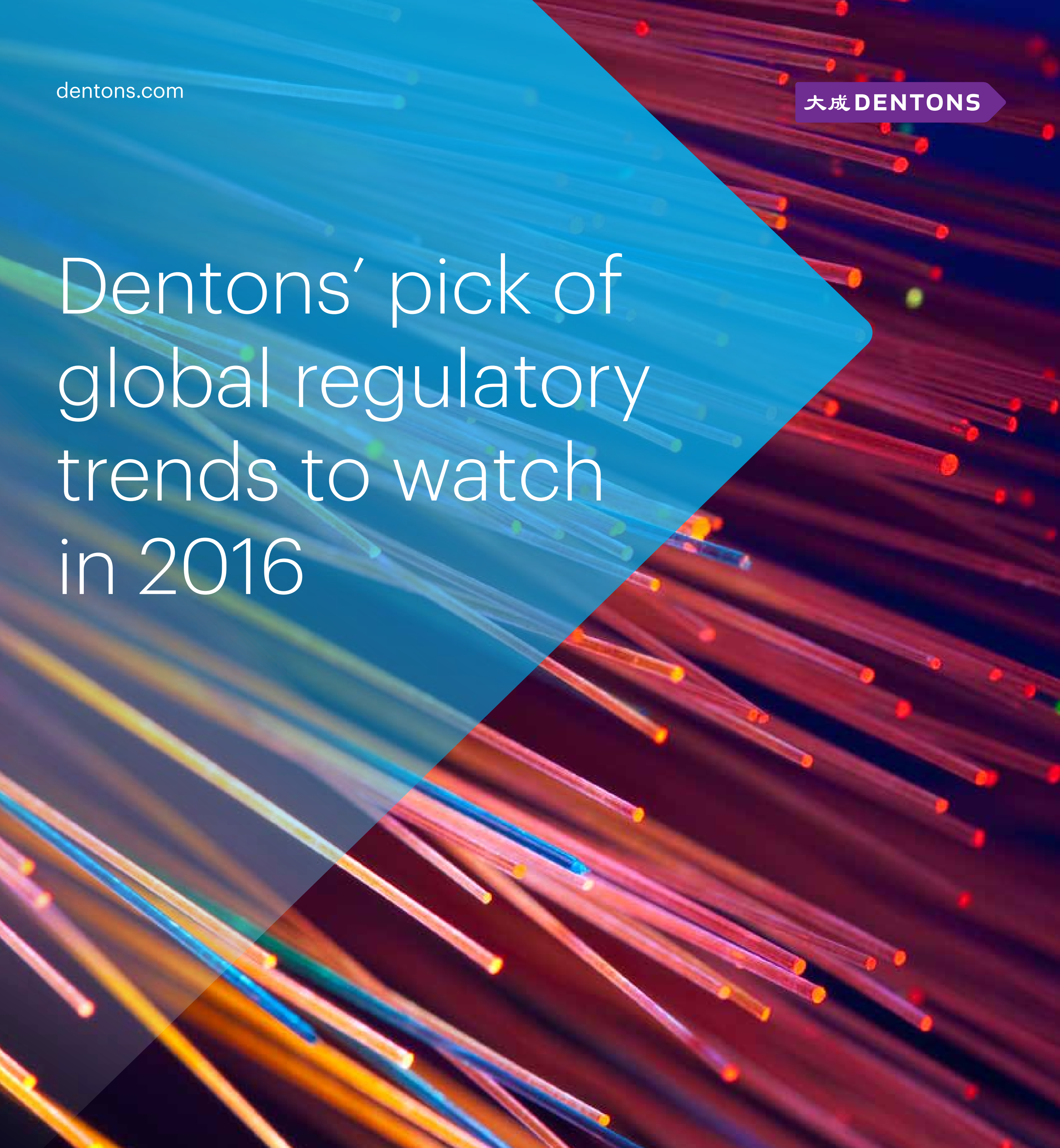
dentons.com

大成 DENTONS



Dentons' pick of global regulatory trends to watch in 2016

Dentons' team of regulatory lawyers from key jurisdictions around the world weigh in on regulatory trends to watch in 2016 in the US, Europe, Canada and China.

Table of contents

1. Competition/antitrust law

Focus on the US

Cartel enforcement activity and stiffer criminal penalties against price fixing

The Department of Justice (DOJ) continues to investigate and seek criminal charges against worldwide cartels. This enforcement activity will remain at heightened levels and continue to be a huge moneymaker for the DOJ. Fiscal 2014 and fiscal 2015 saw billions of dollars in criminal fines paid by companies in a wide variety of industries. In 2015, the DOJ continued its focus on auto parts manufacturers and on enforcing criminal antitrust laws in the tech industry, including electrolytic capacitors and an e-commerce executive for allegedly using algorithm-based software to fix prices. The DOJ continues to prosecute individual wrongdoers, charging 66 individuals in 2015, up from 44 in 2014, while the average prison sentence of 24 months in 2010-2015 has increased by a factor of three since the 1990s. Individual prosecutions will continue in 2016, consistent with the so-called "Yates Memorandum", the September memorandum from Deputy Attorney General Sally Yates that details DOJ policy to target individual wrongdoers involved in corporate misconduct, underscoring the importance of effective compliance programs.

Merger investigations and suits to block certain combinations will continue in 2016

Bolstered by litigation wins in 2015, the DOJ and Federal Trade Commission (FTC) will continue to focus on mergers and bring enforcement actions based on narrow market definitions. DOJ investigations resulted in parties abandoning major acquisitions, including Comcast/Time Warner Cable, Applied Materials/Tokyo Electron, GE/Electrolux, and Bumble Bee/Chicken of the Sea, after incurring huge expenses and paying large break-up fees. The FTC successfully enjoined the proposed Sysco/US Foods combination after an eight-day hearing with the court agreeing with the FTC's narrow market definition and rejecting the parties' argument that the FTC's market was based on an unrepresentative sample of subjective customer preferences. Similarly, the FTC is presently seeking to block the Staples-Office Depot merger on the same basis.

In addition, the health care-related sector has also been under scrutiny. The FTC is and will continue to be active in seeking to block health care combinations. The FTC filed three suits near the end of 2015, all of which are anticipated to be resolved in 2016. For its part, the DOJ will also decide whether to allow several huge health insurance company mergers in 2016.

Pharmaceutical pricing under scrutiny

Pharmaceutical pricing will be under heavy fire in 2016, with investigations by both the DOJ and FTC. While unilateral pricing behavior is not usually subject to antitrust attack, the agencies will look hard for a remedy here. The DOJ continues to expand its ongoing probes of generic drug pricing, with subpoenas seeking information from seven pharmaceutical companies. Both the House of Representatives and the Senate are focused on drug pricing, with the Senate Select Committee on Aging holding a hearing and sending inquiries to a number of drug companies. In November, Democrats launched an Affordable Drug Pricing Task Force and sought hearings on Turing and Valeant. In addition, the Connecticut and New York attorneys general, and the US Department of Health and Human Services are conducting investigations while the FTC, state attorneys general, and private plaintiffs continue to aggressively litigate pharmaceutical companies' conduct at the expiration of patent life.

Challenges to "reverse payments" have proliferated in the wake of the US Supreme Court's *FTC v. Actavis* decision. In *King Drug v. Smithkline Beecham*, the Third Circuit court held that antitrust challenges can reach more than cash payments, including other forms of consideration, likely encouraging even more government and private suits. The FTC has also demonstrated an increased proclivity to seek significant monetary relief in reverse payments cases; its long-standing suit against Cephalon Inc. was US$1.2 billion. So-called "product hopping" was the subject of its first appellate decision in *New York v. Actavis*, in which the court upheld an injunction requiring Actavis to continue to make available an older drug until generic entry, after introducing a new version of the drug, to facilitate generic competition. At the same time, a lower court decision which took a dimmer view of antitrust challenges to product hopping in *Mylan v. Warner-Chilcott* is on appeal before a circuit court and will likely be decided in 2016. If the lower court decision is upheld, the circuit split could be ripe for Supreme Court review.

FTC report on patent assertion entities

The FTC has been studying patent assertion entities, which are "firms with a business model based primarily on buying patents and then attempting to generate revenue by asserting them against businesses that are already practicing the patented technologies." The FTC issued requests for information from 25 such entities across various industries, and 15 non-practicing entities and firms in the wireless chipset sector. The FTC is specifically targeting the wireless industry because of the intensity of patent assertion claims in that sector. The FTC's report, expected in early 2016, may influence court decisions and legislation involving these firms.

Focus on Europe

EU competition authorities focus on internet platforms

Competition authorities are looking at "platforms"—a ubiquitous feature of the "sharing economy"—from a variety of angles. New services, such as Uber, Air B&B and Just Eat, which do not make sales by themselves but instead pair up buyers and sellers, are examples. Platforms such as Uber have been undercutting traditionally highly regulated markets such as metropolitan metered taxis. Is this fair competition, or the sidestepping of important employee, consumer and public protections?

