had been a fairly steady stream of competition claims against card schemes in the UK courts into a feeding frenzy. Even though these claimants are large sophisticated businesses, for most of them this is the first competition damages action in which they have been involved.

As well as gaining the power to hear standalone competition damages actions in October 2015, the CAT was also given new jurisdiction to hear "opt-out" class actions claiming competition damages in the UK. While the opt-out class action regime (where a person is given permission to bring a claim for every member of a particular class, regardless of whether all of those members have given their consent) is well established in the US, these reforms are the first-time opt-out class actions have been allowed for any cause of action in the UK.

An ambitious opt-out class action is being brought against MasterCard, on behalf of every resident in the UK over the age of 16 years who made purchases between 22 May 1992 and 21 June 2008. The claim is being billed as the largest ever amount claimed in the UK's courts. It is not a standalone action, but follows on from a previous Commission infringement decision against MasterCard. A hearing is being held on 18-20 January 2017 at the CAT to determine whether or not this claim can proceed.

Within the UK, the CAT has two big advantages: the waiting time between bringing a case and having it heard is shorter than in the non-specialist courts and there are no fees for bringing a CAT claim (whereas Court fees for almost every other cause of action in the UK have increased substantially in recent years). Additionally, the English Court system has other advantages over other systems within the EU, such as a disclosure system which allows claimants to retrieve extensive information from defendants to help prove their claims, and a "loser-pays" costs system which allows some (albeit, in practice, by no means all) legal fees to be recovered by the successful party.

The consensus is that, having brought successful competition claims, UK retailers may well come back for more. However, with Brexit, the position of the UK's CAT as forum of choice for EU-wide competition claims is under threat. As an EU Member State, the UK currently benefits from the Brussels Regulation on the mutual recognition and enforcement of judgments. Crucially for competition claims, which typically involve multiple purchaser-claimants and seller-defendants across several EU Member States, the Regulation allows a single action to be brought in a single Member State, to which claimants can join defendants from across the EU. The extent to which a claimant will, post-Brexit, be able to bring a claim in the UK against defendants across the EU and enforce it, is unclear.

The taxing question of State aid

The State aid ruling of the Commission against Ireland has brought the EU's State aid rules into the spotlight.

One way of attracting the ire of the Commission is to do something which the Commission believes undermines the Single Market. The Single Market is not just a free trade area or a customs union: its aim is to reduce all barriers to trade, including regulatory barriers, merging 31 national markets into one. Member States of the Single Market (the 28 EU Member States, plus the three EFTA States - Norway, Liechtenstein and Iceland) cannot raise tariff barriers to protect domestic industries from being undercut by competitors who are subsidised by foreign governments elsewhere in the Single Market.

Instead, the Commission (and EFTA Surveillance Authority for the EFTA States) enforces State aid law. This attempts to rein in subsidies which are harmful to the businesses which do not receive them and authorize others deemed to have a positive effect on the Single Market. While State aid enforcement historically targeted direct subsidies, the Commission has now turned its attention to indirect subsidies, through tax revenues forgone, enjoyed by

multinationals. In particular, it has investigated tax rulings by Member States in relation to multinational companies.

According to the Commission, 23 EU Member States make active use of tax rulings. The Commission has examined around a thousand such rulings and at the time of writing had three State aid cases into three rulings open: Amazon, McDonald's and GDF Suez Group (now Engie).

However, the Commission's ruling against Apple's tax affairs in Ireland is the case that made global headlines, in part due to the size of the repayment required. Apple's €13 billion "penalty" is a repayment, not a fine. Remedies under State aid law aim to "correct" the harm done to the Single Market, through requiring that the unlawful subsidy be repaid with interest. Even though the Irish State committed the infringement, it is first in line for this €13 billion (although the Commission has also said that the payment may have to be divided between other Member States, it has not concluded on this point).

One side effect of the Single Market is that it lends itself to a race to the bottom on taxes among Member States. As location within the Single Market is no barrier to trading with customers anywhere in the Single Market, it makes sense to establish a business' base of operations in the Member State with the lowest corporate tax rates. Member States are free to set their own corporate tax rates and to provide tax rulings to multinationals as regards the legality of their tax arrangements.

But at what point do tax rulings become a selective advantage that amounts to State aid? Or to frame the question politically rather than legally, where does a Member State's autonomy to set its own taxes end as a result of its Single Market Membership? These are questions raised by the Commission's multinational tax State aid cases.

In relation to Apple, customers purchasing from Apple in Europe, the Middle East, Africa and India did not make purchases from a local Apple subsidiary (even where buying over the counter at their local Apple Store). Instead, they purchased from one of two Apple entities incorporated in Ireland, benefitting (within the EU) from the Single Market, which allowed for the duty-free transfer of the products from the relevant Irish entity to customers. So far, so good. This is the Single Market operating as it should: businesses can establish themselves in one Member State and trade with customers in other Member States without needing to establish themselves in those other Member States.

The Commission took issue with what happened next. The Apple entities allocated their profits to their "head office", rather than to Ireland, meaning that they did not have to pay corporation taxes on their profits in Ireland but rather the location of the "head office". Thanks to a quirk in Irish tax law (now revoked) the head office did not exist and corporate taxes on the majority of the Apple entities' profits went untaxed. These structures were endorsed by several tax rulings issued by the Irish tax authorities, holding that the arrangements were compliant with Irish tax law.

The Commission decided that the Irish tax rulings endorsed what it referred to as an "artificial" internal allocation of profits, with no factual or economic justification, given that only the Irish branches (and not the head offices, which did not exist in any physical location) were capable of activities which generated income from trading.

The Commission's Apple State aid decision was only published in December 2016. Before then, there was a lot of heat, but not much light, regarding the decision. Much commentary rather missed the point. Many argued that the Commission had no business interfering in the tax affairs of sovereign States, though it is well established that it does, where those tax arrangements amount to State aid. Others have incorrectly suggested that it is Ireland's low rate of corporation tax which is under attack.

The Commission's decision is not without controversy - far from it. One key ground of appeal is likely to relate to the extent to which the Commission has relied on OECD guidance in determining that the tax rulings in Apple were effectively a sham. The Irish Government suggested both during the Commission's investigations and after the decision was reached that it is unjust to judge the Irish Government's tax rulings on Apple's tax affairs by the standards of OECD Guidelines that are non-binding and were published after the tax rulings in question were given. The Commission accepts the non-binding nature of the OECD Guidelines, but regards them as "useful guidance" for Member States in determining whether or not a "market-based outcome" has been reached by the multinational company and endorsed by the tax authority. It is, however, arguable that the Commission's decision has effectively turned the "useful guidance" into a retrospective requirement, as the Commission has used the "arm's length principle" for transfer pricing set out in the OECD Guidelines and taken the Irish authorities' failure to follow this principle as determinative of the presence of a selective advantage (and, therefore, State aid).

To cut through all of this, however, the lesson of Apple is very simple. If a Member State is offering a deal that seems too good to be true, there is a risk that the Commission (or EFTA Surveillance Authority) will rule that it was, in that it contained unlawful State aid which must be paid back. If a Member State offers a deal that appears to game the Single Market in the interests of multinational companies, the authorities will be doubly interested. Apple's tax affairs were subject to just two tax rulings in a 25-year period.

The first ruling reviewed by the Commission's decision, lasted from 1991 to 2007, during which Apple's business grew exponentially and changed from that of a niche personal computer manufacturer into a leading supplier of personal electronics (with products that would have been considered science fiction at the time of the first Commission ruling). Businesses in similar situations should take a second look at their tax arrangements in order to assess the risks.

A final word on Brexit: several commentators have suggested that Brexit will mean that the UK will be free to offer competitive corporation tax deals to multinational companies free from the State aid rules and that this will drive growth for an "independent" UK. Unfortunately, this suggestion does not stand up to scrutiny. The reason a company may incorporate in Ireland and not in a tax haven further afield is that it could use the Single Market to sell from Ireland directly to customers in other Member States without having to worry about tariff or regulatory barriers. A business in a similar position outside the Single Market and faced with tariff and non-tariff barriers would likely find that, no matter how low the rate of corporation tax in the country of incorporation, this would be outweighed by the costs of accessing the Single Market.

E-commerce inquiry by the European Commission

On September 15, 2016, the European Commission (Commission) published its Preliminary Report (the Report) on its E-Commerce Sector Inquiry, which examines market trends and potential barriers to competition in e-commerce in goods and digital content.

The nearly 300-page Report was compiled from voluntary responses to the Commission's questionnaires sent to online retailers, marketplaces, price comparison tools, payment system providers and manufacturers and, for the digital content section, digital rights holders and providers of online content services. A number of those responding supplied copies of their licensing and distribution agreements. In some cases, the responses exposed potentially anti-competitive business practices, which could lead to fines of up to 10 percent of global group turnover.

The inquiry is part of the Commission's Digital Single Market strategy, and according to the Report, aims at "obtaining an overview of the prevailing market trends, gathering evidence on potential barriers to competition linked to the growth of e-commerce and understanding the prevalence of certain, potentially restrictive, business practices and the underlying rationale for their use" in the largest e-commerce market in the world.

The Report's key findings relating to e-commerce in goods include the following:

- Online price transparency is key to supplier and consumer behavior, but there are competition risks from increased price monitoring. The Commission examined evidence of manufacturers monitoring retail prices as a first step to attempt to influence retail pricing. Some retailers use automated software to monitor competitor pricing and pressure the manufacturer to liaise with their competitors about pricing. The UK's Competition and Markets Authority recently fined online poster seller, Trod Limited, more than £160,000 for agreeing

with a competitor to price match using such software. Trod's managing director was disqualified as a company director for five years.

- Increased price competition has changed manufacturers' activities and conduct. The rise in e-commerce has led to more manufacturers competing directly with resellers and selling directly to the end consumer. As a result, manufacturers have increased their use of selective distribution systems and imposed more restrictions on retailers. Certain restrictions are justified where they preserve product quality; for instance, retailers may need to have at least one bricks and mortar store. Under the Vertical Agreements Block Exemption Regulation, where a territory has been exclusively reserved to one retailer, manufacturers are permitted to impose active sales restrictions on other retailers in the network so that they cannot target consumers in that territory. However, passive sales, where the retailer responds to a consumer's request (generally including online sales), must not be restricted.
- Bans on reselling via online marketplaces only prevent sales on one online channel. Such bans do not prohibit goods from being sold on all online channels, such as the retailer's own website, and so marketplace bans do not automatically infringe competition law. This Commission position contrasts with that of the German Federal Competition Office, which held that ASICS's restrictions on marketplace sales did constitute a hard core restriction of online sales. The question of whether marketplace bans are a hard core restriction on online sales has been referred to the European Court of Justice (ECJ) by the German Higher Regional Court in Frankfurt. In the absence of the ECJ finding that marketplace bans constitute a hard core restriction on online sales, the Commission will continue to assess such restrictions on a case-by-case basis.
- Cross-border sales in goods are not yet as common as the Commission would like, but this appears to be due to retailers' own strategies. A draft geo-blocking Regulation was proposed in May 2016 to ban blocking access to websites and automatic re-routing of cross-border consumers. If passed (likely to be in 2017), the Regulation will prevent retailers from blocking access to a website or imposing different sales terms based on a consumer's location or nationality, unless necessary to comply with a legal requirement.

The Commission says there may be further scope to investigate pricing restrictions, restrictions on online sales and territorial restrictions in relation to goods. This signals more investigation and enforcement activity by

the Commission (and national competition authorities) in this area.

The Report's key findings regarding e-commerce in digital content include the following:

- Unlike goods, geo-blocking for digital content reflects contractual restrictions. While the extent of geo-blocking varies widely across Member States and by type of digital content, almost 60 percent of digital content providers are contractually obliged to geo-block.

- Online rights are often sold on a Member State (national) basis and/or bundled with other transmission rights. Content may not be available in all Member States, and may not have the same appeal in different territories when language barriers and different consumer tastes are taken into account. In almost 80 percent of agreements, online rights are bundled with other rights, requiring a higher outlay for smaller companies, particularly online-only content providers which do not use these additional rights.

- The length of licensing agreements may also constitute a market barrier for small companies or new market entrants. More than half of licensing agreements last between 25 and 60 months, although the average duration varies with content type. Some existing content providers have bid matching rights or the right of first refusal to renew a licence. The Commission appeared to consider bid matching favourably, as it increases market transparency. The incumbent licensee can understand who its competitors are and how much its competitors are prepared to pay for content. This conclusion may surprise competition lawyers.

- Given the findings, the Commission considered it may be more appropriate to assess potential restrictions on competition arising from licensing practices on a case-by-case basis.

The final report is due to be published in the first quarter of 2017.