In 2015, the UK's Competition and Markets Authority spoke up in favor of Uber and against Transport for London's proposed restrictions on such services. More such interventions are possible. However, despite looking similar on the outside, platforms tend to offer a slightly different service in different cities (for example, Uber only connects licensed minicab drivers in London, which has not been the case elsewhere), and regulatory responses vary from place to place for each platform. Across the EU, Uber is opening in some cities and closing in others (e.g., the German cities of Hamburg, Frankfurt and Düsseldorf), as the different regulatory environments affect its model in different ways.

The ultimate platform provider is Google. Its primary function as a search engine (a market in which it holds higher market shares in the EU than in its native US), coupled with its use of sponsored and non-sponsored links (including links to its own services), make it a key facilitator between buyers and sellers. As a result, its behaviour has caught the eye of the European Commission, which has subjected it to two investigations for potential abuses of dominance: one into Google shopping and the other into the Android mobile phone operating system. The Commission has also said that it will look at Google's maps and travel services in future.

Each of the European Commission's investigations into Google has been subject to criticism. The Commission has previously tried and failed to settle its investigation into Google shopping in 2014, which followed objections from competitors and politicians alike. In December 2015, a European Parliamentary committee recommended that the Commission both speed up and widen the scope of its investigations into Android. The Commission may reach a decision on one of these investigations at least at some point this year (albeit one that is highly likely to be appealed).

Rogue nation: EU National Competition Authorities and inconsistent enforcement actions taken against most favored nation clauses

Vertical restrictions are an area where the EU competition rules have historically been stricter than in other jurisdictions. Restrictions on distributors' abilities to set independent prices are treated in the EU as being equivalent to cartel arrangements and are not subject to a "rule of reason" test, as is the case in the US.

It is in this environment that the most favored nation (MFN) clauses in agreements between online travel agent (OTA) Booking.com and hotels came under scrutiny by several competition authorities across the EU. While normally a pan-EU case would be handled by the European Commission, this case was handled by the National Competition Authorities (NCAs) of France, Italy and Sweden, who were appointed by the European Competition Network (an association of EU NCAs and the Commission), to lead the investigations. There was an understanding that other NCAs—each of which enforces domestic and EU competition law in its own territory—would not duplicate this work, but that they would be kept informed and contribute to the process.

MFNs can be broadly described as falling into two camps: broad MFNs and narrow MFNs. Broad MFNs require the hotel to give the OTA the same or better room rates, conditions and availability as on any other channel, including those of competitor OTAs. Narrow MFNs merely require the same room rates as are being charged by the hotel itself. Booking.com was not alone among OTAs in requiring hotels to sign to MFNs.

The NCAs' issue with the MFNs was that, by fixing a hotel room's price at the same level as offered by other OTAs, the OTA benefitting from the MFN did not have to compete with other OTAs on the rate of commission charged to hotels. A hotel subject to a broad MFN would be unable to encourage lower commission OTAs who might be willing to offer lower room rates by charging lower commissions.

Booking.com offered identical commitments to the French, Italian and Swedish NCAs, bringing to an end their investigations. These commitments phased out the use of broad MFNs in their contracts in each jurisdiction, with the expectation that other EU NCAs would reach the same findings should Booking.com continue to use broad MFNs in their territories. Each NCA accepted the commitments in a coordinated fashion, announcing their intention to do so on the same day, in April 2015.

What happened next, however, was clearly not coordinated. Although EU law prevents an EU NCA from adopting a decision contrary to a Commission decision, there is no mechanism to prevent EU NCAs from adopting contradictory decisions to each other. This has now occurred with the German NCA, the Bundeskartellamt, reaching its own decision in December 2015, that both the broad and narrow MFNs imposed by Booking.com infringed EU competition law. Therefore, 2016 has begun with three pressing questions which are, as yet, unanswered:

- Which (if any) other EU NCAs will prohibit narrow MFNs?
- Whose interpretation on the legality of narrow MFNs under EU competition law is correct?
- Will we ever see NCA-led pan-EU competition law enforcement again, given this failure to agree?

The Pay TV investigations: To what extent can territorial licensing survive in the internet age?

Historically, the European Commission has used competition law in order to drive forward the integration of the European single market. Agreements between competitors—and even non-competitors—to restrict the territories into which they supply goods and services have been regarded as breaches of the Article 101 of the Treaty on the Functioning of the European Union (TFEU), the prohibition on anticompetitive agreements. However, broadcasting has, until now, been something of an exception to the rule, as the Commission has recognized that national broadcasters generally broadcast only to viewers in one Member State. No longer.

In July 2015, the Commission sent a statement of objections to Sky UK, a UK telecommunications company and broadcaster, and the six leading Hollywood film studios. The Commission had come to the preliminary conclusion that the territorial restrictions between Sky and the studios were unlawfully restrictive of competition insofar as they gave absolute territorial protection to broadcasters outside of the UK. The Commission argued that as a result, Sky was prevented from providing its services to end-users based outside the UK. Simultaneously, the Commission is also undertaking investigations into Canal Plus, Sky Italia, Sky Deutschland and DTS's arrangements with film studios and cross-border access to pay TV services in France, Italy, Germany and Spain. None of these have yet reached the formal objections stage. The roots of these cases go back to 2011, when the Court of Justice of the EU ruled in the Murphy case that an export prohibition on TV decoding devices was a restriction of competition "by object", prohibited by Article 101 TFEU.

Murphy and the Commission's Pay TV investigations raise a number of tensions with two well-established principles of EU law:

- The principle that the right of communication to the public is not subject to exhaustion, i.e. the doctrine that that once a broadcast has been authorized in one part of the EU, it cannot be prevented from being broadcast elsewhere; and
- The ruling in Coditel II, which states that a rights holder can limit the authorization that it grants—including its territorial scope—without infringing Article 101 TFEU.

The Commission's public position appears to suggest it takes the contrary position.

Additionally, two directorates of the Commission (independent of the Commission's competition directorate) are currently working on their own proposals for preventing what they describe as "unjustified geo-blocking," whereby consumers of online content (including online Pay TV, a distribution channel recently taken up by Sky UK), are blocked and redirected based on their location, limiting choice. The directorates published an impact assessment on the subject in December 2015, noting that using competition enforcement to prevent unjustified blocking had major shortcomings. For example, any enforcement action would fail in cases where a non-dominant blocking entity was imposing the blocking on its own initiative (by avoiding the prohibitions of anticompetitive agreements and abuse of dominance).

Therefore, these investigations appear set to be both tricky and political. As a matter of good practice, the different directorates of the Commission will wish to avoid reaching contradictory conclusions. Hearings took place in the Sky investigation in January 2016, and a decision is expected later in the year.

Criminal cartel enforcement in the UK: A declaration of independence from US enforcement?

While criminal sanctions against individuals for cartel infringement are the norm in some jurisdictions, the UK has lagged behind. Until 2015, the only criminal convictions of UK citizens for cartel infringement had been driven by US law enforcement. For example, British Airways' Keith Packer served time in Florida for his role in the Air Cargo cartel and the guilty pleas in the UK of the Marine Hose cartelists were procured by US authorities who had threatened them with extradition.

In 2015, the Competition and Markets Authority reported its first independently obtained conviction for a criminal cartel. The conviction was a guilty plea; those who chose to plead not guilty were acquitted. However, their successful defences rested on the prosecution failing to prove dishonesty, a requirement which has now been removed from the UK cartel offence. With the elimination of the dishonesty requirement, increased resources for criminal enforcement, and an independently gathered conviction in hand, the UK's success in prosecuting cartels may be about to increase.

Focus on Canada

Competition Bureau advocates and policy-makes on innovation

The application of competition law to innovative business models will be a continuing theme in 2016. The Competition Bureau will play a lead role both as an advocate of competition policy in traditionally regulated industries and as an enforcer.

Over the past two years, Canadian municipalities have grappled with the regulation of new ride-sharing apps – most notably, Uber. In June 2015, the Ontario Superior Court of Justice declined to grant the City of Toronto an injunction against Uber, finding that, based on the wording of the relevant provisions of the Toronto Municipal Code concerning taxis, the Code did not apply to Uber's business model. Following the Court's decision, in a high profile White Paper submitted to the City of Toronto, the Competition Bureau advocated in favor of relaxing restrictions on taxis instead of increasing restrictions on digital ride-sharing services, such as Uber. We anticipate the Bureau will continue to advocate for deregulation of traditional taxis as the municipalities assess how to deal with Uber.

In 2015, the Bureau also publicly advocated in favor of a proposal of the Canadian Radio-television and Telecommunications Commission that would allow consumers to access video-on-demand (VOD) services unbundled from other services, such as a cable television or internet subscription. The Bureau believes that such reforms will assist Canadian providers to compete with online (over-the-top) providers, such as Netflix.

The Bureau published Draft Intellectual Property Enforcement Guidelines (IPEGs) for public consultation in the summer of 2015. The Draft IPEGs (which have not been finalized and remain in draft form at the time of publication), like previous incarnations of the IPEGs, reaffirm the Bureau's view that intellectual property rights and competition law are complementary. However, the Draft IPEGs also offer insights into the Bureau's approach to current issues, such as standards essential patents (SEPs) and patent settlements, and it is clear that the Bureau's views have evolved. Whereas the Bureau indicated in 2014 that patent settlements that delayed generic entry beyond the life of the patent would generally be pursued as a criminal cartel matter, the Draft Guidelines now indicate that "in the vast majority of cases," it will consider patent settlements under the civil provisions of the Act and that criminal enforcement will be the exception where the intent of the parties was to engage in price fixing, market allocation or restrict output. We anticipate that the Bureau will finalize its Draft Guidelines in 2016 and will be keen to investigate any credible complaint regarding a patent settlement that results in anti-competitive effects.

Competition Bureau to proritize criminal enforcement against cartels and bid-rigging despite suffering some setbacks

The investigation of criminal cartel conduct remains one of the Competition Bureau's most significant enforcement priorities. This is especially true of domestic cartel conduct and international cartels that have a material connection to Canada. The Bureau's investigation into automobile parts, in particular, has been very active over the past two years, yielding a CA$4.5 million fine against Japanese bearings manufacturer, NSK, and a CA$4.7 million fine against Panasonic in 2014. Two corporations and two individuals in the ocean freight industry pleaded guilty to price-fixing charges and faced fines of approximately CA$1.7 million.

In 2015, two contested proceedings reached their conclusions: one in the Bureau's favor and the other in favor of the accused. In particular, Pétroles Global was fined CA$1 million by the Superior Court of Québec for retail gasoline price-fixing. In the other case, a jury acquitted all accused in a bid-rigging case involving the procurement of IT services for government agencies. Another significant setback for the Bureau in 2015 was the staying of proceedings in the chocolate price-fixing proceedings against the remaining defendants. This marked the end of the Bureau's investigation into allegations of price-fixing by Canadian chocolate manufacturers, which had been ongoing since 2007, pursuant to which Cadbury received immunity and Hershey pled guilty and paid a CA$4 million fine.

The Bureau's prioritization of enforcement resources to Canadian cartels (such as retail gas and Québec construction), and international cartels with a significant nexus to Canada (such as auto parts) will continue in 2016. Moreover, international cartels will continue to attract attention from plaintiffs in class proceedings. In 2015, for example, the air cargo class action and lithium ion batteries class action were both certified by the Ontario Superior Court of Justice.

More economic evidence required for merger enforcement

In the first Supreme Court of Canada decision relating to the mergers provisions of the Canadian *Competition Act* in almost 20 years, the court reversed earlier decisions of the Competition Tribunal and the Federal Court of Appeal in the Tervita case, which required a divestiture of assets on the basis that efficiency gains exceeded anti-competitive effects. The court set forth a methodology for analyzing a merger in which there are anti-competitive effects as well as efficiency gains, and noted the Competition Bureau's failure in that case to quantify "quantifiable" anticompetitive effects. The case may make merger challenges by the Bureau harder to win. In addition, it will have significant ramifications for how the Bureau proceeds in future cases where the efficiency defence is likely to be raised by the merging parties; in particular, a higher volume of economic evidence will need to be collected and adduced.

Focus on China

As China's Anti-Monopoly Law enters its eighth year in force, its enforcement by China's antitrust authorities has increased significantly. In 2015, China launched substantial enforcement actions in respect of monopoly agreements and abuse of dominance such as the Qualcomm investigation and a series of investigations in auto sector for monopoly agreements. Given that China, the world's second largest economy, is still at a relatively early stage of antitrust law development, it can be expected that the Chinese antitrust authorities will accelerate the pace of enforcement in 2016 as they gain experience.

Chinese authorities crack down on cartels

After more than seven years of enforcement of its Anti-Monopoly Law, China entered into a "new normal" phase in 2015. Both the National Development and Reform Commission (NDRC) and the State Administration for Industry and Commerce (SAIC), the two antitrust authorities responsible for pursuing cartels and other behavioral violations, are well-established and actively pursuing investigations against cartels.

In 2015, NDRC continued to crack down international cartels, including imposing a fine of $63 million on a Ro-Ro shipping cartel formed by eight carriers who fixed prices and shared markets. Similar to the auto parts cartel investigated by NDRC the year before, the Ro-Ro shipping cartelists who had been investigated in the US or EU previously raced to NDRC to apply for leniency. The first three carriers applying for leniency were granted fine exemption or reduction, underlying the importance for companies to include China in their global leniency strategy.

Another noteworthy category of cases to watch are cartels organized by government agencies. In a recent case, the NDRC prosecuted a local telecom regulator that organized four local telecom operators to coordinate on their sales promotion. The telecom operators were fined $2.12 million. This case demonstrates that it may not be an effective defense to argue that the cartel was arranged by a government agency.

SAIC investigated a number of domestic cartels in 2015, which mainly involved market sharing practices in sectors such as construction and insurance. Both sectors have been viewed as prone to conspiracies, and there have been a number of cases in these sectors during recent years. As a result, it is expected that a focus on these sectors will continue over the next several years. In addition, for the first time, SAIC has sanctioned a boycott organized by a trade association of exhibitions held by third parties.

For 2016, we anticipate that international cartels will continue to be in the crosshairs and sectors, such as transportation, and electronic components may be targeted. As for domestic cartels, industries including automotive, healthcare, telecom, insurance and construction, are expected to be under scrutiny.

China is in the process of refining its antitrust enforcement, with new legislation to come out in respect of immunity applications, a leniency mechanism and a fine calculation methodology. All of them will bring China's cartel enforcement up to a new level.

Vertical agreements under scrutiny

Resale price maintenance (RPM) will be a continued focus of NDRC in its enforcement against vertical monopoly agreements. In 2015, NDRC fined two auto makers $75 million for restricting resale prices of their dealers, continuing NDRC's antitrust reform of the auto industry since 2014.

In addition, healthcare is a key industry where NDRC has enhanced its RPM enforcement, partly due to complaints about the relatively high price of healthcare in China.

So far, neither NDRC nor SAIC has publicized decisions relating to non-price vertical monopoly agreements. However, SAIC has been studying how to deal with certain non-price restraints, such as exclusive distribution and

MFN clauses. In addition, although China does not have a block exemption for vertical restraints as in the EU, antitrust guidelines being drafted for the auto industry will be useful references for other industries in respect of non-price vertical restraints.

Industries producing goods and services closely related to the livelihood of the general public will continue to be an enforcement and legislative priority for Chinese authorities in 2016. Companies doing business in China will need to ensure they avoid engaging either in resale price maintenance or non-price vertical restraints.

Abuse of dominance in intellectual property and domestic monopolies

The enforcement of abuse of dominance will continue to be an area to watch in 2016.

In particular, antitrust authorities are likely to pursue anti-competitive conduct relating to intellectual property rights (IPRs). Of significant interest will be how agencies address refusals to license IPRs (e.g., settlements or commitments to license under reasonable terms).

In addition, standard essential patents (SEPs) have become a focal point of China's antitrust enforcement. In 2015, NDRC fined Qualcomm $975 million for its abuse of a dominant market position in the wireless communication industry by charging unfairly high royalties under its SEPs and tying its non-SEPs with its SEPs. NDRC has also pursued other companies, especially patent assertion entities, for similar anti-competitive practices.

Apart from challenging particular practices, NDRC is now taking the lead to draft antitrust guidelines for abuse of IPRs, which are expected to be enacted in 2016.

SAIC has made considerable efforts to remedy competition issues in domestic monopoly industries, such as telecom, water supply, gas supply and cigarettes, in addition to carrying out industry reform. SAIC has also taken enforcement action against a refusal to deal for the first time. In 2015, SAIC sanctioned an abuse of dominance regarding a refusal to deal by a supplier of medicinal ingredients for gout who was found to hold a dominant position.

Merger control on the rise

The Ministry of Commerce (MOFCOM), the antitrust authority responsible for merger control, reviewed a record number of cases in 2015, representing a 36 percent growth from the previous year. Significantly, 74 percent of the cases were cleared within Phase 1 (i.e. 30 calendar days), primarily due to the simplified procedure introduced in 2014. The simplified procedure has significantly improved MOFCOM's efficiency in reviewing merger filings, reducing the waiting period.

In 2015, only two cases were approved subject to conditions. With respect to Nokia's acquisition of Alcatel-Lucent, MOFCOM required Nokia to commit to license its SEPs in the telecom industry under FRAND terms without misusing injunctions and to inform its licensees or potential licensees if it transfers certain SEPs to third parties in the future (in order to provide an opportunity to assess the impact of such transfer on the royalty rate charged by Nokia). This case is consistent with several previous cases involving SEPs where MOFCOM required commitments despite the fact that those SEPs holders had already undertaken to license their SEPs under FRAND terms in accordance with the policies of standard setting organizations.

The other merger case involved NXP's acquisition of Freescale. This is the first case where MOFCOM applied a combination of fix-it-first remedy and an up-front buyer remedy, requiring NXP not to consummate the acquisition before divesting its radio-frequency power transistor business to a buyer who had been identified and approved by MOFCOM during the review procedure. This remedy was consistent with that adopted in the EU.