Big Data and social media: competition, privacy and consumer protection

Since the Commission first outlined its strategy on Big Data in 2014, Big Data has continued to rank highly on the agenda of a number of European and national regulators. A number of themes have emerged over the past few years and may be further developed in 2017.

What is Big Data?

Big Data may be broadly characterized as a large volume and variety of personal data—a record and source of information held by a company about matters like an individual's location, personal contacts and behavior. Individual users often provide access to their personal data in return for access to social media and other applications, with the recipient company using Big Data for targeted advertising, marketing and pricing. Given the personalized nature of the information, a company holding a large volume of Big Data may find itself holding a unique asset which is very hard to replicate.

Control of Big Data leading to competition concerns

EU Competition Commissioner Margrethe Vestager has suggested that the possession and control of unique data sets should be scrutinized by competition enforcement bodies to avoid companies exploiting such data to exclude their competitors from the market. This statement echoed the findings of a joint study by the national competition authorities in France and Germany, which found that data could create market power where it cannot be reproduced and if the scale of data collection is important. In such a scenario, a competitor would need the infrastructure, as well as the customer base, to create an equivalent data set.

Merger control

The Commission examined whether the acquisition of another firm's data could confer market power in Facebook's 2014 takeover of WhatsApp. The merger was cleared, with Facebook informing the Commission that it was unable to match data between a consumer's Facebook and WhatsApp accounts. But in 2016, WhatsApp announced that it would link WhatsApp phone numbers

with those held on Facebook accounts. The Commission is currently investigating whether Facebook provided incorrect or misleading information during the merger investigation. Facebook has until January 31, 2017, to respond to the Commission. The Commission could fine Facebook up to one percent of its turnover if it finds that Facebook broke the procedural rules which apply to EU merger notifications.

The interface with data privacy and consumer protection

Facebook's statement that it could not match data with WhatsApp was arguably not integral to obtaining merger clearance in 2014. The Commission stated at the time that privacy-related concerns were subject to EU data protection laws, not merger control. Nonetheless, the Facebook/WhatsApp case highlights the value of data in a merger control context. As a result, the Commission is currently consulting on whether a deal-size threshold should be introduced in merger reviews, to ensure that data-rich transactions do not escape merger scrutiny. At present, mergers are only notifiable in the EU if they meet the relevant turnover thresholds. A deal-size threshold would capture the value of technology and other companies despite the fact that they have yet to achieve significant revenues.

The European Data Protection Supervisor (EDPS) has issued an opinion stating that merger laws should protect privacy, data protection and freedom of expression. It also highlighted a broader competition risk that a dominant company could exploit consumers who do not understand the type and extent of data being collected. Where unfair terms and conditions are applied by a dominant company, the EDPS's view is that this is both a consumer protection and competition issue.

Commissioner Vestager noted in her speech on data in 2016 that less than a quarter of Europeans trust online businesses to protect their personal information, and 81 percent of individuals feel that they do not have complete control over their personal data online. While the primary responsibility lies with data protection regulators, Vestager stated that competition enforcers may be able to help resolve such consumer mistrust, by ensuring that companies compete based on the data security and privacy standards that consumers expect.

This intersection of competition and data protection law is high on the radar of a number of national competition authorities, with the German Federal Cartel Office investigating whether Facebook's terms of use in relation to user data are abusing Facebook's potentially dominant position on the market, by imposing unfair conditions on its users. Additionally, the data sharing arrangement between Facebook and WhatsApp has come under scrutiny by several regulators, showing the overlap between data protection, consumer protection and competition regulation. In the UK and Germany, the data sharing arrangement has been analyzed by data protection regulators, while the Italian Competition Authority is exercising its consumer protection powers to carry out what it terms as a "double antitrust investigation." It is examining whether WhatsApp has forced users to accept the data sharing terms and conditions by making users believe that they had to share data with Facebook to continue using the WhatsApp service. While WhatsApp's FAQs clearly state that this is not the case, sharing information was the default option when accepting the terms and conditions, and the wording used when consumers were prompted to accept the new terms and conditions was allegedly ambiguous. The Italian Competition Authority is also investigating more widely whether WhatsApp's terms and conditions are fair to consumers.

Which regulator is best placed to review the transaction?

Companies are continuing to find more innovative ways to collect and use social media data. UK car insurer Admiral briefly proposed using Facebook data to give a discount of 5-15 percent based on the prospective customer's Facebook activity, using their posts and "likes." This was quickly rejected by Facebook, and the UK Information Commissioner's Office issued a statement emphasizing the importance of treating personal information fairly, even

where it is shared on social media. Companies must ensure that consumers understand how their data is collected and used, again raising issues across competition, data privacy and consumer protection.

The nature of the regulatory investigations into Big Data shows that several national regulators can carry out investigations and take enforcement action. The EDPS suggested creating a Digital Clearing House as a network of regulatory bodies to share information about possible digital abusive conduct. Going forward, regulators will need to work together to ensure a harmonized approach to the regulation of Big Data across all areas – and they will need to be prepared to see this as an ongoing priority if they are to keep up with the speed of innovation in companies' use of Big Data.

Focus on China
Six antitrust guidelines to be issued

Since January 2016, the National Development and Reform Commission (NDRC) has been active in developing antitrust guidelines, the following of which are expected to be issued in 2017:

- *Guidelines for the Prohibition of Acts of Abusing Intellectual Property Rights*
- *Guidelines on Commitments of Business Operators in Anti-monopolistic Cases*
- *Guidelines on the Application of the Leniency Program for Horizontal Monopolistic Agreement Case*
- *Anti-Monopoly Guidelines for the Automotive Industry*
- *Guidelines on the General Conditions and Procedures for the Exemption of Monopolistic Agreements;* and

- *Guidelines on the Determination of the Illegal Income Derived from the Monopolistic Acts of Business Operators and the Determination of the Fines Thereof.*

These guidelines will provide companies with greater clarity on how China's Anti-Monopoly Law (AML) will be enforced.

Concerted practice under scrutiny

In 2016, both NDRC and the State Administration for Industry and Commerce (SAIC), the two antitrust authorities responsible for pursuing price-related antitrust violations and non-price-related violations, respectively, investigated and penalized undertakings cases for engaging in concerted practices.

In July, NDRC fined three pharmaceutical companies for reaching and implementing monopoly agreements in respect of estazolam API tablets. In this case, the three pharmaceutical companies did not conclude a written agreement to "jointly boycott" or "increase price consensually". One of the three pharmaceuticals did not even make an oral commitment to join the above conduct. However, NDRC determined that the three companies implemented a concerted practice because they had communicated their intentions and such conduct constituted a monopoly agreement. This is the first case in which a "concerted practice" has been found to be a monopoly agreement in practice, a significant development in China's antitrust enforcement practice.

In addition, SAIC also published penalty decisions on three payment chipper manufacturers for reaching and implementing monopoly agreements through a concerted practice, including allocating the sales market of payment ciphers, as well as fixing and consistently adjusting the price.

Healthcare industry and automobile industry targets of enforcement

In 2016, both the healthcare and automobile industries were targeted by NDRC for antitrust investigations.

NDRC showed its determination to probe and penalize acts of monopoly in the pharmaceutical industry through its *Circular on the Launch of a Dedicated Nationwide Review of the Pricing of Pharmaceuticals* (Drug Price Circular), as part of an investigation campaign carried out from June 1 to October 31. NDRC has already punished three companies in the healthcare industry in 2016, two of which involve pharmaceutical firms and the other medical devices. The most recent enforcement in this industry was the penalty Medtronic received in respect of a vertical monopoly agreement in December 2016. In this case, NDRC stated that it would consistently monitor the medical device industry to prevent anti-competitive conduct in the manufacture and sales of medical devices.

In addition, NDRC circulated two rounds of questionnaires to healthcare companies. As a result, many companies in the healthcare industry have been conducting increasingly intense antitrust compliance training for senior management and employees, especially for key departments like sales and retail. They have also updated their antitrust checklists and compliance manuals in accordance with the various AML developments, such as the NDRC's Drug Price Circular and the questionnaires noted above. Thorough internal reviews and investigations are being undertaken on legal documentation (including contracts and agreements) and business models. Many companies are engaging outside counsel to assist in self-reviews, particularly those companies that have received the second questionnaire as it focuses on those suspected of AML violations based on results from the first round.

AML enforcement in the auto industry has entered into a "new normal" phase in 2016. Although NDRC only investigated one case in this industry at the end of 2016, it will continue to keep a close eye on the auto sector. In addition, the Auto Guidelines, expected to be issued in 2017, are the only sector-specific guidelines drafted.

Competition initiatives: A fair competition review system

The State Council of China released the *Opinions on the Establishment of a Fair Competition Review System* in the Course of the Creation of the Market System (Opinions) on June 14, 2016. The Opinions target practices that prevent the development of a nationally-unified market with fair competition, including local protectionism, regional blockades, industry barriers, enterprise monopolies, preferential treatment in violation of laws or reductions in, or damage to, the interests of market players. They also specify the overall requirements and basic principles of the administrative review system. In addition, the Opinions clarify the scope, method, standards for, and exemptions from, the fair competition review system which is aimed at eliminating monopolistic acts by all government bodies and other organizations legally empowered to administer public affairs.

Following the Opinions, many local governments, including Jiangsu, Guangdong, Liaoning, Ningxia, and Chengdu, have circulated and published their own opinions or decisions for implementing the system. They have also established clear deadlines for evaluating and abolishing existing anti-competitive policies or regulations.

In addition, NDRC and its local counterparts published more than four cases in 2016 involving administrative monopolies in Beijing, Shanghai, Shenzhen, and another 12 provinces and cities, including Chongqing. For 2017, as the fair competition review system is rolled out, administrative monopolies should be curtailed, leading to a more competitive culture in markets in China.

Merger control: second case adopting "fix it first" approach

The Anti-Monopoly Bureau of the Ministry of Commerce (MOFCOM) has gained substantial expertise through its active enforcement and ongoing communications with its foreign counterparts. The speed of merger clearances has been greatly enhanced in recent years, especially after the introduction of the streamlined procedure for simple concentration cases in 2014. For example, MOFCOM spent an average of 24 days to clear a simple case in the first half of 2016. That said, there are still constraints on resources devoted to merger review within MOFCOM and the involvement of other agencies in the merger review process continues to delay the review process. Parties should take the notification period into account at the transaction's inception, and try to prepare complete and convincing materials as early as possible in the merger process.

In 2016, MOFCOM, the antitrust authority responsible for merger control, released the second case of MOFCOM approval using a "Fix-It-First" approach - Anheuser-Busch InBev's acquisition of SABMiller. The first case was NXP's purchase of Freescale in November 2015. For concentrations with competition concerns, parties may consider this approach to gain flexibility and reduce time pressures.

Another notable development in 2016 is that Lam Research did not proceed with its acquisition of KLA-Tencor due to antitrust concerns raised by MOFCOM. Merger control considerations should, therefore, be of key importance to multinational companies planning global acquisitions.

Revised Anti-Unfair Competition Law

In February 2016, the revised draft of PRC *Anti-Unfair Competition Law* (revised AUCL draft) was published and public opinion was solicited. In November 2016, the revised AUCL draft was passed to the Standing Committee of the National People's Congress for deliberation and a new AUCL is expected to be published in 2017.

The revised AUCL draft improves the legal definition of unfair competition, supplements the provisions relating to combating commercial bribery, strengthens the protection of business secrets and competition in the Internet field, increases civil liability compensation, and raises fines on illegal acts.

In addition, the revised AUCL draft introduces the concept of superior bargaining position, and proposes stricter requirements for strong market players. Those with greater bargaining power (in terms of funds, technologies, market access, sales channels, or procurement of raw materials) such that it is difficult for counterparties to turn to other business operators, are likely to be in a "superior bargaining position". Any unfair actions taken by such market players may fall under the scope of the AUCL, meaning they will be regulated by, and punished according to the law.

Enforcement against anti-competitive loyalty discounts

In November 2016, SAIC found Tetra Pak Group violated the AML for abusing its dominant market position in three segments of the aseptic carton package market and issued a fine of about US$97 million after a four-year investigation. In the Tetra Pak case, SAIC for the first time employed Article 17(7) of the AML—a catch-up provision to prohibit the abuse of market dominance—by determining Tetra Pak's illegal loyalty discounts as "other abusive conduct" under such provision.

For 2017, more cases involving loyalty discounts may be investigated and penalized. Undertakings need to review their discount systems and determine whether there are retroactive sales discounts and customized discounts. Further, undertakings must assess whether such discounts lead to anti-competitive effects by inducing customers to purchase a fixed amount or portion of products. If an undertaking expects to maintain such loyalty discounts, it should be able to justify the rationale.