In addition to reviewing filings, MOFCOM also increased enforcement of filing requirements, penalizing parties to nine merger transactions. As the average investigation time for a failure-to-file case was 228 calendar days—much longer than the average review time for cases duly filed with MOFCOM—merging parties would be well-advised to comply with the merger control rules and avoid unnecessary costs.

Finally, in 2016, MOFCOM may issue revised merger control rules, which are expected to further improve the efficiency and transparency of MOFCOM's review work.

Private enforcement of antitrust law trending upwards

The enforcement of antitrust law through actions for damages by private parties is expected to increase significantly over the next year. Antitrust civil suits have become more common with 141 new cases being launched between January and October 2015. Two types of cases attracted the most attention: cases involving IPRs and cases involving consumers suing companies for damages following prosecutions by NDRC.

In regard to the first category, defendants are alleged to have abused dominant positions involving SEPs and other patents by charging unfairly high royalties, engaging in tying and refusing to license patents. While some of the cases have settled, some are ongoing including a case involving a refusal to license rare earth-related patents. A decision in this matter should shed light on the Chinese judiciary's position on applying the essential facility doctrine to patent licensing.

The second type of case is the follow-on action case involving consumers suing companies after the latter were fined by NDRC for engaging in anticompetitive activity. Cases have involved civil suits following on from an insurance cartel and the distribution of infant formula.

Both types of cases have significant ramifications for companies doing business in China, and cases like these are expected to increase in the near future, on a larger scale. It is noteworthy that Chinese companies have been more sophisticated in utilizing antitrust law to achieve commercial goals, and Chinese consumers and consumers' associations may increasingly initiate collective follow-on actions.

2. Foreign investment review and national security

Focus on the US

Scope of foreign investment review expanding in the US

The US maintains an extensive, though voluntary, foreign investment review process under the Committee on Foreign Investments in the US (CFIUS). This multi-agency review process has often been viewed as politically motivated, but at its core serves as both national security and foreign policy purposes. The underlying statute authorizes the US President to block transactions determined to be contrary to US national security interests, and further authorizes CFIUS to negotiate and agree to mitigation to address any national security concerns, while allowing the transaction to proceed.

In the last several years, the role of CFIUS focus has expanded, with a greater emphasis placed on acquisitions involving properties in any sector that are "proximate" geographically to US government or US military facilities, transactions involving critical infrastructure (such as LNG facilities, transportation hubs and energy assets), potential acquisitions of critical technologies important to defense production or raising cybersecurity concerns, and transactions that place important government supply chain assets under foreign control. While the physical proximity standard has not been defined, the use of this factor in reviewing foreign acquisitions has become increasingly relevant as a key consideration for companies seeking to acquire US commercial interests.

A related development is the expansion of CFIUS reviews to include "greenfield" investments; CFIUS reviews have included land acquisitions in the US, by foreign parties—a development with uncertain regulatory support. Following the Ralls case, in which CFIUS forced a Chinese investment enterprise to divest and terminate a greenfield alternative energy project due to the proximity to a US Naval Air facility concerns, a number of Congressional supporters of stricter investment reviews have proposed amendments to the CFIUS statute that would expressly permit review of greenfield investments. With the number of CFIUS reviews rising, increasing oversight of the CFIUS process by investors and political leaders is likely.

New legislation relating to homeland security

The US$1.1 trillion omnibus bill passed in the final legislative days of 2015 contained many homeland security provisions, including changes to the US Visa Waiver program. While not precisely tied to foreign investment, the increased scrutiny on immigration matters creates spillover effects for foreign investments in the US, particularly as scrutiny of the EB-5 visa program continues. As a policy matter, sectors such as telecommunications and energy remain subject to enhanced review by the CFIUS committee, given concerns over cybersecurity and infrastructure security.

Focus on Europe

The EU supports foreign investments as one part of its common commercial principles and has been negotiating a number of economic agreements, with the objective of improving foreign investments. Notably, the Transatlantic Trade and Investment Partnership (TTIP) with the US and the Bilateral Investment Agreement with China are the latest European external economic efforts.

Since an EU-wide comprehensive investment policy is still missing and will be introduced progressively, rules restricting and monitoring foreign investments are to be found in national laws of the EU Member States. As a result, administrative procedures and limitations on foreign investments for national security reasons may differ across the EU.

Generally, governments of each EU Member State may review the acquisition of domestic companies by foreign buyers (i.e. investors located outside the territory of the EU or the EFTA Agreement) in individual cases in order to avoid national security risks in any sector regardless of the size of the companies involved in the acquisition. Special rules apply to the acquisitions of certain defense and IT security companies. In regards to the latter, the current negotiations for selling Airbus Group's defense electronics unit in Germany are worth watching in 2016, particularly as Germany must approve this transaction under its foreign trade and investment laws.

Focus on Canada

New government, new approach to foreign investment?

As Canada's foreign investment review law, the *Investment Canada Act* (ICA), tends to be a law that is more political than most, foreign investors in Canada may wonder how Prime Minister Justin Trudeau's new Liberal government will treat them in 2016. Will national security reviews of foreign acquisitions or establishments of Canadian businesses continue unabated at the higher levels of the past few years or will they become less frequent? Will the new government clarify the "net benefit to Canada" test for review of foreign investments? In an uncertain economic climate, in which the Canadian economy has been devastated by plummeting oil prices, will the current policy ban on acquisitions of control of Canadian oil sands businesses by non-Canadian state-owned enterprises (SOEs) be re-considered?

Will national security reviews continue with the same frequency?

The Canadian government introduced a national security screening process into the ICA in 2009; the review applies to investments of any magnitude that could be "injurious" to Canada's national security. The federal Cabinet has wide discretion to determine the relevant risk factors and prohibit a proposed investment or require divestiture of a completed investment transaction. However, in the first few years after the review process was established, the government rarely took action to challenge foreign investments on the grounds of national security.

This changed a few years ago as the Canadian government seemingly found an increasing number of foreign transactions that raised concerns. Although there is very little transparency in the conduct of these reviews, practitioners have noted numerous reviews, including prohibitions of transactions as well as divestitures. The first formal disallowance under the national security regime was in the fall of 2013 relating to the acquisition by Accelero Capital of MTS's Allstream Division, a national fiber optic network that provides critical telecommunications services to businesses and governments, including the Canadian government.

Since 2013, there have been a significant number of national security reviews. For example, in 2015, the government rejected the establishment by a Chinese SOE of a fire alarm manufacturing facility in Québec in a location deemed to be too close to the Canada Space Agency headquarters and issued a divestiture order against a private Chinese company that had purchased a Québec company specializing in fiber components, modules, lasers and amplifier systems for applications in a number of sectors, including defence and security. Significantly, the Chinese company in the latter case has sought judicial review of the decision.

With a new government led by a prime minister who is regarded as friendlier to China and more internationalist than his predecessor, foreign investors will keenly monitor the extent to which the Canadian government scrutinizes transactions involving targets in sensitive sectors, such as telecom, defence and technology. Although the new government may have a less ideological perspective on security issues, the current global threats to security arising from terrorist attacks, cyberespionage and military aggression by certain states (or aspiring ones) suggest the government will maintain a continued close eye on foreign investments in these sectors.

Changes to "net benefit to Canada" review?

Apart from national security, the ICA provides for review of significant foreign investments under the "net benefit to Canada" test. The new government has signalled that foreign investors require greater clarity in the application of this test which involves the government's consideration of numerous factors, such as the impact of the investment on employment, capital expenditures, the participation of Canadians in senior management and governance. It is anticipated that factors such as the impact of a foreign investment on innovation, economic growth and productivity may receive greater weighting given the new government's announced priorities and the current level of economic uncertainty. It remains to be seen whether the government will issue new guidance to clarify what it has previously characterized as political decision-making under the ICA.

Apart from "net benefit," another issue to watch is whether the new government adheres to or relaxes the current policy ban on acquisitions of control by state-owned enterprises of Canadian oil sands businesses. With the devastating slump in oil prices wreaking economic havoc in Canada's oil patch, loosening constraints on foreign acquisitions of oil sands businesses may be viewed as necessary to stimulate further investment in Alberta.

In 2015, the ICA's 2009 amendments were implemented, which established an enterprise value threshold for review (replacing a simpler but cruder "book value of assets" review threshold)—currently, at CA$600 million in enterprise value of the target Canadian business. This threshold will increase to CA$800 million in 2017 and to CA$1 billion in 2019. If the Trans-Pacific Partnership is implemented in Canada, it will raise the review threshold for non-SOE TPP investors to CA$1.5 billion in enterprise value (as will the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) for its members).

Focus on China

In 2015, China continued its efforts to streamline its regulations regarding foreign investment to encourage the gradual opening of China's markets. Of primary import was the release of a draft version of an updated Foreign Investment Law and a related Explanatory Note, released on January 19, 2015. The current draft represents a balance between reducing the regulatory burden on foreign investors and establishing greater control over attempts to avoid foreign investment regulation.

The major proposed changes under the draft Foreign Investment Law are as follows:

- A default principle of "national treatment" for foreign investors. This allows foreign investors to make investments on the same terms as Chinese investors without additional approvals or sector restrictions, except as otherwise required by law. Because foreign investments typically require numerous approvals at present, such a change would greatly streamline foreign investment.

- The adoption of a "negative list" approach in regulating market entry of foreign investors. China's State Council would set out industries where foreign investment is either restricted or prohibited. Sectors not on this "negative list" would be open to foreign investors on the same terms as Chinese investors. This approach has been adopted in the Shanghai Free Trade Zone.

- The principle of "de facto control" in determining whether a company should be treated as a foreign-invested enterprise (FIEs). To determine whether a domestic entity is under "de facto control" of foreign entities and should be classified as an FIE, authorities would conduct a more extensive analysis of the entities controlling an enterprise, rather than just examining its shareholders. This change is believed to target Variable Interest Entities (VIE), by which foreign investors avoided restrictions on foreign investment in certain sectors by establishing off-shore companies with contractual control over Chinese shareholders. It is unclear whether Chinese authorities would apply this change only prospectively, or also retroactively to companies that already use the VIE structure, such as Alibaba and Baidu. If adopted, this proposed change could have significant repercussions for foreign investors.

- No provisions regulating the corporate form of FIEs, whereas in past FIEs have been subject to different corporate rules and procedures than domestic enterprises. Commentators believe that this signals an intent to unify the treatment of FIEs and domestic enterprises under the PRC Corporate Law (or Partnership Law, as applicable), in terms of establishment, corporate governance, liquidation and other corporate matters. This may also imply eliminating the corporate forms unique to FIEs: equity joint venture, contractual joint venture and the wholly foreign-owned enterprise. If so, FIEs may need to convert to a corporate entity under the PRC corporate legal regime.

- Establishing a national security review system for foreign investments. Foreign acquisitions of a controlling stake in domestic enterprises have long been subject to a national security review by the State Council, but no formal statute governed this process. The draft law would seemingly provide more clarity for this process, as it is expected that implementation rules would be drafted detailing the national security review process. However, the draft law would also broaden the scope of such reviews to any investment, "where foreign investment infringes upon, or may infringe upon, national security." Current rules require a national security review only where foreign investors acquire sensitive military facilities, enterprises in the vicinity of key and sensitive military facilities, national defense, agriculture, energy and resources, infrastructure, transportation services, key technologies and major equipment manufacturing.

Though released in January 2015, the draft Foreign Investment Law has not been finalized and entered into force, and as a draft, it may undergo further changes before being finalized.

3. Cybersecurity and international data transfer governance to dominate the privacy agenda

In 2016, cybersecurity will dominate the agenda of the C-Suite. However, that will not be the only data governance concern for organizations. Re-tooling how organizations move data internationally will also be a major pre-occupation of general counsel and privacy officers.

Focus on the US

International data transfers will dominate the agendas of global businesses headquartered in the US in the wake of the Schrems decision by the European Union Court of Justice. On October 6, 2015, the EU Court declared that personal data cannot be transferred from the EU to the US in reliance on the recipient organization's Safe Harbor certification. The US Safe Harbor program allowed organizations to certify compliance with the Safe Harbor Principles and to voluntarily bring themselves within the jurisdiction of the Federal Trade Commission if they fail to comply with the Safe Harbor Principles. Although the European Commission has been working on a potential Safe Harbor 2.0, a US law that would grant Europeans the right to sue over data privacy violations in the US has been delayed in the US Senate. This delay complicated negotiations, since this has been a major political sticking point. However, as of the time of writing this article, political agreement had been reached on a so-called "EU-US Privacy Shield", which, according to the European Commission press release, "will protect the fundamental rights of Europeans where their data is transferred to the United States and ensure legal certainty for businesses." For further details and updates on this rapidly evolving story, please follow our blog.

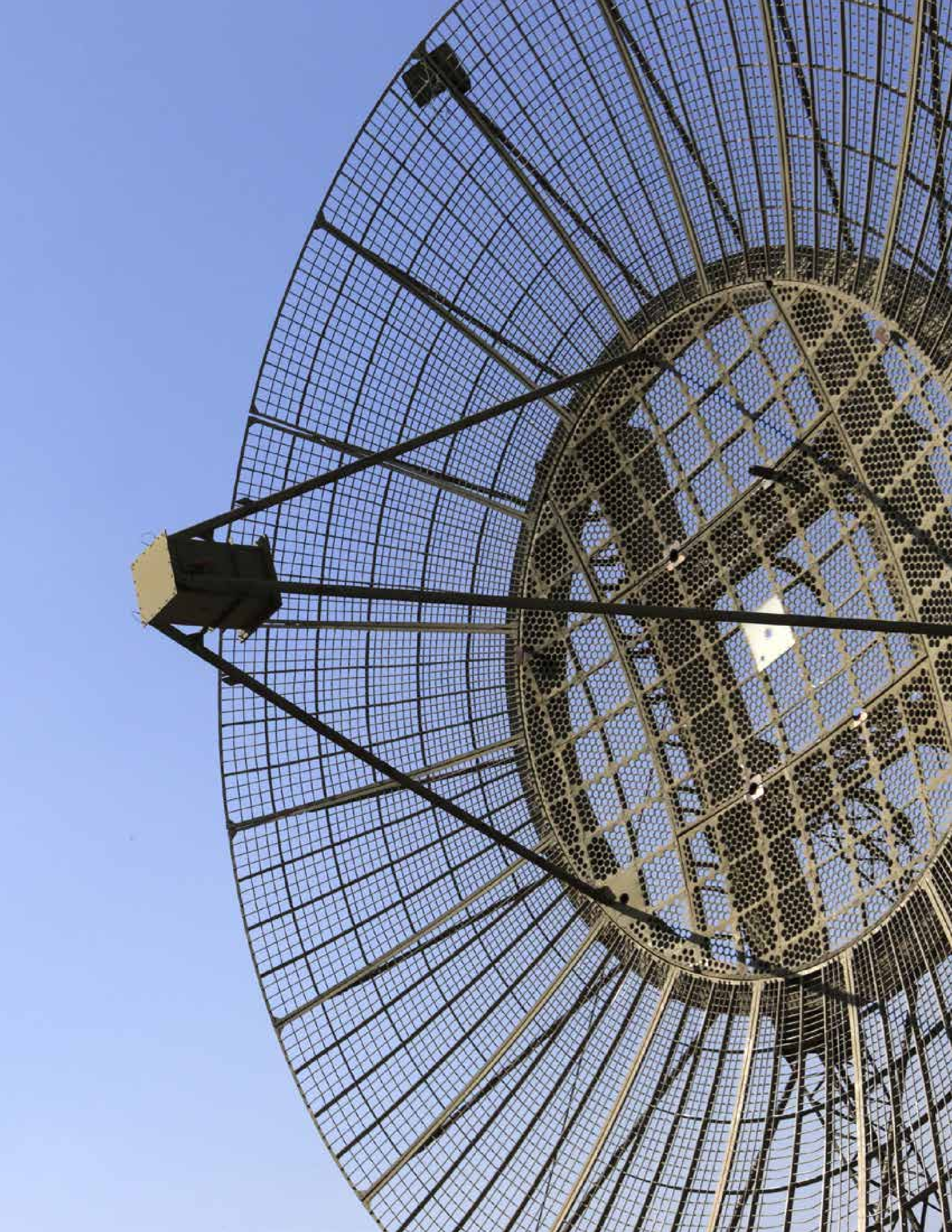
For now, organizations moving data from Europe to the US—including within a company or between companies in the same corporate group—should be working on mapping data flows and aligning those data flows with EU Standard Contractual Clauses (also known as Model Clauses), through which the transferor and transferee make binding commitments about handling the data that is the subject of the transfer. These clauses provide EU residents with third-party beneficiary rights to enforce these commitments and have been endorsed by the European Commission as still being viable methods by which to transfer data.

On the data security front, the *Cybersecurity Information Sharing Act* (CISA) was signed into law by President Obama on December 18, 2015, keeping cybersecurity high on the agenda as the year ended. The statute is intended to facilitate information sharing with the government about cybersecurity threats. The statute is not without its critics. Technology companies and civil libertarian groups have warned that the legislation is a major threat to privacy by allowing organizations to monitor all information on their systems without regard to whether it is personal information. Although personal information is supposed to be removed (if it is not relevant) when disclosing cybersecurity threat information to the government, there are questions about whether and how this will be done.

CISA was not the only regulatory initiative in the US in 2015. The Securities and Exchange Commission announced that its Office of Compliance Inspections and Examinations will continue to focus on cybersecurity controls at broker-dealers in 2016. The Food and Drug Administration has identified cybersecurity as a major threat to medical devices and has issued draft guidance to manufacturers. The National Highway Traffic Safety Administration has also put cybersecurity on the agenda, beginning with a roundtable held in Washington in January. There have also been several bills before Congress to enshrine vehicle cybersecurity into law.