Chinese courts have become more accustomed to SEP and antitrust suits

Since the landmark abuse of dominance case in 2011, *Huawei Technologies v. InterDigital*, courts in China have accepted roughly 80 lawsuits related to patent infringement and antitrust issues, two areas of law which have increasingly overlapped.

Several types of standard essential patents (SEP) lawsuits have been adjudicated in China. Patent holders are plaintiffs in most of the cases, including patent infringement suits in which the patentee seeks an injunction and damages against the misusers.

An ongoing case involving an SEP is Qualcomm's ongoing suit against Meizu, in which the US software firm is asking the court to rule that the terms of the licensing agreement it offered to Meizu complied with the AML and Qualcomm's fair, reasonable and non-discriminatory (FRAND) licensing obligations.

Focus on Canada

Overview

2016 was an active year for competition law enforcement and guidance. Key guidance was issued by the Competition Bureau (Bureau), Canada's antitrust enforcement agency, regarding its approach to key tech and IP issues, such as patent settlements and standards essential patents, in the Bureau's revised *Intellectual Property Enforcement Guidelines*. Furthermore, courts weighed in on long-running doctrinal debates, including whether the discoverability principle applies to private causes of action for damages under the *Competition Act*, whether umbrella purchasers (who purchase products from non-cartel members) can sue cartel members, and the Competition Tribunal broadened Canada's approach to what constitutes an abuse of dominance.

For mergers and cartels, the Bureau's most significant enforcement areas, two high-profile, cross-border mergers were abandoned because of enforcement proceedings in the US, even though in one case (Superior Plus-Canexus), the Bureau cleared the merger on the basis of efficiencies. The Bureau extracted remedies in several other mergers, including in Parkland-Pioneer, which had been the subject of an interlocutory injunction. The Bureau continued to focus on concentration in the gasoline station industry. In addition to Parkland-Pioneer, two other transactions concerning gas stations were subject to remedies. Concerning cartels, the Bureau continued to lay changes and extract guilty pleas from participants in the Québec construction industry and the auto parts industry.

Legislation and enforcement guidance

There were no significant legislative amendments in 2016. In late September, however, the Liberal government introduced Bill C-25, which, when passed, will amend the affiliation rules in the *Competition Act* (Act) to treat partnerships, trusts, sole proprietorships, and non-incorporated business entities similarly to the manner in which corporations are currently treated. These amendments were considered under the previous Conservative government alongside more controversial reforms that would have authorized the Commissioner of Competition (Commissioner) to investigate and report on price gaps between products in the US and Canada. That bill died on the order table when the federal election was called in August 2015, but Bill C-25 is expected to be passed in early 2017.

As noted above, the Bureau also released new Enforcement Guidelines regarding Intellectual Property (IPEGs). The new IPEGs replace previous guidelines that dated back to 2000. As was the case under the previous IPEGs, the Bureau will continue to apply the general provisions of the Act to conduct amounting to "something more" than the mere exercise of intellectual property rights. The revised IPEGs also offer significant new guidance regarding the Bureau's enforcement approach to product switching, patent assertion entities (or "patent trolls"), patent settlements, and standard essential patents.

Mergers

2016 was an active year for mergers in Canada, with several high-profile transactions cleared without remedies, including Shaw Communications' acquisition of WIND; Lowe's acquisition of RONA on the basis of effective remaining competition from other home improvement retailers in locations of overlap; AB InBev's acquisition of SABMiller and the divestiture of some of SABMiller brands to Molson Coors on the basis of global divestures; and Hydro One's acquisition of Great Lakes Power Transmission on the basis that the parties' transmission assets serviced different customers.

Following the abandonment of Staples' proposed acquisition of Office Depot after the FTC obtained an interim injunction prohibiting closing, the Bureau withdrew its challenge of the transaction before the Tribunal. The Bureau also cleared Superior Plus Corp.'s proposed acquisition of Canexus Corporation on the basis of efficiencies, notwithstanding a challenge by the FTC in the US on the basis that it would reduce competition in North America regarding sodium chlorate and the subsequent abandonment of the transaction by the parties.

The Bureau resolved its ongoing challenge to Parkland's acquisition of Pioneer Energy through a mediated consent agreement that saw Parkland agree to divest itself of gas stations in six local markets in Ontario and Manitoba. The Bureau also obtained remedies in numerous mergers, including from Iron Mountain regarding its acquisition of Recall, requiring Iron Mountain to divest records management assets in six cities; and from Couche-Tard regarding its acquisition of gas stations from Imperial Oil, requiring Couche-Tard to divest itself of two gas stations.

Cartels

Concerning cartels, 2016 saw further guilty pleas related to the Québec construction industry, with Chalifoux Sani Laurentides Inc. being fined CA$118,000 (with charges against its owner stayed) related to bid-rigging for sewer services, as well as Les Entreprises de ventilation Climasol Inc. fined CA$130,000 and its president CA$10,000 related to bid-rigging for a private ventilation contract.

The auto parts investigation is ongoing with Shinowa Corporation being fined CA$13 million by the Ontario Superior Court of Justice for bid-rigging related to electronic power steering gears. Nishikawa Rubber Co., Ltd., on the other hand, pled guilty and was fined US$130 million in the US related to sales in both Canada and the US, which the Bureau noted resulted from "unprecedented cooperation" with the Antitrust Division of the US Department of Justice.

Abuse of dominance

In April 2016, the Tribunal found that the Toronto Real Estate Board (TREB) had engaged in abuse of dominance by restricting access to, and use of proprietary Multiple Listing Service data, adversely affecting innovation, quality and range of real estate brokerage services in Toronto. In so doing, the Tribunal ruled that although the dominant trade association did not itself compete in the adversely affected market (in this case, real estate brokerage services in Toronto), it had a "plausible competitive interest" in it in protecting some of its members from new entrants. The Tribunal decision is currently under appeal before the Federal Court of Appeal.

The Bureau followed up on its victory against TREB by launching an application against the Vancouver Airport Authority for restricting access for the supply of in-flight catering at Vancouver International Airport, another market in which the alleged dominant firm did not compete.

In 2016, the Bureau closed its investigation into Google's online search services and its investigation into TMX Group Limited's restrictions on market data.

Litigation

In 2015, the Ontario Court of Appeal ruled in *Fanshawe College of Applied Arts and Technology v. AU Optronics* Corporation that the "discoverability" principle applied to private actions for damages based on the breach of

the cartel conspiracy provisions of the Act. The discovery principle is a common law rule which provides that a limitation period begins to run not necessarily from the defendant's conduct but from when "the material facts on which [the claim] is based have been discovered or ought to have been discovered by the plaintiff by the exercise of reasonable diligence." The appellate decision, which arose in the context of the LCD panel class action, has the potential to provide plaintiffs with more time in which to bring claims in cartel class actions.

In the same case, the court also ruled that the statutory cause of action in the Act did not foreclose the ability of the plaintiff to claim damages pursuant to tort law.

In certifying the cathode ray tube class action in *Fanshawe College of Applied Arts and Technology v. Hitachi, Ltd.*, the Ontario Superior Court of Justice held that "umbrella" purchasers (who purchased alleged cartelized products from non-defendants) had valid causes of action against the named defendants pursuant to restitutionary law.

Focus on Mexico

A reinvigorated COFECE

Although competition has been a public policy issue for more than 20 years in Mexico, the enactment of the new Economic Competition Law in 2014 invigorated the Federal Economic Competition Commission (COFECE) with new authority (including the fact that it became an autonomous agency) and breadth of activity. Since the 2014 reform, COFECE no longer has jurisdiction in the telecommunications and broadcasting industries, which are now under the purview of the Federal Institute of Telecommunications. COFECE has focused its resources on a number of other industries that impact consumers in the Mexican market, and where antitrust oversight is deemed necessary (such as food supply, drug pharmaceuticals, transportation, among others). Since 2014, COFECE investigations and sanctions have grown significantly. From January to September 2016, COFECE economic sanctions reached around US$30 million; this

amount is expected to grow in 2017. Furthermore, Mexico has moved up in the World Economic Forum's ranking of effectiveness of competition policy from 114th in 2013 to 58th in 2016, with estimated benefits to consumers in the order of US$115 million.

Like other jurisdictions, anticompetitive conduct in Mexico is defined as either absolute monopolistic practices (per se) or relative monopolistic practices (rule of reason). These practices can be sanctioned by imposing economic fines and criminal penalties on perpetrators of anticompetitive behavior. Furthermore, COFECE has the authority to investigate barriers to competition in relevant markets by imposing actions to promote effective competition (e.g. ordering the divestiture of assets or stock ownership among market participants).

Also, COFECE's leniency program is expected to grow through 2017. Since its implementation in 2006, the leniency program has permitted leniency applicants to avoid criminal sanctions and to receive substantially lower economic fines while also being an effective tool to detect cartel behavior in a number of Mexican industries.

Deregulation of the energy sector

As part of the 2014 sweeping reform of the energy sector—a main driver of the Mexican economy—private companies were allowed to participate in the entire value chain of the energy sector and state-owned, vertically-integrated monopolies in both the oil and gas, and power sectors were eliminated. Since then, COFECE has been playing a vital role in deregulating the market to ensure that effective competition conditions are in place. COFECE has issued several opinions regarding the procedure for divestiture of assets and setting the ground rules (including asymmetric regulation) relating to the assets and market share of Mexico's largest state-owned energy company, Petróleos Mexicanos (Pemex). Furthermore, COFECE has sanctioned Pemex for anticompetitive conduct, including relative monopolistic practices, such as tie-in arrangements. As such, COFECE is expected to continue to play an important role in deregulating and divesting Pemex, thereby providing opportunities for private sector participation through 2017.

Additionally, the Mexican Government has begun the liberalization of gasoline and diesel pricing to end-consumers, which is expected to be completed by the end of the year. COFECE—along with the Ministry of Finance and Public Credit, and the Energy Regulatory Commission—will monitor this process to prevent Pemex or private companies from engaging in anticompetitive conduct. Special attention will be given to price fixing and market allocation, along with mergers between market competitors. Further, COFECE has already issued opinions to local governments to eliminate restrictions on the establishment and operation of service stations to promote much-needed competition in the sector. Because of the current public outcry regarding gasoline prices, it is expected that COFECE will closely scrutinize the sector to ensure effective competition through 2017.

Cartel-like horizontal agreements under scrutiny

In 2016, COFECE commenced investigations and prosecution of cartel conduct in several sectors of the Mexican economy. These include: recent investigations of barriers to competition in the ports of Puerto Progreso; sanctions against firms in the maritime passenger transportation sector in the state of Quintana Roo; and investigation of the production, distribution, and marketing markets of pharmaceutical drugs in Mexico. These investigations and prosecutions will likely increase in Mexico, with a special focus on cartels that have already been penalized in other jurisdictions and directly affect the Mexican economy. In addition, bid-rigging in government procurement will likely be a focus for enforcement in 2017.

3. National security and foreign investment review

Focus on the US

Defense and national security

The 115th Congress will mark the first opportunity in a decade for a Republican-controlled House and Senate to work with a Republican president. In 2017, leading GOP defense and national security policymakers on Capitol Hill will work with the Trump Administration to craft legislation and conduct hearings in support of the President's key defense priorities, including:

- Developing a new approach to counter ISIS;
- Eliminating existing defense spending caps established by the Budget Control Act;
- Increasing the strength, size and readiness of the US Armed Forces;
- Improving federal cybersecurity infrastructure and capabilities; and
- Identifying efficiencies and other cost-cutting mechanisms within the Department of Defense (DoD) bureaucracy;
- Leveraging DoD innovation initiatives to foster greater collaboration with non-traditional commercial interests.

Although Senate and House Armed Services Committee Chairmen John McCain and Mac Thornberry may not be in lockstep alignment with the Trump Administration across the defense policy spectrum, enough common ground exists to provide for a productive year of legislating and oversight by their respective committees in 2017.

Building on Congressional passage of defense acquisition reform measures over the past two years, McCain and Thornberry, with cooperation from Democratic members of their respective committees, will continue to champion legislation to streamline the DoD procurement process and enhance the Department's innovation programs in an effort to, in Thornberry's words, "get better technology into the hands of the warfighter faster and more efficiently." Cybersecurity will be another major policy focal point for defense lawmakers during the 115th Congress. McCain has indicated that he intends to use his committee's oversight function in 2017 to ensure that the DoD and the Armed Forces have "the resources, personnel, and capabilities necessary to defend, deter, and respond to our adversaries in cyberspace."