Focus on Europe

In what may prove to be the biggest privacy development in 2016, the European Commission released its draft European General Data Protection Regulation (GDPR). The GDPR is an ambitious revamping of privacy law for EU members, which could come into effect in 2018 if approved by the EU Parliament. However, it has major implications for organizations operating outside of Europe. The GDPR would apply to the processing of personal data



of individuals who are located in the EU even if the entity that has collected or is processing the personal information is not located in the EU. The effect of this clause is to sweep in cloud services and online retailers that do not otherwise have any connection to the EU. Many organizations, such as those processing sensitive data, must designate a data protection officer and develop compliance programs. Fines for violating the GDPR could reach 4 percent of a company's annual worldwide turnover. Breach reporting to the appropriate national supervisory authority and individual notifications will be required. In addition, the GDPR provides individuals with greater rights to control their data. Among other things, individuals have a "right to erasure" when the data is no longer necessary to be used for the purposes for which it was collected or the data subject withdraws consent.

On the heels of the GDPR, the European Commission has announced agreement on the Network and Information Systems Directive (NISD) which, if approved by the European Parliament and the European Council, will impose significant cybersecurity obligations on operators of essential services and digital service providers (such as online e-commerce platforms and cloud service providers), who offer services in the EU. The NISD requires Member States to implement legislation that meets the minimum standards to manage cybersecurity risk in the NISD. The NISD will require organizations to take appropriate technical and organizational measures to manage cybersecurity risks and will require significant cybersecurity incidents to be reported to regulators.

Focus on Canada

Canada's position as an "adequate jurisdiction" for the purposes of international data transfers from Europe may come under closer scrutiny if the GDPR is enacted (see Focus on Europe). An "adequate jurisdiction" is a designation that allows for the free flow of personal data to Canada. In the wake of the international turmoil created by the Schrems decision (see Focus on the US), certain gaps have come to light. In particular, businesses are beginning to recognize that Canada is not an adequate jurisdiction in relation to the movement of employee data, except employee data used in connection with a federal work, undertaking or business (e.g., airlines, railways, and banks). Organizations that move human resources data between Europe and Canada urgently need to put into place contractual clauses to protect that information.

In 2014, Canada's Anti-Spam Legislation came into force and has had unexpected effects on Canada's participation in e-commerce channels. This draconian law requires opt-in express consent by recipients to commercial electronic messages unless certain exceptions apply. The law is out-of-step with anti-spam legislation with the US, which is, from an e-commerce perspective, Canada's most integrated trading partner. Unlike the US law, Canada does not exempt messages that are predominantly transactional and does not permit pre-checked, opt-out consent. Organizations are now finding that they have difficulties in conducting unified marketing programs. Worse, many US-based organizations have failed to appreciate that they need to comply with this legislation. In 2015, the Canadian Radio-television and Telecommunications Commission launched an aggressive enforcement campaign, which is not expected to abate in 2016. If that is not enough incentive for organizations to comply, the prospect of class actions should be; these are on the horizon as of July 1, 2017. Organizations would do well to get their compliance programs in order as soon as possible.

Cybersecurity also finds center stage in 2016 in Canada. The breach of security safeguards provisions in Canada's *Digital Privacy Act* are likely to come into force in 2016. Organizations will be required to log data breaches. Failing to do so will be an offence with the potential for a CA$100,000 fine. In addition, organizations will be required to report data breaches to the Office of the Privacy Commissioner of Canada and to make individual breach notifications if there is a real risk of significant harm. Importantly, the harms that are recognized are not limited to financial harms. They include embarrassment and reputational harm.

One uncertain development is whether Canada will enact legislation like CISA (see Focus on the US), or legislation similar to what is proposed in NISD (see Focus on Europe). The *Protection of Canada's Vital Cyber Systems Act* was being developed by the previous government and was intended to require companies operating vital systems to safeguard security and report hacking incidents to government agencies. Will that effort be shelved by the new Liberal government? Probably not; at least not completely. Cybersecurity was recently on the agenda of a meeting of justice and safety ministers from across the country. Our bet is that the new Liberal government will be compelled to do something on this topic, given the developments in Europe and in the US.

Focus on China

Organizations using encryption technology in China should take note of the recent Counter-Terrorism Law of China. This law contains obligations that require telecommunications operators and internet service providers to assist Chinese law enforcement conducting terrorism prevention or investigation activities by, among other things, providing access to decryption keys. Organizations are also required to implement systems to conduct surveillance of information systems for terrorist activities and to delete terrorism-related information. If you have not done so already, we recommend reviewing the application of this law as soon as possible.

Focus on data transfers and the Trans-Pacific Partnership (TPP)

The TPP has implications for international data transfers. In particular, signatories must not impede the international transfer of data or require that data be localized within their territory, subject to exceptions. For more on the TPP and Privacy, see our recent post.

4. Economic sanctions and trade

Easing of economic sanctions against Iran

The International Atomic Energy Agency's recent certification that the Government of Iran has met its obligations under the P5+1 Nuclear Agreement resulted in the United States and European Union relaxing substantial portions of their sanctions measures against Iran. The Agreement was concluded between Iran and China, France, Germany, Russia, the United Kingdom and the US on July 14, 2015, and constituted the roadmap to be pursued in ensuring that Iran's nuclear program remains exclusively peaceful. This has paved the way for increased commercial engagement with Iran and Iranian entities, and was the precursor to Canada's announcement on February 5, 2016 that it has also eased its economic sanctions regime.

The central components of the Joint Comprehensive Plan of Action (JCPOA)—the agreement ultimately concluded between Iran and the P5+1—are the roll-back of sanctions against the Iranian petroleum, petrochemical, oil and natural gas industries, restoration of financial ties with certain Iranian banks (including the Central Bank of Iran), and the elimination of the vast majority of US extra-territorial sanctions imposed after 2012.

With respect to the EU and the UK, the majority of the nuclear sanctions targeting Iran's energy, mining, financial and shipping sectors have been removed. In addition, technical assistance, financial assistance, brokerage services and insurance related to these sectors is now permitted. In the US, the Office of Foreign Assets Control issued guidance confirming that foreign affiliates and subsidiaries of US companies may engage in commercial activities involving Iran, provided that adequate controls are in place. Pursuant to Canada's recently amended sanctions, the blanket prohibitions on imports from Iran, exports to Iran and the provision of financial and other services to or from Iran have all been scaled back to a significant degree, subject to certain remaining restrictions.

While some sanctions remain in place in relation to the military and telecommunications sectors, the most significant legal obstacles to foreign commercial activity in Iran have now effectively been rescinded. Consequently, new trading opportunities will be opening up in Iran from both a strategic partnership and investment/expansion perspective. Businesses interested in undertaking commercial activities in Iran or with Iranian entities should therefore consider the evolving sanctions landscape in order to assess the potential for new or expanded markets.

The Trans-Pacific Partnership Agreement moves toward ratification

On November 5, 2015, the much-anticipated draft text of the TPP Agreement was released. In light of the release, businesses engaged in trading activities within the TPP zone can begin to analyze the potential benefits that may be leveraged as a result of tariff elimination and other preferential trading terms that will come into effect with the implementation of the TPP.

The draft text is the culmination of more than five years of often protracted negotiations between the 12 Pacific Rim countries that are parties to the TPP. The TPP is the largest trade agreement negotiated in the last 20 years, and is expected to substantially reduce barriers to trade and investment among its member countries, namely Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the US, and Vietnam. Together, these 12 TPP economies comprise 40 percent of global economic output and more than 800 million consumers, and span a region that is expected to constitute two-thirds of the world's middle class by 2030. The deepening of economic integration between member states that is expected to result from the implementation of the TPP will serve to facilitate the cross-border trade in goods and services, as well as foreign direct investment.

Although an agreement has been reached by the TPP members' trade representatives, the road to implementation may be long. The legal texts must be finalized and subjected to a legal "scrub," and the final text will then need to be implemented or ratified domestically by each of the 12 parties. Each member is expected to have completed its domestic implementation and ratification processes within two years of signing the TPP. That being said, even if some members have not ratified the TPP within this two-year timeline, the agreement will nonetheless come into effect as long as six of the original 12 signatories, representing 85 percent of the total GDP of the TPP economies, have successfully ratified. At present, there remains uncertainty with respect to the likelihood of ratification by certain key member states including, most notably, the US as the November 2016 Presidential election approaches.

The agreed-upon draft of the TPP text contains 30 chapters which address both standard trade agreement provisions and more novel content related to e-commerce, state-owned enterprises and capacity building. Among the most noteworthy TPP provisions are the following:

Market access/National treatment

At its most fundamental level, the TPP will substantially reduce, and in some cases eliminate, tariffs on thousands of products. The timing of tariff reductions varies depending on the product, with some reductions coming into effect immediately and others being phased in over several years. Businesses whose trading activities are expected to be affected by the TPP should therefore review each member country's respective tariff reduction schedules to assess the financial impact.

The TPP also contains a commitment for all member states to provide non-discriminatory "national treatment" to each other's goods, subject to certain limited exceptions.

Rules of origin

The TPP accords preferential duties to those goods that qualify as "TPP Originating" by containing a specified amount of content originating from the member countries. Specific rules of origin are prescribed for textiles and apparel, among other products. The TPP's rules of origin will be crucial to understanding how businesses may benefit from the TPP (through lower input costs or better access to export markets), and to what extent certain market participants will be challenged by increased import competition.