Cybersecurity will also take a prominent role with respect to relations with Russia. While speculation abounds regarding how the Administration will work to "reset" the US-Russia relationship, bipartisan coalitions are already forming in the Senate to pressure the new administration to maintain the sanctions imposed in late 2016. Legislation codifying those sanctions is already circulating, and while its passage might not be certain, it serves notice on the incoming executive team that Congress intends to play a role in key foreign policy and national security areas.

In the coming year, defense lawmakers will also continue to exercise their policymaking and oversight authority over matters relating to ongoing US military activities, including in Iraq, Afghanistan, Syria and Somalia.

Additionally, the congressional Armed Services Committees will continue to focus on:

- Russia's activities along Europe's Eastern Flank and in the Middle East;
- Iran's influence and participation in ongoing conflicts in the Middle East, as well as that nation's compliance with the Joint Comprehensive Plan of Action (aka the Iran Nuclear Deal);
- North Korea's continued development of its nuclear weapons program; and
- ISIS's expansion of its global footprint, with a particular focus on the continent of Africa.

Foreign investment — national security review

Foreign direct investment will likely see policy changes early in the new Administration. The incoming Commerce Secretary's views are not clear, but the role of the Committee on Foreign Investment in the United States (CFIUS) arose during confirmation hearings. A consensus is building in both houses that CFIUS must be strengthened, both as a direct national security measure and as a quid pro quo to China's restrictions on US investment. At least two measures are already circulating to add to CFIUS jurisdiction and authority. With bipartisan support forming, CFIUS changes could include mandatory reviews of certain transactions and enhanced scrutiny of transactions involving state-owned or controlled entities.

Focus on China

Foreign investment rules and national security review

In 2016, China continued its efforts to streamline regulations regarding foreign investment. A key development in that direction was the adoption of a filing system for foreign investment enterprises (FIEs). The current regulations encourage foreign investment by creating a more favorable investment environment as well as reducing transactional costs. Based on the current climate, it is likely that the Chinese Government will continue to modify foreign investment rules to attract more FIEs into China.

The major proposed changes under the current policies and regulations are as follows:

Creation of additional Free Trade Zones

In addition to the four Free Trade Zones (FTZs) of Shanghai, Guangzhou, Shenzhen and Fujian, the Chinese Government introduced seven additional FTZs on August 31, 2016 in the cities of Liaoning, Zhejiang, Henan, Hubei, Chongqing, Shanxi and Sichuan. The purpose of the new FTZs is to attract more foreign participation in Chinese industries, to show China's openness to foreign investments and to publicize the continued evolution of China's opening up to the rest of the world. The seven additional FTZs provide foreign investors with a greater opportunity to enter the Chinese market and likely signal that the Chinese Government will take additional steps to promote free trade and amend existing trading rules.

Replacement of approval with the filing system in the FDI regulatory regime

A major milestone in 2016 was replacing an approval regime for foreign direct investment with a simplified filing regime for FIEs that fall under the scope of encouraged and permitted sectors. Four laws were amended: the Law on Sino-foreign Equity Joint Ventures (EJV Law), the Law on Sino-foreign Cooperative Joint Ventures (CJV Law), the Law on Wholly Foreign-owned Enterprises (WFOE Law) and the Law on Protection of Taiwanese Investment in Mainland China (Taiwanese Investment Law) with effect from October 1, 2016. The amendments change the processes from approval to a "record filing" with the Ministry of Commerce (MOFCOM) or its local counterparts for the establishment of a FIE or implementing any change to an FIE. This represents a significant legal development in foreign direct investment in China and is likely to trigger a major systematic reform in China's regulatory regime. .

Draft amendment to the Foreign Investment Guideline Catalogue open for public opinion

The draft new amendment to the Foreign Investment Guideline Catalogue (the Catalogue) aims to reduce market access restrictions for FIEs and was open for public comment at the end of 2016. The updated Catalogue will retain the existing list of sectors that the government has encouraged FIEs to enter as well as add new sectors. The creation of a simplified Negative List entitled "Special Administrative Measures for Foreign Investment Access (Negative List for Foreign Investment)" will replace the existing list of restricted and prohibited sectors and will list all industries that have restricted access.

National security updates in 2016

Under the 2015 Draft Foreign Investment Law (FIL), the national security review system implemented through administrative regulations in 2011 will be replaced with a new codified national security review system (NSR) as provided in Section Four of the FIL. The new NSR system would widen the scope of the review to cover any FIEs that may endanger national security in contrast with the original system implemented under the 2011 NSR system where FIEs were only subject to NSR if they had any connection to the military or national defense or they acquired a controlling interest in an enterprise in a key industry sector. Detailed regulations under the FIL are expected to be issued in the future. The new NSR system would empower the government to block foreign investments that may be contrary to national policy and such a decision would not be subject to appeal or challenge either by administrative or judicial review. While the outlook for foreign investment in China is generally positive, the Chinese Government remains focused on protecting key industries and scrutinizing foreign investments that may affect national security.

Focus on Canada

2016 witnessed a number of significant developments in Canadian foreign investment review.

Background

Canada's foreign investment review law, the *Investment Canada Act* (ICA), requires foreign investors acquiring control of a Canadian business to file either a simple notification or an application for review under a "net benefit to Canada" test. Only transactions that meet certain review thresholds are subject to pre-closing ministerial review and approval. The ICA also requires notifications when a foreign investor establishes a new Canadian business. In addition, the ICA also contains a national security screening process relating to foreign investments, irrespective of size and whether or not they involve the acquisition of a controlling interest.

Fewer "net benefit" reviews as review thresholds increase

2017 will likely see a significant increase in review thresholds under the ICA, and as a result, fewer reviews.

In its Fall Economic Statement, the Canadian Government indicated its intent to raise the review threshold for investments by foreigners in Canada to CA$1 billion in target enterprise value in 2017 – two years ahead of schedule. The review threshold determines which foreign acquisitions of control of Canadian businesses are subject to pre-closing approval by the Minister of Innovation, Science and Economic Development under the ICA's "net benefit to Canada" test.

In addition, as a result of the Canada-European Union Comprehensive Economic and Trade Agreement, the review threshold for investors from the European Union will rise to CA$1.5 billion in target enterprise value. Through most-favored-national (MFN) requirements in trade agreements, other countries including the US, Mexico and Korea will benefit from this increased threshold. The precise timing for implementation of this increase in the review threshold is not clear at this point.

National security review out of the shadows?

The national security review process was used only sparingly following its introduction in 2009 but has been invoked more frequently during the past few years. Foreign investors and their legal counsel facing these reviews have complained about the lack of transparency, predictability and scope of the process.

An example of this was a challenge by a Chinese investor, O-Net Communications Holdings Limited (O-Net), of the previous Government's rejection of its acquisition of ITF Technologies Inc. (ITF), a Québec company specializing in fiber components, modules, lasers and amplifier systems. This case also represented the first time that a Cabinet decision on national security under the *Investment Canada Act* has been litigated.

In 2015, O-Net filed an application for judicial review of the Cabinet order seeking to have it quashed on several grounds. First, O-Net claimed that its rights to procedural fairness were breached, as the order was made without providing O-Net with any insight or basis for the national security concerns or an opportunity to respond to them. Second, O-Net claimed that the order was unreasonable, as Cabinet failed to take into account relevant considerations. More than a year later, in a consent order dated November 9, 2016, the Federal Court set aside the Cabinet order that required the divestiture and ordered a "fresh" review of the investment.

The Government has not publicly stated why it has agreed to set aside the Cabinet order and undertake a "fresh review." One can speculate that there were missteps or miscommunications in the process. Alternatively, some have argued that the agreement to re-review the transaction is related to Prime Minister Trudeau's more favorable view of China than his predecessor's government. Whatever the reason, it will be interesting and particularly telling if the result of the second review is different, as it may suggest that "national security" is a more subjective and malleable concept than one might expect.

In 2016, the Canadian Government also took measures to increase the transparency of the national security review process. In August 2016, the Director of Investments at Innovation, Science and Economic Development Canada (ISED) issued the Investment Canada Act Annual Report for 2015-16 (the Report). For the first time, the Report included a discussion of the frequency and nature of national security reviews since the introduction of the national security review process in 2009. In particular, the Government noted that there have been eight reviews, seven of which resulted in Cabinet orders and one which led to a withdrawal.

In December 2016, the Government also addressed the criticism that the national security review process generated uncertainty for foreign investors by releasing guidelines on the National Security Review of Investments (Guidelines). The Guidelines outline the types of factors the Government will consider when determining if a proposed investment in Canada will be injurious to Canada's national security. These factors focus largely on traditional security concerns, including the impact of an investment on sectors such as defence, telecommunications, technology and critical infrastructure. The Government also included a few factors that could be construed broadly, for example, a transaction's effect on the supply of critical good and services to Canadians and on Canada's international relations.

The Guidelines go beyond illuminating national security considerations to include information on how to navigate the national security review process. For example, they signal the Government's willingness to engage in early consultations with investors to assess whether there are any national security concerns. This offer of early engagement is welcome as there is no formal preclearance procedure in Canada. Although for definitive reassurance that their investments will not be challenged on national security grounds, investors must await the expiry of national security review periods set out in regulations, consultation with the Government well before closing is likely to give investors some insight into whether there is a national security risk. In addition, the Government's openness to consultation may serve to allay an investor's concerns that coming forward to the Government would be regarded as an admission that an investment poses a national security threat.

These new developments in national security review are welcome. However, it remains to be seen whether investors undergoing a national security review will feel any more enlightened about the Government's national security concerns than in the past.

4. Privacy and data protection

Focus on the US

The new Federal Communications Commission (FCC) privacy rules for internet service providers (ISP) and telecommunications companies (telcos) will face an uphill battle

In a controversial ruling by the FCC on October 27, 2016, the Commission approved new privacy rules applicable to broadband and other telecommunications service providers that establish a new framework for the collection, use, and protection of customer information. The new rules afford special protection to sensitive "customer proprietary information" (or "customer PI") which includes data elements such as precise geo-location, health, financial and children's information; Social Security numbers; content; call history; and web browsing and application usage histories and their functional equivalents. Such sensitive customer PI now requires "express informed consent" (e.g., opt-in approval) from customers if the provider intends to share or use this information. The FCC has called the Order "sensitivity-based" because all other customer PI is considered non-sensitive and subject to customer opt-outs. The Order also expands the scope of providers' reporting obligations for data breaches, now requiring providers to notify affected customers of any breach "without unreasonable delay and no later than 30 calendar days after it reasonably determines that a breach has occurred, subject to law enforcement needs."

Several industry groups have filed petitions for reconsideration of these new rules, including NCTA-The Internet & Television Association, the American Cable Association, and CTIA-The Wireless Association, arguing, *inter alia*, that the FCC erroneously relied on its authority pursuit to Section 222 of the *Communications Act* in establishing these new rules, as Section 222 governs telephony services only. With an incoming GOP administration, the fate of the FCC's Order is tenuous at best, with some experts reasoning that the GOP could use the pending petitions as a basis to reverse course and repeal the new rules. Added to the opposition of numerous industry groups, members of the new administration have also voiced widespread opposition to the Order, further jeopardizing the future of the new privacy rules.

Focus on Europe

Legislative reform picks up steam

The European General Data Protection Regulation (GDPR) comes into effect in EU Member States on May 25, 2018. The UK government has confirmed that the GDPR will apply in the UK on commencement, as Brexit will not yet have taken place. The UK Government has also confirmed that primary and secondary legislation will be brought in to implement the GDPR (*e.g.*, for interaction with the existing *Data Protection Act 1998* (DPA) and to cover Member State discretion, such as children's consent).

It remains unclear as to how the GDPR will apply after Brexit. From a practical perspective, aligning UK law with the GDPR seems sensible, as the UK will need to ensure compliance if it wants to continue trade with the European Economic Area. The UK Information Commissioner's Office (ICO) has released the following guidance on the GDPR: overview of the GDPR, privacy notices and 12 steps to take now.

The European Network and Information Security Directive (NISD) came into force in 2016 and must be implemented by EU Member States into national law by May 2018. The NISD imposes new cybersecurity obligations in respect of critical national infrastructure. The NISD also introduces breach reporting obligations for "operators of essential services" (organizations operating in the electricity, oil, gas, air transport, rail, water transport, road and bank sectors) and "digital service providers" (online marketplaces, online search engines and cloud computing services).

Again, it is not clear as to how Brexit will affect NISD. However, the ICO has previously interpreted security requirements under the DPA to apply to cyberspace, and the UK Government has also confirmed that cybersecurity "must be part of" data protection.

Accordingly, it is likely that NISD will in any event be implemented into national law.

Proposed e-Privacy EU Regulation – more red tape or the necessary alignment with the new EU data protection rules?

The e-Privacy EU Directive (2002/58/EC, further amended in 2009) applies to processing electronic communications data carried over public networks (largely to telecommunications providers and ISPs but also includes provisions on cookies, electronic marketing and notification of data breaches). It aims to ensure the free flow of data in the EU, and the protection of privacy and confidentiality in electronic communications. Along with the Personal Data Protection Directive (95/46/EC), it constitutes the data protection framework in the EU.

With the Personal Data Protection Directive being replaced by the EU General Data Protection Regulation (GDPR), effective as of May 2018, the European Commission decided that the e-Privacy legislation must be adopted to align it with the new rules, and as a result, on January 10, the EC proposed a new E-Privacy Regulation. This regulation is to replace the e-Privacy Directive and will become one set of rules applicable directly across the EU member states at the same day as the GDPR, i.e., on May 25, 2018. The aim of the new rules is to ensure consistency in data protection and to align and complement the general rules laid down in the GDPR. The key proposed changes include:

- As with the GDPR, broadening the territorial scope and application to data processed in servers outside the EU to end-users inside the EU;
- Expansion to the over-the-top services providers (OTT) which offer online communication services and are not currently subject to the provisions of the e-Privacy Directive (e.g. WhatsApp, Facebook Messenger, Skype);
- Covering machine-to-machine communication, if the information exchanged is classified as personal;
- Expanding coverage to include metadata which, due to technological developments, has a strong privacy component (e.g., time and location of communication), including the need to have end-user consent to process such data (unless needed for billing) and the conditions to receive consent are the same as in the GDPR;
- More user friendly rules on cookies, including using the appropriate technical setting to express consent and the need to periodically (i.e., every six months) send reminders on the right to withdraw consent;
- Revised spam regulations, including the obligation to display the phone number or specific prefix identifying the unsolicited marketing communication; and
- High financial sanctions of up to €20 million or four percent of the total worldwide annual turnover.

As in the case of the GDPR, industry lobbying against the proposal is fierce with repeated calls to simply repeal the e-Privacy Directive and to rely on the GDPR without the need to adopt any specific rules for the industry. The reasoning is that the stronger rules would jeopardize the harmonization ensured by the GDPR and would adversely affect data-driven revenue of online media. Unsurprisingly, social advocacy organizations praise the proposal and warn that the lack of rules in the e-communications sector would negatively impact the privacy of users, expose them to abusive tracking and intrusive behavioral advertising.

Germany

The path to GDPR implementation is not straightforward

In August 2016, the German Federal Ministry of the Interior (FMI) had submitted a draft bill for an implementation law which takes advantage of the regulatory scope given by the EU-General Data Protection Regulation (GDPR). The bill was met with criticism from several parties, including from the Federal Data Protection Office and the Federal Ministry of Justice and Consumer Protection. Due to the criticisms, a newly revised bill was drafted and published in November 2016.

The newly redrafted Federal Protection Data Act (BDSG-E) deals in particular with the following key elements:

i. Restrictions on information duties: The BDSG-E intends to restrict the information rights given in Article 13 (information that must be provided when collecting personal data from the data subject) and Article 14 (information that must be provided when collecting from a third party) of the GDPR. According to the FMI's draft, the company's obligations within the meaning of Article 13 of the GDPR are to be abolished.

ii. Data protection officers: Section 36 of the BDSG-E places a general obligation on companies to appoint a data protection officer, should the company permanently employ at least 10 persons to process personal data.

iii. Administrative fines for infringements: BDSG-E intends to introduce a threshold for fines of up to €300,000 in regards to any natural person (e.g. employee) who breaches the provisions of the GDPR whilst exercising his/her duties on behalf of the controller/processor.

The proposed bill by the FMI is complex and does not seem to be wholly in line with the GDPR. Although the FMI had attempted to strengthen the economy by providing numerous exceptions to companies' information obligations, given that many of the provisions potentially contradict the GDPR, its aim may not have been achieved.

Regarding the implementation of new data protection processes, German companies now have to decide whether to follow the provisions laid out in the GDPR or the BDSG-E.

The revised bill has now been forwarded and will be discussed in cabinet this January 2017.

Focus on China

Rapid changes as China moves on cybersecurity and data protection

On November 7, 2016, the *Cybersecurity Law of the People's Republic of China* (Cybersecurity Law) was adopted by vote at the 24th Session of the Standing Committee of the Twelfth National People's Congress (24th SC of the NPC). The Cybersecurity Law will come into force on June 1, 2017.

The Cybersecurity Law is a fundamental national law containing comprehensive provisions regarding the protection of personal information. Consistent with international standards, Article 41(1) provides that, "when collecting or using personal information, internet operators shall comply with the principles of legality, justification and necessity, make public the rules for the collection and use,

clearly indicate the purposes, methods and scope of the information collection and use, and obtain the consent from the data subjects." Article 44 provides that, "no individuals or organizations may steal or otherwise illegally obtain personal information, or illegally sell or provide personal information to others."

In addition, the Cybersecurity Law stipulates restrictions on cross-border transfer of Critical Infrastructure Information (CII) for the first time, which may present greater challenges for both domestic enterprises and multi-national companies operating in China and engaging in the cross-border transfer of data. The restriction only applies to operators of CII in China. Personal information and crucial data collected and generated in operations in China are not permitted to be stored or transferred overseas. If it is truly necessary for a business to transfer CII overseas, a security assessment must be conducted in accordance with measures to be further elaborated by relevant departments of the State Council. At present, the identification of CII operators, the definition of crucial data, the criteria for determining the business necessity for transfer of CII overseas as well as the security assessment procedures, among other things, remain to be interpreted or specified by relevant departments. Enterprises should focus closely on the evolving legislative developments of supporting regulations.

On December 27, 2016, the *Third Draft of General Rules of the Civil Law* (Third Draft of GRCL) was published on NPC's website for public comments. The legislative procedure of the GRCL is soon to be completed after three deliberative sessions of the SC of the NPC. The Third Draft of GRCL provides that "personal information of a natural person shall be protected by law. No organizations or individuals may illegally collect, use, process or transfer personal information, or illegally provide, make public or sell personal information". If enacted, the protection of personal information will be a basic right in the Civil Law for the first time.

On December 27, 2016, the *Draft of Electronic Commerce Law* (Draft ECL) was published for public comments on NPC's website for the first time. The law contains provisions on collection, processing, sharing, access and deletion of e-commerce data. Such provisions basically follow internationally recognized principles on data protection. Article 45 states that e-commerce users have the right to make independent decisions on their own personal information.

It is noteworthy that the Draft ECL provides that e-commerce operators must not compel users to agree to their collection, processing and employment of personal information by threatening to refuse to provide services to such users. In addition, prior consent must be obtained if e-commerce operators want to modify their privacy policies and remedies shall be provided if the users do not agree to such amendment. At present,

the privacy policies of many e-commerce enterprises would not be compliant with this new law. It is advisable that e-commerce operators revise or develop their privacy policies in accordance with the new law since it is expected to be formally issued next year. The maximum fine to be levied for violation of such provisions is RMB500,000. Furthermore, a company's business license may be revoked.

On September 30, 2016, the Cyberspace Administration of China (CAC), which is in charge of guiding and supervising the relevant departments to strengthen the management of internet information content, investigating and punishing related violations, issued the *Draft of Regulations on Protection of Child Internet Users* (Draft Regulations). The first round of public comments was completed on October 31, 2016. The Draft Regulations provide that any collection or employment of children's personal information by internet must be marked with warning signs in a clearly visible position, indicating the source, content and purpose of the information collected, with the consent of the child or its guardian." In addition, a specific privacy policy for children must be developed, which proposes a higher standard for protecting children's personal information collected and used through the internet.

Focus on Canada

Eyes on Europe while preparing for mandatory breach reporting

2017 brings us closer to three legal developments that require accommodation for all businesses holding personal information: the coming into force of the *Digital Privacy Act* provisions on mandatory breach notification; the approaching date of May 25, 2018 when the sweeping changes of the *General Data Protection Regulation* (GDPR) will come into force in Europe and will also apply to non-European organizations that offer goods and services in Europe; and the announced amendments to the *Anti-terrorism Act*.

With respect to Mandatory Breach Notification, regulations are being finalized based on wide ranging consultations and will specify modalities of application. Still, at this point, the adopted legal provisions which will amend the *Personal Information Protection and Electronic Documents Act* point to the following measures that should be undertaken now:

- Organizations should have clear criteria to exercise their discretion to assess when a breach "*creates a real risk of significant harm*" and therefore is subject to notification;
- Organizations should also have a clear decision-tree to establish who will decide whether to notify.

With the GDPR, privacy requirements are more stringent, for example with respect to consent and privacy governance, or unprecedented, for example with the "right to be forgotten" and the right to data "portability" – to name but a few, all requiring corresponding changes to internal polices in Canadian organizations. The GDPR may also bring into question Canada's "adequacy status" to receive personal data from Europe. On that front, it is the Government of Canada that is on the hot seat on behalf of Canadian business to ensure Canadian law is amended, as needed, to correspond to the new level of requirements.

Amendments to the *Anti-terrorism Act* are viewed with trepidation, amidst an unresolved debate on the role of businesses in relation to law enforcement authorities: what are their obligations to State and customer?

Focus on Mexico

As Mexico's legal framework continues to evolve to fight more effectively organized crime and corruption, concerns have been raised about the potential effects that such efforts will have on the protection of personal data privacy. Most notably, under the Federal Telecommunications and Broadcasting Law (the Telecom Law or *Ley Federal de Telecomunicaciones y Rafiodifusión*)—enacted with the recent package of structural reforms aimed at transforming

Mexico's economic landscape—security surveillance regulations under the Federal Law have raised doubts about the protection of personal data privacy.

The Telecom Law includes a chapter that regulates the obligations of telecommunications companies, requires them to cooperate with governmental agencies entrusted with duties of national security and crime prevention. For instance, mobile phone carriers are required to produce and make available upon government request, detailed records on, among other items:

- The real time geolocation of mobile phones and other devices served by them;
- Communications rendered and received by those phones and other devices, at a level of detail that allows governmental agencies to identify accurately the user by name—or corporate name—and domicile, and the technical specs of the phone, including international fabrication codes; and
- The type of communication (e.g. live voice, recorded voice, messaging or multimedia, supplementary services employed), as well as other specifics commonly known as surveillance metadata, including time, place, origin, destination, duration and location of the transmission.

Telecommunications carriers must respond to a government agency's request within 24 hours. Moreover, the statute allows government agencies to request the contents of the communications, provided they have obtained a judicial order to that effect.

Not surprisingly, the ability of the government to request this information has been questioned by data protection civil organizations, which argue that these requests contravene privacy and data protection principles embodied in the Mexican Constitution. In that regard, the Supreme Court of Justice set an important precedent last year by resolving an *amparo* action—a federal judicial remedy akin to a writ of *mandamus or habeas corpus*—challenging the constitutionality of the relevant legal provisions. The judgment was mostly favorable to surveillance authorities as it validated the carrier companies' obligation to maintain metadata records for two years (contrary to the decision rendered by the European Court of Justice in 2014), and to provide geolocation information without requiring a judicial order. However, the Supreme Court also stated that government requests for metadata are subject to judicial order (as are the contents of the communication), thereby clarifying an uncertainty in the law.

In this context, we expect that 2017 will, once again, establish new precedents on the relationship between surveillance and data privacy, as civil organizations have made public their intention to continue legal challenges before international courts. In addition, it is expected that the draft of the new General Law to Protect Personal Data Possessed by Agencies (*Ley General de Protección de Datos Personales en Posesión Sujetos Obligados*) that was approved by the Senate in 2016, will continue towards legislative enactment and thereby broaden the data privacy legal framework.