Technical barriers to trade

In the interest of creating a "fair, predictable and open regulatory system" that promotes the flow of goods, the TPP establishes rules governing product standards and conformity assessments. These rules focus on ensuring transparency and non-discrimination in the adoption and implementation of regulatory measures, and will have specific implications for the trade in wine and distilled spirits, medical devices, pharmaceutical products and cosmetics, organic products, and information and communications technology products that employ cryptography.

Intellectual property

The TPP is generally expected to strengthen intellectual property protections, particularly with respect to copyright and the enforcement of the rules pertaining to patent registration, trademarking, trade secrets, and counterfeit and pirated goods. The Agreement contains a prescribed process for addressing geographical indications (sometimes referred to as "appellations of origin", e.g. Scotch Whisky), and establishes a minimum period for data exclusivity with respect to biological pharmaceuticals. The TPP will also enable rights holders to seek redress where intellectual property rights have been violated across the TPP region, providing additional certainty and transparency with respect to intellectual property rights enforceability in member states.

Procurement

While the Agreement will grant TPP suppliers access to government procurement contracts within new TPP markets—specifically in Australia, Brunei, Malaysia and Vietnam—it also expands market access at the sub-national level in Chile, Peru and Australia, and with respect to certain US regional power authorities. The procurement rules established by the TPP are intended to encourage fair and open procurement procedures by creating rules on non-discrimination, transparency and impartiality.
It should be noted that Canada, the US and Mexico have also agreed to a separate mechanism that will harmonize the tendering provisions in the NAFTA's Chapter 10 with the new standards set out in the TPP.

Electronic commerce

Electronic commerce has so far been the subject of few coordinated international regimes. TPP member states have agreed to a set of rules that prohibit the application of duties to products that are transmitted electronically, that prohibit the mandatory localization of servers as a condition for serving a market, and that seek to protect against the unauthorized disclosure of users' personal information. The TPP also addresses fraudulent and deceptive commercial practices, and the dissemination of unsolicited commercial electronic messages.

Transparency and anti-corruption

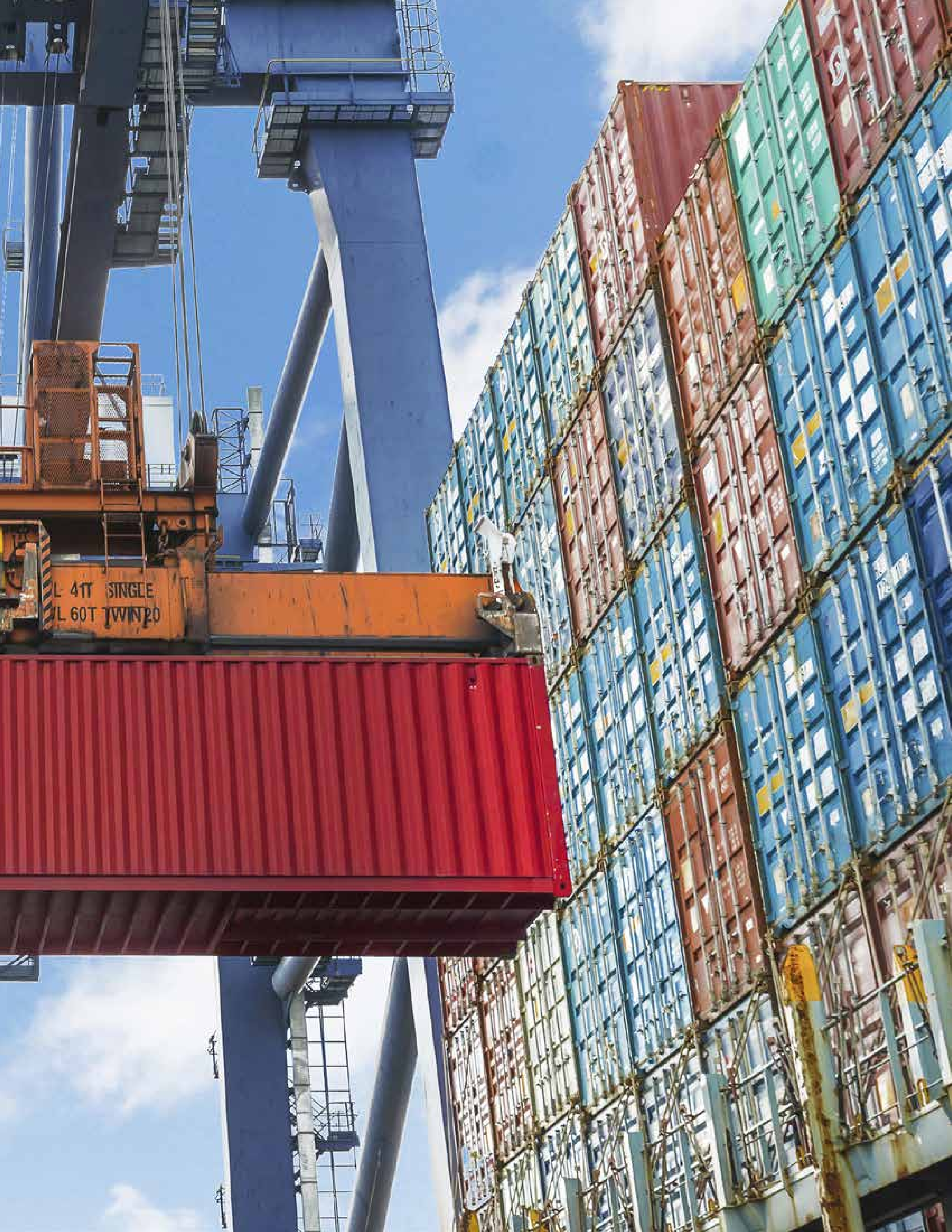
The TPP seeks to reduce corruption and enhance transparency in cross-border trade and investment by setting new ethical standards in the Asia-Pacific region. However, it is notable that these provisions are not subject to the TPP's dispute settlement mechanisms, addressed below. If properly implemented by the member countries, the transparency commitments of the TPP may be beneficial to stakeholders and their advisors in global restructurings, by ensuring they have access to government information that allows them to better understand the local market and regulatory dynamics.

Investor-state dispute settlement

Chapter 9 of the draft TPP contains investment-related commitments, and establishes a dispute settlement mechanism allowing investors of a member state to make a claim against a foreign member state where the investor believes the investment-related commitments of the TPP have been breached by the host state. The non-discriminatory treatment guaranteed to qualifying investors and investments under the TPP is subject to certain exceptions, for example, those that apply in respect of environmental protection measures. The draft TPP text contains the typical protections usually seen in international investment agreements, including a minimum standard of treatment protection. Another key feature is a "denial of benefits" provision for enterprises. This specifies that in order to obtain the protections of the TPP, an enterprise must have "substantial business activities" in the territory of another member state.

The road forward

As the tariff reductions come into force, some industries will face increased import competition as a result of the TPP. Multiple factors might affect the success of an industry aside from trade liberalization, and isolating the impact of trade agreements from other factors buffeting a particular industry is challenging at the best of times. That said, the TPP is not yet finalized and will not come into effect for many months (or even years), and accordingly, businesses engaged in trading activities within the TPP zone have time to review their supply chains, commercial strategies, and balance sheets in order to assess their opportunity for, or vulnerability to, offshore competition.


L 41T SINGLE
L 60T TWIN20

5. Anti-corruption

Focus on the US

An active FCPA docket anticipated

When compared to prior years, 2015 was relatively quiet for *Foreign Corrupt Practices Act* (FCPA) enforcement actions in the US. Although the total number of enforcement actions was slightly higher than the previous year, there was an absence of the very large monetary settlements that garnered enormous attention in the recent past. This record, combined with continued criticism that their enforcement actions in the past failed to hold individuals accountable for violations of federal law, including the FCPA, may be the reasons for two significant changes in the government's approach to enforcement. This raises the question as to whether the coming year will be much less quiet than the previous year.

In a September 2015 DOJ Memorandum titled, "Individual Accountability for Corporate Wrongdoing", US Deputy Attorney General Sally Yates hit the reset button on policies that govern the investigation and possible prosecution of corporate misconduct. The most significant 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..." Applying this policy to FCPA enforcement investigations would require the company to disclose information it had regarding any employees, business partners or anyone else that had a role in the bribery violation to get the "cooperation credit." This "cooperation credit" has in the past been a key mitigating factor in the DOJ's charging decisions and subsequent punishment for corporate wrongdoing. Whether intended or not, the *Yates Memorandum* makes the in-house counsel's job much harder. In simple terms, in-house counsel and their outside counsel will have to carefully consider the legal and ethical issues that present themselves when it appears not everyone in the conference room agrees with what course to take to mitigate the legal risks associated with bribery allegations.