Focus on Colombia:

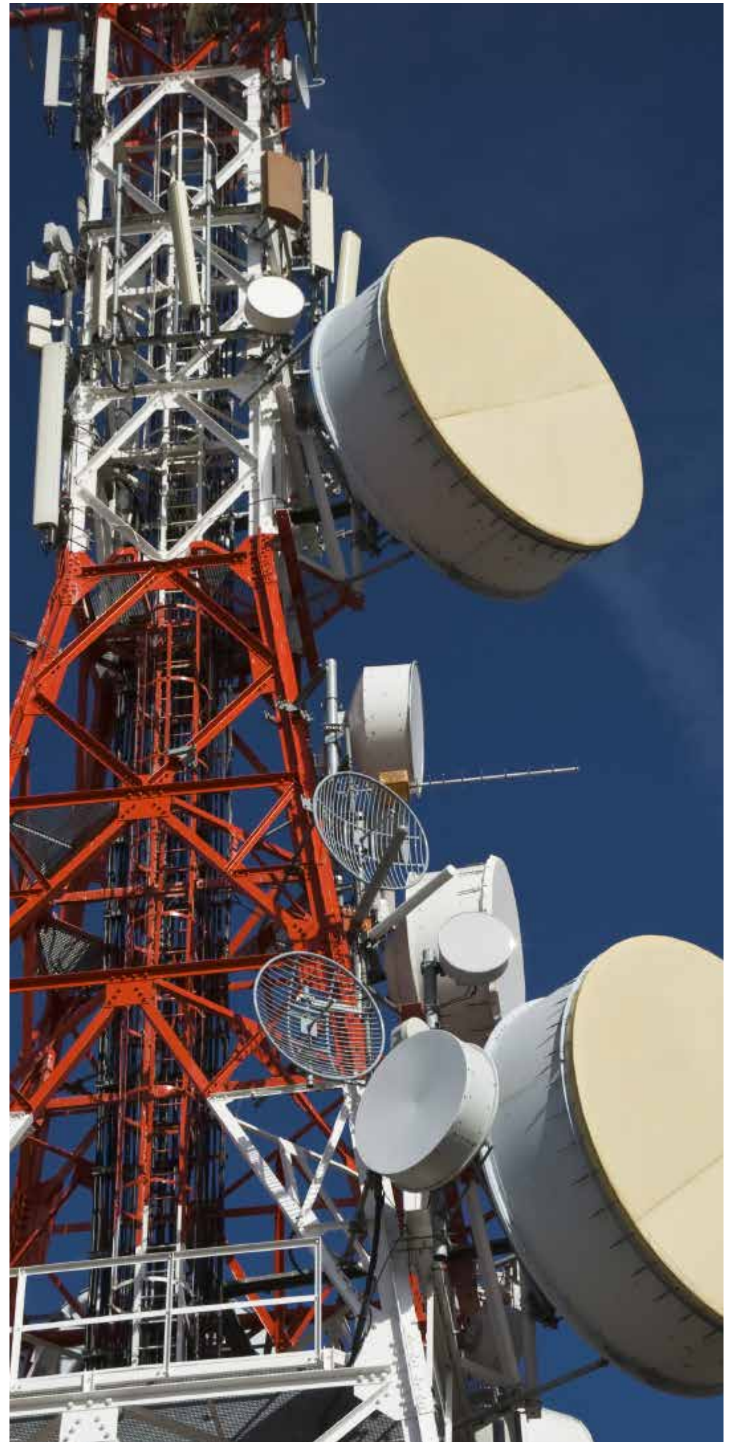
Extended and expanded powers to regulate data processors

In Colombia, three specific regulations relating to privacy are significant: Bill No. 91 of 2016, Decree 1079 of 2017 and the Guidelines on declarations on conformity.

First, in August 2016, the Colombian Congress presented Bill No. 91, which seeks to extend the jurisdiction of the Colombian Privacy Law as well as the competence of the Colombian authorities. The authorities would be entitled to carry out investigations or any legal action, ex officio or upon request, against natural or legal persons located outside Colombian territory which process personal data. On October 26, 2016, the Bill was approved in first debate, by the first commission of the Senate.

Second, in October 2016, the Colombian data protection authority (Superintendence of Industry and Commerce) published a guide that establishes parameters for any natural and/or legal person seeking a declaration of conformity for the international transfer of personal data. Accordingly, those requesting a declaration must provide information such as: (i)The name and purpose of the personal databases that will be the subject of the international transfer, as well as a description of the processing; (ii) A copy of the contract, agreement or document explaining the conditions of the transfer and the security and confidentiality measures that will be implemented for the protection of the personal information; (iii) A copy of the regulations regarding the protection of personal data of the country to which the information will be transferred, among other information.

Finally, in November 8, 2016, the Ministry of Commerce, Industry and Tourism issued Decree 1759, which extended the registration deadline in the National Registry of Databases. Consequently, all private sector entities and semi-public entities registered in the chambers of commerce of the country, must register their databases before June 30, 2017. Moreover, natural persons, public sector entities and private entities that are not registered in the chambers of commerce, must register their databases no later than June 30, 2018.



5. Economic sanctions and trade

Focus on the US

Trade

International trade was a significant issue during the presidential campaign and one which President Trump returned to often on the trail. First, he promised that trade agreements would come under much greater scrutiny in his administration and that trade enforcement efforts would increase. He has already pulled out of the Trans-Pacific Partnership (TPP) Agreement and plans to renegotiate the North America Free Trade Agreement (NAFTA). His inaugural remarks presage an "America First" strategy that is likely to have meaningful ramifications in the trade arena. His proposed appointment of John Lighthizer, a free-trade critic, further signals the President's intent to address what were described during the campaign as imbalances in US trade. Lighthizer has endorsed limiting free trade where needed to protect domestic industries. Both during his prior tenure in the Reagan Administration, and in private practice thereafter, he worked to provide protection for US industries under siege from open trade policies. His appointment ties in directly with that of proposed Commerce Secretary Wilbur Ross, who has both promoted and used trade remedies and trade restrictions to help insulate businesses he owns (first steel, then textiles).

The trade team that President Trump has assembled will likely develop a clear and coordinated strategy of revisiting existing agreements that they believe do not afford adequate quid pro quo protections for US industries, and using non-trade strategies to accomplish those means as well. In particular, President Trump's team is likely to take an aggressive stance regarding China's currency actions, and its desire to be reclassified as a market economy in the WTO.

TPP

On January 23, 2017, President Trump signed an executive order withdrawing the United States from the TPP. While the US had signed an agreement signifying its intention to implement the TPP Agreement, it had not been sent to Congress and had not been ratified by the required number of countries for it to go into effect. With significant Democratic and Republican congressional opposition, passage of the TPP, while supported by many in the business community, was never a foregone conclusion, so withdrawing from it will have little or no immediate impact on the US economy. The bigger issue with TPP is what happens next. The remaining eleven countries may ratify the Agreement without the United States. Alternatively, smaller subgroups—some involving China—may form. There will be future Pacific Rim trade agreements and the issue will be whether the US is part of those negotiations. To counter China's attempts to exploit discontent arising from the US rejection of the Agreement, the Trump Administration may launch an assertive agenda of bilateral agreements, or look for alternative strategies to keep China's influence at bay. China's desire to move these countries away from close relationships with the US will have to play a role in how the Administration approaches these trade issues, which are integrally intertwined with important national security concerns.

NAFTA

President Trump spent much of his time on the campaign trail, especially in the Midwestern "rust belt" states, expressing his dissatisfaction with NAFTA. He promised that his administration would renegotiate NAFTA to make it a better deal for US businesses and employees. While it is certainly an option for him to sign an executive order right away withdrawing from NAFTA, which would cause significant problems because many business models—including the location of manufacturing facilities—have been designed with the understanding that NAFTA would remain in force. Withdrawing suddenly from NAFTA would disrupt supply chains and could put manufacturers located in North America at a disadvantage compared to foreign producers, particularly those from China. In addition, withdrawal from NAFTA would require Congress to pass legislation to address the implementing statutes it put in place after NAFTA was signed and ratified. Already, both the Mexican and Canadian governments have agreed to reopen the NAFTA negotiations and have indicated the

priority issues that they would want to discuss. Given that his campaign pledge was to renegotiate NAFTA to obtain better terms for the US (with the threat to withdraw if Mexico and Canada refused to renegotiate), President Trump may focus his early discussions on identifying areas for renegotiation with Mexico and Canada.

Other trade priorities

As to other positions taken by President Trump, such as a 45 percent tariff on goods from China, there is a good chance that the new administration will ultimately back off. Imposing an across-the-board tariff increase—apart from its questionable legality—would be a disproportionate response, like using an axe where only a scalpel is needed, as many products imported from China are not produced in the United States and the additional tariff would simply be a large tax increase on American consumers. That said, the focus on China will not go away. The more likely policy approach would be the use of existing trade laws to protect sensitive industries such as steel. There is already discussion of a Section 201 petition for import relief involving steel, and a similar action to address issues of overcapacity in aluminum could also be taken. Overall, the Trump Administration could turn out to be more focused on managed trade as opposed to the traditional Republican free trade position. A key issue for the new administration will be whether—given competing demands on the public purse—they can target sufficient resources to the issue of enforcement. The best trade agreement with the strongest enforcement mechanisms is ineffective without the manpower and resources to carry out their mission.

Focus on Canada

Trade agreements

Canada's trade policy priorities will largely be driven by the Trump Administration's actions with respect to NAFTA. While there are indications that Canada is diversifying its trading patterns, with Asia and Europe taking an increasing share of merchandise trade, the US still purchases approximately 75 percent of all Canadian exports. Getting the relationship right with the Trump administration and preserving the crucial advantages of NAFTA is mission critical for the Canadian economy.

The Trump Administration has not specifically targeted Canada in its statements concerning the need to review NAFTA. However, the incoming administration repeats that its priority and focus will be in repatriating manufacturing jobs to the US. Canada will need to work hard to remind US decision-makers of the highly integrated nature of Canada-US supply chains and of the benefits of NAFTA for both countries.

As a trading nation highly dependent on predictable access to foreign markets, Canada is particularly vulnerable to the backlash against globalization that was exemplified in 2016 by the Brexit vote, the difficulties in securing ratifications of the Canada Europe Comprehensive Economic and Trade Agreement (CETA) and the US election. The UK is the main entry point for Canadian investment in the EU and Canada's third largest trading partner (after the US and China). But the terms of the UK's exit from the EU, and its impact on the CETA, remain uncertain and are unlikely to be settled in 2017. This presents continuing risks for Canadian traders and investors, and major challenges for policymakers.

With the Trans-Pacific Partnership Agreement likely to fold, and with US – EU free trade talks likely suspended by the Trump Administration, the anticipated landscape for Canadian traders has shifted significantly. This presents some risks but, on the bright side, the successful conclusion of the Canada – EU CETA may present significant competitive advantages for Canadian traders and investors.

Sanctions

The Trump Administration's approach to sanctions is also likely to have a major impact in Canada. If US sanctions on Iran and Russia are radically changed, will Canadian sanctions also be modified or will sanctions imposed by Western allies increasingly diverge? If sanctions become

very different from one country to the next, this will have a significant effect on the risks and opportunities faced by Canadian companies in competing for a share of Russian and Iranian business. To date, Canada has signaled that it has no intention of relaxing Russian sanctions or of tightening sanctions against Iran. However, Canada may need to qualify this approach as developments unfold in the US.

Trade disputes

Often referred to as the biggest trade dispute on the planet, the softwood lumber wars with the US were reignited in 2016 with the filing of a fresh petition targeting lumber exports from Canada to the US. This dispute will work its way through the US anti-dumping and countervailing duty process in the US and will continue to be a major irritant in the Canada-US relationship. Unless the US and Canada can come to a new agreement to manage lumber trade (the prospect of which currently seems remote), it is likely that the US legal process will sprout fresh cases before NAFTA Chapter 19 and WTO Dispute Settlement Body panels. In the interim, US importers of Canadian lumber will likely start paying new countervailing duties in February 2017, and anti-dumping duties in May 2017.

In the last several years, there has been a steady stream of Canadian anti-dumping and countervailing duty cases filed, particularly in relation to imported steel products, with China being the most frequent target of these investigations. This trend is likely to continue in 2017 with a fairly busy docket of new cases and various reviews of existing measures working their way through the Canada Border Services Agency and the Canadian International Trade Tribunal.

6. Anti-corruption

Focus on the US

Anti-corruption enforcement in the United States has changed dramatically in the past year and its future remains unclear. What direction will Attorney General Jeff Sessions take the US Department of Justice (DOJ) on anti-corruption enforcement is the overarching question, but there are many more worth considering. Will Sessions' unnamed lieutenants continue the aggressive cooperation credit requirements outlined in the Yates Memorandum and administration of self-disclosures under the DOJ Foreign Corrupt Practice Act (FCPA) Pilot Program? Will there continue to be a growing number of books and records actions brought by the US Securities and Exchange Commission (SEC)? Finally, do the enormous settlements at the end of 2016 reflect a clearing of the enforcement pipeline, or are there a number of matters being worked up toward completion in 2017?

A new team takes over at DOJ and the SEC

First, it's worth noting that Senator Sessions' confirmation hearing testimony on January 10 and 11, 2017, may have answered one of the questions regarding whether he would continue current enforcement policies and strategies. Sessions' testimony was generally supportive of ongoing DOJ's efforts to hold individual wrongdoers accountable; however, his testimony did not provide specific support for ongoing FCPA enforcement strategies, and the DOJ policies targeting individual conduct that was laid out in the Yates Memorandum. It also bears mentioning that Senator Sessions is no stranger to the prosecution of bribery conduct. In his United States Senate Judiciary Committee Questionnaire responses, Senator Sessions highlighted a case that focused on bribery as one of the most significant litigated matters that he personally handled. Although United States v. William Broadus et al. did not involve the Foreign Corrupt Practices Act, it was described by Sessions as "the most significant corruption case involving the criminal justice system" in the district where he served first as Assistant United States Attorney and later as the United States Attorney.

Second, the Attorney General and the Trump administration will have to identify and win confirmation for several key FCPA enforcement leadership positions at the DOJ, including the Deputy Attorney General and the Assistant Attorney General responsible for the Criminal Division. The same will be true at the SEC, where the President has nominated Jay Clayton to succeed Mary Jo White as the SEC Chairman, but still needs to name a Head of Enforcement. Until we see which nominees successfully come through the confirmation process, it will be hard to predict which current policies and approaches will be adopted by the new administration. Clayton's past criticism of the enforcement of anti-bribery actions against US business organizations may result in the SEC reducing some of its recent high profile efforts to the DOJ. Given the relative successes of recent enforcement actions, it makes sense to assume those approaches will still be in place over the next year and to consider the legal risk they generate for global business operations until either organization announces a change in their anti-bribery laws.

The DOJ's Yates Memorandum changed the fundamentals for internal investigations

Given the mood and sentiment behind the 2016 national election, it seems unlikely that the incoming leadership team will drop the DOJ's attempt to generate greater individual accountability for violations of federal statutes through fairly new policies. In 2015, the publication of the Yates Memorandum ushered in a new era for how attorneys should successfully handle corporate internal investigations, including those where allegations of Foreign Corrupt Practices Act violations have been made. At the outset, the Yates Memorandum dramatically changed the way in which investigations are conducted by pressuring corporations and their counsel to prospectively assist with the effort to hold individual wrongdoers accountable. The most notable portion of the memorandum for legal counsel representing business organizations was the following: "[I]n order to qualify for any cooperation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct." Now, in order to receive cooperation credit,

companies have to disclose any employee wrongdoing regardless of status or title. This credit remains one of the key factors in the DOJ's charging decision and when relevant, the amount of monetary risk the organization faces to resolve its ongoing investigation.

The government's focus on individual prosecutions, and leveraging of corporate self-disclosures to get there, is not likely to dwindle in 2017. At the December 2016 International Conference on the Foreign Corrupt Practices Act, the DOJ Deputy Attorney General Yates and then-SEC Enforcement Director Andrew Ceresny both gave speeches that emphasized prosecuting individual wrongdoing and persuading companies to self-disclose. Yates noted that the DOJ is "pleased with what [they have] accomplished in focusing on individual actors and that "...we cannot forget that behind every bribe and illegal payment is one or more individuals who knew what they were doing was wrong and nonetheless broke the law.... As I've seen over and over again during my career, the best way to deter individual conduct is the threat of going to jail. That's what truly changes behavior."

As evidence of the SEC's commitment to hold individuals accountable, Ceresny highlighted its recent settlement with Och-Ziff Capital Management. The hedge fund agreed to pay close to US$413 million in fines to the SEC and the DOJ, while CEO Daniel Och agreed to pay US$2.2 million to the SEC—reportedly the largest SEC settlement amount by an individual in FCPA history—and CFO Joel M. Frank settled civil charges, with a penalty to be assessed at a future date. "This case sends the message loud and clear that CEOs will be held responsible if they do business with persons with close ties to government officials when due diligence raises significant red flags," Ceresney said. "It is only by holding such senior decision-makers responsible that we will deter such conduct." During his speech, Ceresney also pointed to the fact that the SEC has chosen not to bring an action against a company that had self-reported as a concrete example of the tangible benefits that self-reporting and cooperation can bring.

What the leadership of both the DOJ and SEC has made clear is that individual prosecutions of FCPA violations are likely only to increase in the coming months and years as cases currently under investigation make their way through the pipeline. Yates commented that "[i]t won't be every case, but the investments we're making now are likely to yield a real increase in the years ahead."

While the Yates Memorandum laid out "six key steps" for how to best pursue individual wrongdoers, it left many practitioners with more questions than answers. Over the past two years, however, the DOJ and SEC continue to reveal insights on how to effectively and successfully conduct a FCPA investigation. Regardless of these insights into what actually constitutes sufficient cooperation in the eyes of the enforcement authorities, the principal challenges that remain for the corporation's lawyers in a post-Yates world are the legal and ethical issues the policy triggers. Foremost among these are "who is my client" and "what are my legal and ethical responsibilities to that client in light of the Yates Memorandum".

The future of the DOJ's FCPA Pilot Program is less clear

In April of last year, the DOJ implemented a new one-year FCPA Pilot Program, aimed at encouraging voluntary self-disclosure, cooperation and remediation. In exchange for self-disclosure, the DOJ offers the possibility of a so-called "declination" of prosecution (which traditionally means that although a crime has been committed, the DOJ will not prosecute it), up to 50 percent reduction in criminal fines and the avoidance of an appointed compliance monitor. In line with the Yates Memorandum, the Pilot Program requires disclosure of all relevant facts regarding individuals involved in the misconduct, including the company's former and current officers, employees and agents.

While the idea of reduced fines or even a declination in return for self-disclosure, cooperation and remediation is not new, the Pilot Program seeks to provide a more detailed framework for describing the potential amount

of fine reduction, which is potentially a useful tool for companies to evaluate whether to self-disclose or not. Generally, the Pilot Program aims to provide more transparency in how the DOJ will treat companies that self-disclose but ultimately the success of the program lies in how the DOJ applies it. It remains to be seen how the program will affect corporate disclosures generally, and with respect to individual cases, whether the DOJ will apply the guidelines in a manner that provides more certainty to self-disclosing companies.

In June of 2016, the government announced the first two prosecutorial declinations under the Pilot Program. Both cases involved allegations that the company's Chinese subsidiary had engaged in bribery. Employees at Akamai's Chinese subsidiary allegedly provided US$40,000 in improper gift cards, meals and entertainment to officials at state-owned entities to build business relationships. Nortek's Chinese subsidiary allegedly made improper payments and gifts to Chinese officials totaling US$291,000 to influence regulatory actions and fines, according to the SEC.

International cooperation on anti-corruption appears to be locked in

Another critical component of FCPA enforcement that the DOJ and SEC leadership forecasted for 2017 is the continued increase in international cooperation between US and foreign authorities. At the same December 2016 conference noted earlier, Ceresney reinforced the strides the SEC Enforcement has made over the last few years in international cooperation. He noted that increased collaboration with international regulators and law enforcement has been pivotal to the SEC's success in the FCPA space, remarking that "[a] s global markets become more interconnected and complex, no one country or agency can effectively fight bribery and corruption alone." Ceresney highlighted the global investigations of VimpelCom and Embraer, both of which resulted in charges brought by the SEC and DOJ in the US, and by authorities in the Netherlands and Brazil, respectively, as two recent examples of successful cooperation between international authorities. According to Ceresney, such cooperation and coordinated global resolutions send strong messages of deterrence to companies and individuals.

Our Firm's lawyers representing clients in investigations involving conduct outside of the US repeatedly experience closer levels of governmental cooperation between the countries where the alleged conduct took place and the United States. This increasing trend puts a premium on legal counsel that places due consideration on the requirements of all applicable global laws, legal privileges and local cultures.

Conclusion

Unless a radical shift in enforcement priorities occurs in 2017, the anti-corruption enforcement initiatives currently in play at the DOJ and SEC will remain a significant legal risk for those companies operating on a global basis with a jurisdictional connection to the United States, however slight. Given this risk, coupled with the ever-higher levels of enforcement by countries where the underlying corrupt conduct takes place, organizations' leadership and their counsel need to take the necessary proactive steps to identify and mitigate their exposure.

Focus on the UK

The Serious Fraud Office (SFO) has shown its commitment to penalize firms engaged in bribery and corruption. This is exemplified by the SFO's decision to enter into a significant Deferred Prosecution Agreement (DPA) with Rolls-Royce PLC, the British car and aero-engineering company. The agreement was approved on January 17, 2017 by the President of the Queen's Bench division, Sir Brian Leveson.

Conduct of Rolls-Royce

The DPA was agreed following a four-year investigation by the SFO, and relates to bribery and corruption involving intermediaries in multiple overseas markets. The DPA covers Rolls-Royce's conduct across seven jurisdictions: China, India, Indonesia, Malaysia, Nigeria, Russia and Thailand, and involves the company's civil aerospace business, defence aerospace businesses and its former energy business. The allegations include:

- Agreements to make corrupt payments to agents in connection with the sale of civil aircraft engines and in connection with supply of gas compression equipment;
- Concealment or obfuscation of the use of intermediaries involved in its defence business in countries where the use of intermediaries is restricted; and
- Failure to prevent inducements or bribery by Rolls-Royce employees or intermediaries.

Sir Leveson described the investigation as revealing "the most serious breaches of the criminal law in the areas of bribery and corruption, some of which implicated senior management and, on the face of it, controlling minds of the company."

A distinctive DPA

This is the third and most significant DPA which the SFO has levied since the statutory power became available in 2014. Previous DPAs, against Standard Bank in late 2015 and an unnamed party in 2016, totalled approximately £26 million and £6.5 million, respectively. This DPA agreed with Rolls-Royce, reaching nearly £500 million, is by far the highest penalty that has ever been imposed by the SFO for bribery.

In addition to the SFO agreement, Rolls-Royce also reached a parallel DPA with the US Department of Justice totalling US$169.9 million and a Leniency Agreement with Brazil's Ministério Público Federal for US$25.5 million.

Notably, this is the first time that the UK's proportion of the total global settlement is larger than that of the US. Further, three agencies across the globe working together,

in this case from Europe and the Americas, may suggest a trend towards more aggressive, unified approach to anti-corruption enforcement.

An interesting feature of the DPA is that Rolls-Royce did not self-report. Self-reporting is one of the fundamental objectives of the DPA regime. Once the SFO investigation commenced, however, Rolls-Royce actively cooperated and the level of cooperation led to a final discount of 50 percent. Commentators have questioned whether the decision may encourage boards of directors not to self-report when it may still be possible to obtain a DPA and a discount without doing so.

Decision to impose a DPA rather than prosecute

The allegations against Rolls-Royce relate to systematic and extensive bribery and corruption. In reaching his decision, the Judge took into account several aggravating factors, including that the offences were multi-jurisdictional, spanned across three decades, related to the award of large value contracts and involved senior employees.

Sir Leveson agreed that the total sum of the UK settlement (£497.25 million plus interest and the SFO's costs of £13 million) reflected the seriousness of the conduct displayed. While this high figure may demonstrate that the SFO and UK courts are taking bribery and corruption seriously, the question has been asked: if Rolls-Royce is not prosecuted in these circumstances, in what circumstances will a company be subject to prosecution?

The Judge highlighted that he had to consider what impact a prosecution, rather than a DPA, would have on "employees, others innocent of misconduct or what might otherwise be described as the consequences of a conviction." Subject to the terms being fair, reasonable and proportionate, Sir Leveson concluded that it was in the interest of justice that the conduct of Rolls-Royce be resolved through the mechanism of a DPA.

What next?

There are currently a number of ongoing bribery and corruption investigations being conducted by the SFO and we will be monitoring whether the agency decides to prosecute, or prefers to enter into DPAs.

Focus on China

In 2016, China continued to vigorously enforce its anti-corruption laws. In addition, the supreme judicial bodies issued interpretations specifying penalties in corruption-related criminal cases while the Anti-Unfair Competition Law, which includes commercial bribery, continues to be reviewed.

Judicial interpretation on handling criminal cases involving embezzlement and bribery

On April 18, 2016, the Supreme People's Court and the Supreme People's Procuratorate issued the *Interpretations on Certain Issues Concerning the Application of Law in Handling Criminal Cases Involving Embezzlement and Bribery* (Interpretations), which provide specific sentencing criteria for corruption crimes based on the Amendment (IX) to the Criminal Law of the People's Republic of China (Amendment (IX)) promulgated in 2015.

The Interpretations are significant for businesses operating in China, as Chinese law provides that the death sentence may be imposed where the amount of embezzlement or the accepted bribes is "especially huge" and the crime involves particularly serious circumstances, such as adverse social consequences, or significant harm to the interests of the State and the people. The Interpretations expand upon the meaning of certain expressions used in anti-corruption laws, such as "relatively large amount," "huge amount," and "especially huge amount." Further, the Interpretations provide that, "other serious circumstances," such as the intended use of money and property, as well as the criminal record of the suspect, must be taken into account when determining penalties.

It is noteworthy that, generally speaking, the penalty for receiving bribes is heavier than offering bribes. However, the Interpretations state that the penalty for offering bribes may be greater than receiving bribes under certain circumstances.