The second noteworthy FCPA development was a public acknowledgement by the DOJ last October that it would use a more proactive approach to its investigations. This approach stands in stark contrast to prior years when it relied heavily on corporate self-disclosure to generate investigative leads. The change, according to DOJ spokesperson Peter Carr, was designed to focus on "bigger, higher impact cases." The different approach, coupled with a tripling of the agents responsible for FCPA investigations, suggests that the Department will use high-profile actions, including prosecutions of culpable individuals, to address what it believes to be an opportunistic environment for anti-bribery investigations and prosecutions. Based on similar increases in investigative agents in the past (i.e., relating to health care fraud), it is likely that 2016 will see a significant increase in the volume, size and magnitude of FCPA investigations and possible prosecutions.

What remains unclear is the collateral or secondary repercussions of these changes. While it is clear that US-based individuals have greater exposure after these developments, it is less clear whether the countries where the conduct took place will also step in following the mandated disclosure under the *Yates Memorandum* and initiate their own prosecutions. The policy will certainly make it easier for them to prosecute their citizens after the company discloses their conduct. History suggests they will do so as there were instances in 2015 when countries used disclosures and settlements made in the US, as well as formal and informal agreements to collaborate with that country's investigative agencies, to pursue their own enforcement actions. It is uncertain where this strategy will be used in 2016; the only way to know for certain is to put the question to enforcement personnel where the secondary action might be brought. In the meantime, the US government's recent course changes certainly suggest an active anti-bribery docket in 2016.

Focus on the UK

Serious Fraud Office agrees to first Deferred Prosecution Agreement and more are likely

Since the UK *Bribery Act* (UKBA) took effect in mid-2011, we have been waiting for the first prosecution for the "failure to prevent bribery" offence—the UKBA's initiative to make covered businesses responsible for bribery committed by agents and intermediaries (and not necessarily affiliates) anywhere in the world for the benefit of the covered business. Since February 2014, UK enforcement agencies have had the power to agree to so-called deferred prosecution agreements (DPAs) with corporations who commit a range of offences, including offences under the UKBA and money laundering legislation. Following a court hearing in November 2015, the Serious Fraud Office (SFO) confirmed the approval of the first DPA. The DPA relates to the conduct of an affiliate of Standard Bank plc (now ICBC Standard Bank plc) in connection with a fundraising for the Tanzanian government. Two senior executives of the sister company appointed an agent, with the promise of paying it one percent of the amount raised. Two of the three shareholders of the agent were related to the government, and the transaction moved swiftly after the agent's appointment. Standard Bank was ultimately alerted and made reports to the SFO and the UK agency then responsible for processing reports of money laundering suspicions. The SFO and the relevant judge agreed there was no prospect of Standard Bank claiming it had adequate procedures (which would have been a defence), and that it had, therefore, breached the UKBA. The SFO and the judge agreed on a DPA rather than an immediate prosecution, so provided Standard Bank meets the conditions of the DPA, the prosecution, currently stalled, will be dropped in three years' time.

The SFO said that the case had proved where the "high bar" for co-operation could be. The SFO had previously indicated that for it to consider a DPA as an appropriate alternative, there would need to be a high degree of willingness to cooperate and that this should prove to be the case in fact. The SFO advised that any company considering this route should take note that, although "adequate procedures" were not discussed in this particular case, the important thing is to assess the situation as it arises and take appropriate action. For example, regardless of what any procedures might say, if a red flag seems obvious, it should be treated as such. The judge's comments on how Standard Bank acted once it became aware of the problem were also of key importance. The SFO has suggested the bank's conduct was a prime reason for the SFO deciding a DPA was appropriate, and stressed it would use DPAs only when a narrow set of specific factors suggested it would be the best route. But we expect at least one more to follow soon.

While we still await the first prosecution or DPA that analyzes whether procedures were "adequate" for the purposes of the defence to a "failure to prevent" an offence, this case is the first illustration of how DPAs are likely to operate in the future. It also shows that the SFO expects to be alerted sooner rather than later, so the timing of liaising with enforcement agencies will be essential.

In other legislative developments in 2015, the government confirmed it would not be extending the "failure to prevent" offence to other financial crimes, but introduced statutory protection for those who report suspicions of money laundering in good faith.

Focus on Canada

Continued anti-corruption crackdown

In 2015, Canada saw a crackdown on anti-corruption as enforcement authorities laid charges and investigated a number of cases under the *Corruption of Foreign Public Officials Act* (CFPOA).

For example, in January 2015, RCMP officers raided the Toronto office of MagIndustries Corp., a public company listed on the TSX that is controlled by a Chinese company and has subsidiaries in the Republic of Congo, where it is developing a CA$1.5 billion potash mine. The allegations reported (none of which have been proven) include improper payments to Congolese officials. There is wide speculation that the RCMP could lay charges in 2016.

In February 2015, the RCMP charged SNC-Lavalin Group Inc. and affiliated entities (SNC) with one count of corruption under the CFPOA (as well as fraud under the *Criminal Code*). The corruption charge stems from SNC's business dealings in Libya. It is alleged that over a period of 10 years, commencing in 2001, SNC, through agents, gave, or offered to give, approximately CA$48 million to Libyan officials, including the son of former Libyan dictator

Muammar Gaddafi, for the purpose of securing benefits. The RCMP investigation led to convictions in Switzerland of former SNC executives for corruption and money laundering related to SNC's activities in Libya. In a related development, SNC announced in December 2015 that it had reached an administrative agreement with Public Works and Government Services Canada, allowing it to avoid a federal bidding suspension (which otherwise would have applied under the federal government's Integrity Regime).

Looking ahead, it is reasonable to assume there will be more enforcement activity under the CFPOA in 2016. Enforcement authorities have demonstrated in recent cases that they are willing to bring charges of international corruption against individual executives of companies (either located in Canada or abroad), in addition to the companies themselves. They are expected to do so with ever increasing vigor, particularly if they achieve some measure of success in any of the ongoing cases.

Domestic corruption was also the focus of attention in 2015, and this is likely to continue in 2016. November 2015 saw the publication of the final report of the Québec Commission of Inquiry on the Award and Management of Public Contracts in the Construction Industry (better known as the "Charbonneau Commission"). The report detailed extensive corruption, bribery and other improper schemes in public contracting for construction services in the province and made 60 recommendations on how to clean up the problem. The Government of Québec has insisted that it is keen to implement the recommendations of the report and there is likely to be significant activity on this front in 2016.

One of the recurring themes of the Charbonneau Commission inquiry was that the problems observed in Québec were also present in other provinces. Accordingly, as the Government of Québec deals with its serious construction industry corruption problems, it is expected that other provinces will closely monitor the situation and may decide to follow some of the steps taken by Québec.

Whistleblower protections were also a key theme that acquired fresh prominence in 2015. The Charbonneau Commission report made a number of recommendations touching upon improvements to whistleblower protections but perhaps the most profound change in this regard was the announcement by the Ontario Securities Commission (OSC) that it would be introducing a whistleblower bounty program, the first time in Canada that significant whistleblower bounties have been proposed by a regulatory authority. The new policy—which is expected to come into force in the Spring of 2016—demonstrates the importance the OSC attaches to encouraging whistleblowers to come forward with information about violations of securities law, and it will be interesting to see whether information received under the new policy will lead to more enforcement and whether other regulatory authorities will follow with their own whistleblower bounty programs.

Contributors

Editor: Sandy Walker

US

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

Michael E. Zolandz (National Security)
Partner, Washington, DC
D +1 202 408 9204
michael.zolandz@dentons.com

Kenneth J. Nunnenkamp (National Security)
Partner, Tysons
D +1 703 574 4241
kenneth.nunnenkamp@dentons.com

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

Europe

Dr. Jörg Karenfort (Competition/Antitrust)
Partner, Berlin
D +49 30 26 47 33 05
joerg.karenfort@dentons.com

Emma Radmore (Anti-corruption)
Managing Associate, London
D +44 20 7246 7206
emma.radmore@dentons.com

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

Canada

Sandy Walker (Competition/Foreign Investment)
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 (Cybersecurity/International Data Transfer)
Partner, Toronto
D +1 416 863 4424
timothy.banks@dentons.com

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

Carmen Francis (Trade)
Associate, Toronto
D +1 416 862 3452
carmen.francis@dentons.com

China

Jet Deng (Competition)
Partner, Beijing
D +86 10 5813 7038
zhisong.deng@dachenglaw.com

Ken Dai (Competition)
Partner, Shanghai
D +86 21 5878 1965
jianmin.dai@dachenglaw.com

Todd Liao (Foreign Investment)
Partner, Shanghai
D +86 21 2315 6028
todd.liao@dentons.com

Dentons is the world's first polycentric global law firm. A top 20 firm on the Acritas 2015 Global Elite Brand Index, the Firm is committed to challenging the status quo in delivering consistent and uncompromising quality and value in new and inventive ways. Driven to provide clients a competitive edge, and connected to the communities where its clients want to do business, Dentons knows that understanding local cultures is crucial to successfully completing a deal, resolving a dispute or solving a business challenge. Now the world's largest law firm, Dentons' global team builds agile, tailored solutions to meet the local, national and global needs of private and public clients of any size in more than 125 locations serving 50-plus countries. www.dentons.com.