In addition, the Interpretations extend the definition of "money and property" to include material interests that can be converted into a monetary amount, such as the decoration of houses, waiving of payments for debts, membership services and travel.

Further, "seeking benefits for others" constitutes a criminal offense even where a person accepts money or property after having performed their duties or functions.

Anti-commercial bribery in revised Anti-Unfair Competition Law

On February 25, 2016, the Legislative Affairs Office of the State Council released the Anti-Unfair Competition Law (the Revised Draft AUCL) to solicit public comments. The Revised Draft AUCL details relevant prohibitions on commercial bribery and elaborates on the meaning of commercial bribery to include the following:

- Seeking organizational, departmental or personal economic benefits relating to public services offered by government agencies, public institutions, or public enterprises, such as power supply companies;
- Paying economic benefits to another undertaking without making a truthful record thereof in the contract and accounting documents; and
- Paying or offering to pay economic benefits to a third party having influence on a transaction while causing harm to the lawful rights and interests of other undertakings or consumers.

In addition, commercial bribery is defined as an economic benefit given—or promised to be given—to the other party in a transaction, or to a third party that can influence the transaction, to encourage them to solicit for undertaking a transaction opportunity or competitive advantage. As well, where any staff member of an undertaking makes use of commercial bribery to seek any transaction opportunity or competitive advantage for the undertaking, such act shall be deemed the act of the undertaking. Since the Revised Draft AUCL has not yet come into effect, there may be further amendments.

Given the promulgation of relevant laws, regulations, judicial interpretations, and policies, it is believed that China will continue to crack down on anti-corruption in 2017. With the expansion of anti-corruption offences, the legal risks—and consequences—associated with doing business in a manner that does not comply with these laws have increased significantly.

Focus on Canada

In 2016, Canada continued to demonstrate its appetite to enforce the *Corruption of Foreign Public Officials Act* (CFPOA), although at a steady rather than spectacular pace. In December 2016, charges under the CFPOA

were laid against Calgary businessman Larry Kushniruk, President of Canadian General Aircraft, in connection with an alleged conspiracy to bribe military officials in Thailand over a commercial aircraft transaction. This case reflects a growing trend in Canada of favoring the pursuit of charges against individuals in bribery and corruption matters. In addition, the high-profile and large-scale CFPOA proceedings against SNC-Lavalin Group Inc. moved forward in 2016, with a preliminary hearing being set down for September 2018. The RCMP also continues to run other active CFPOA investigations which are yet to result in charges, but prosecutions are expected to flow from at least some of these in due course.

The slow and steady pace of CFPOA enforcement has fueled debate in 2016 over whether Canada should introduce a regime that allows for Deferred Prosecution Agreements (DPA) to be reached in CFPOA and other white collar cases, similar to the DPA regimes widely utilized in the US and, more recently, in the UK. Supporters of the initiative argue a Canadian DPA regime would provide law enforcement with a more efficient alternative in resolving CFPOA cases for less egregious conduct, by providing a mechanism to encourage corporations to self-report and remediate instances of corruption in their organizations. In addition, by promoting the proactive implementation of compliance programs, DPAs free up valuable investigative and prosecutorial resources, which could be better deployed in pursuing the most compelling and serious cases. On the other side, critics argue DPAs would result in an "enforcement-lite" approach that allows wrongdoers to escape without having to face the prospect of a conviction, and would likely soften the deterrent effect of the current enforcement regime. Importantly, the Canadian Government has taken note of the debate, and is currently engaged in a review of the issues surrounding DPAs through an initial consultation process. We anticipate further significant developments on this very important issue in 2017.

Domestic corruption enforcement also captured the news in 2016, focusing particularly on the construction and engineering sector in Québec. Former Laval mayor Gilles Vaillancourt pleaded guilty to fraud charges in connection with an alleged corruption scheme, receiving a six-year sentence and a multi-million dollar restitution order as a result. Another former mayor, Robert Poirier, was convicted along with France Michaud, the former vice president of the engineering firm Roche, regarding a corruption scheme in relation to the award of contracts for a water treatment facility in Boisbriand. The same impugned transaction also led to the former Québec Deputy Premier and Minister of Municipal Affairs, Nathalie Normandeau, being charged with corruption-related offences in March 2016. We fully expect to see this trend of domestic corruption enforcement to continue in 2017 and beyond.

On the legislative side, 2016 saw the submission of the first reports under the *Extractive Sector Transparency Measures Act* (ESTMA), a federal anti-corruption act which requires extractive sector companies operating in Canada to report on payments made to foreign and domestic government entities. From 2017 onwards, the obligation will extend to the reporting of payments made by extractive sector companies to Canadian indigenous government entities.

Another significant development in 2016 was the introduction of the whistleblower regime of the Ontario Securities Commission (OSC). The regime provides for a whistleblower bounty to be paid to informants whose tips result in successful enforcement action, as well as for enhanced whistleblower protection. Early reports suggest that the OSC has already received a large volume of tips from whistleblowers, many of whom are no doubt hoping to take advantage of the potential reward on offer, which may be as high as CA$5 million. We will have to wait and see whether 2017 provides more ammunition to the proponents of the controversial whistleblower scheme than its critics.

Focus on Mexico

On July 19, 2017, the new General Law of Administrative Liabilities (the General Law or Ley General de

Responsabilidades Administrativas) is set to take effect, a key development in Mexico's continued efforts to fight corruption and increase transparency at all government levels.

This new law will repeal and replace the Federal Law of Administrative Liabilities for Public Servants (*Ley Federal de Responsabilidad Administrativa de los Servidores Públicos*), and the Federal Anti-corruption Law in Government Procurement (*Ley Federal Anticorrupción en Contrataciones Públicas*), and will greatly expand the scope of liability of private parties (e.g., corporations) for acts of corruption at the administrative level, as private parties may be held liable for improper conduct carried out by individuals acting in their name or on the behalf of others (i.e. officers, directors, liaisons, employees, contractors, advisors, among others). However, when determining the degree of liability of these companies, the existence and enforcement of an integrity policy—which must meet the requirements set forth in the General Law—will be considered as a mitigating factor.

Other notable provisions of the General Law include the following:

i. Public officials must prepare and file three sworn statements disclosing: (a) their assets; (b) any potential conflicts of interest; and (c) evidence of compliance with their tax obligations. These statements will be stored at the digital platform of Mexico's National Anti-corruption System (NAS), with access upon request for anti-corruption enforcement authorities. Redacted versions of these statements will be publicly available.

ii. Public officials involved in public contracting procedures will be subject to closer supervision and will have to abide by, and act in accordance with, a protocol for contracting procedures to be issued by the Coordinating Committee of the NAS.

iii. Other procedures arising from administrative offenses will be carried out with the involvement of three separate authorities: (a) the Investigative Authority (*Autoridad Investigadora*); (b) the Rendering Authority (*Autoridad Substanciadora*); and (c) the Adjudicative Authority (*Autoridad Resolutora*). In procedures for serious offenses or those carried out by private parties, the Federal Court of Administrative Claims will act as the Adjudicative Authority. Criminal liability may also be pursued by the District Attorney.

Given that the existence and enforcement of an integrity policy that is consistent with and abides by the requirements set forth by the General Law will be considered as a mitigating factor when prosecuting private parties, and that responsible parties may choose to come forward to the authorities under a leniency program pursuant to which applicable fines may be reduced, it is of the utmost importance for private parties to review, update, amend and/or implement (as necessary) their relevant policies and guidelines to ensure compliance (including implementing training sessions). Needless to say, this applies to all private parties doing business in Mexico, but is particularly important for those parties which regularly engage with public servants and government agencies.

The General Law follows a set of Constitutional Amendments on anti-corruption enacted in 2015, and the introduction of the NAS and amendments to existing statutes (such as the Federal Criminal Code) in 2016 as part of Mexico's commitment to maximum transparency.

Contributors

Sandy Walker (Managing Editor)

US

Stephen D. Libowsky (Competition/Antitrust)
Partner, Chicago
D +1 312 876 2529
stephen.libowsky@dentons.com

Michael E. Zolandz (Foreign investment review/ National security/ Trade and economic sanctions/Public affairs)
Partner, Washington, DC
D +1 202 408 9204
michael.zolandz@dentons.com

Stephen L. Hill (Anti-corruption)
Partner, Kansas City
D +1 816 460 2494
stephen.hill@dentons.com

Michelle Shapiro (Anti-corruption)
Partner, New York
D +1 212 398 4877
michelle.shapiro@dentons.com

Petrina McDaniel (Privacy and data protection)
Partner, Atlanta
D +1 404 527 4385
petrina.mcdaniel@dentons.com

Peter Stockburger (Privacy and data protection)
Managing Associate, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com

Todd Daubert (Privacy and data protection)
Partner, Washington
D +1 202 408 6458
todd.daubert@dentons.com

Kenneth J. Nunnenkamp (Public affairs)
Partner, McLean
D +1 703 574 4241
kenneth.nunnenkamp@dentons.com

Europe and the UK

Richard Jenkinson (Competition/Antitrust/Public affairs)
Associate, London
D +44 20 7246 7590
richard.jenkinson@dentons.com

Nick Graham (Privacy and data protection)
Partner, London
D +44 20 7320 6907
nick.graham@dentons.com

Sophie Albrighton (Competition/Antitrust)
Associate, London
D +44 20 7246 7037
sophie.albrighton@dentons.com

Adrian Magnus (Competition/Antitrust)
Partner, London
D +44 20 7320 6547
adrian.magnus@dentons.com

Tatiana Kruse (Privacy and data protection)
Of Counsel, London
D +44 20 7320 6153
tatiana.kruse@dentons.com

Tanvi Mehta (Privacy and data protection)
Associate, London
D +44 20 7246 7422
tanvi.mehta@dentons.com

Constantin Rehaag (Privacy and data protection)
Partner, Frankfurt
D +49 69 45 00 12 248
constantin.rehaag@dentons.com

Valeria Hoffman (Privacy and data protection)
Senior Associate, Frankfurt
D +49 69 45 00 12 250
valeria.hoffman@dentons.com

Daren Allen (Anti-corruption)
Partner, London
D +44 20 7246 7651
daren.allen@dentons.com

Canada

Sandy Walker (Competition/Foreign investment review/National security)
Partner, Toronto
D +1 416 863 4517
sandy.walker@dentons.com

Paul M. Lalonde (Anti-corruption)
Partner, Toronto
D +1 416 361 2372
paul.lalonde@dentons.com

Timothy M. Banks (Privacy and data protection)
Partner, Toronto
D +1 416 863 4424
timothy.banks@dentons.com

Adam S. Goodman (Competition/Antitrust)
Partner, Toronto
D +1 416 862 3416
adam.goodman@dentons.com

Anthony Cole (Anti-corruption)
Partner, Calgary
D +403 268 3036
anthony.cole@dentons.com

Chantal Bernier (Privacy and data protection)
Counsel, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Hon. James Moore (Public affairs)
Senior Business Advisor
D +1 604 691 6418
james.moore@dentons.com

Joe Lougheed (Public affairs)
Partner
D +1 403 268 6884
joseph.lougheed@dentons.com

China

Jet Deng (Competition/Antitrust/Privacy and data protection)
Partner, Beijing
D +86 10 5813 7038
zhisong.deng@dachenglaw.com

Ken Dai (Competition/Antitrust/Privacy and data protection)
Partner, Shanghai
D +86 21 5878 1965
jianmin.dai@dachenglaw.com

Emilia Shi (Foreign investment review/National security)
Partner, Shanghai
D +86 21 0283 827
emilia.shi@dentons.cn

Mexico

Rogelio Lopez-Velarde (Competition/Antitrust)
Managing Partner, Mexico City
D +52 55 3685 3334
rogelio.lopezvelarde@dentons.com

Fernando Quesada (Competition/Antitrust)
Associate, Mexico City
D +52 55 3685 3333
fernando.quesada@dentons.com

Dante Trevedan (Anti-corruption)
Senior Associate
D +52 55 3685 3316
dante.trevedan@dentons.com

Amanda Valdez (Privacy and data protection)
Partner, Mexico City
D +52 55 3685 3313
amanda.valdez@dentons.com

Jorge Lopez (Privacy and data protection)
Associate, Mexico City
D +52 55 3685 3333
jorge.lopez@dentons.com

Colombia

Juanita Acosta (Privacy and data protection)
Partner, Bogota
+57 1 313 7800 ext. 358
juanita.acosta@dentons.com

Lina Cala (Privacy and data protection)
Associate, Bogota
+57 1 313 7800 ext. 105
lina.cala@dentons.com

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com

© 2017 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.

CSBrand-1636 Regulatory Trends Brochure Final — 09/02/2017