BRIEF LOOK AT THE SUBMARINE CABLE LANDSCAPE: RECENT CHANGES IN EU AND US REGULATION

Andrew D. Lipman and Ulises R. Pin
Email: andrew.lipman@morganlewis.com

Morgan, Lewis & Bockius LLP, 1111 Pennsylvania Ave. NW, Washington, DC 20004

Abstract: A changing geopolitical climate and increased focus in on cybersecurity and national security concerns, including ownership of critical infrastructure, will impact submarine cable development in the coming years globally. Changes in the United States and the EU regulatory landscape in recent years have reflected a growing sense of heightened economic nationalism on both sides of the Atlantic Ocean, even as the EU looks to make changes that lead to greater unification in the regulatory environment.

In the United States, the political landscape has resulted in heightened national security review of transactions involving foreign investors and which involve critical infrastructure, such as submarine cables. The Team Telecom review process involves more scrutiny in recent years and has become even more time consuming during the current administration, adding significant time concerns and uncertainty to the process of landing a new cable or obtaining control of a cable touching the United States. Combined with the passage of legislation expanding the scope of CFIUS regulations and the reversal on net neutrality, international and intercontinental submarine cable owners and operators must navigate an increasingly complex legal and regulatory landscape.

In recent years, the EU has set a number of regulatory frameworks that impact the telecommunications sector. Notably, the General Data Protection Regulation overhauls EU data protection legislation. Recently, the EU also adopted a unified Electronic Communications Code, and has made political agreements on both a framework for screening foreign direct investments into the EU and a Cybersecurity Act to address security issues impacting critical infrastructure across the EU. Similar to the United States, the movement of EU towards protectionist national security rules will also be a significant consideration of submarine cable operators when designing new networks and acquiring existing systems touching Europe.

1. INTRODUCTION

As the global demand for data continues to grow at an extraordinary rate, a changing geopolitical climate and increased focus in on cybersecurity and national security concerns, including ownership of critical infrastructure, will continue to impact submarine cable development in the coming years. With more than three billion current Internet users, Internet traffic is anticipated to reach 30 gigabytes per capita by 2021. Given their capacity, speed and security, submarine cables, which carry over 99% of all international communications, remain the preferred medium for transporting Internet traffic.

Recent changes leading to greater unification in the regulatory environment, particularly in the European Union or "EU", point toward harmonization of regulatory requirements with respect to trans-Atlantic submarine

cable routes. However, an increasingly politicized environment resulting in heightened economic nationalism also creates impediments to investment in, and deployment of, submarine cable networks, particularly in the United States and the EU.

Let's briefly explore some of the regulatory considerations on the horizon and how they may impact submarine cable licensing and operations in the coming years.

Certain countries, including the United States, the United Kingdom and several EU members, are becoming increasingly economically nationalistic, spurred by drivers such as trepidations about terrorism, foreign policy and, in some instances, sluggish economic recovery or promotion of local economy. For example, in the U.S., there was some recent debate about whether to extend the Jones Act to ships that lay and repair submarine cables, thereby requiring that ships be built in the U.S. and have a majority of the crew as U.S. citizens. However, parties in opposition have strongly argued that such measures would have a detrimental impact on the efficient protection of critical submarine cable infrastructure that spans the globe, and the proposal has been halted for the time being.

The emergence of China as a new counterbalance to American hegemony in the world and its well-publicized acquisitions of critical technologies in the West coupled with the highly politicized environment in the United States and Europe has resulted in economies less open to foreign investment, particularly with respect to China, the Middle East and Russia.

First, we will dive into the U.S. regulatory landscape and the regulations that are affecting submarine cables today. Next, we will take a look at the EU and its recent changes that seem to be leading to greater unification in the regulatory environment.

2. THE U.S. REGULATORY LANDSCAPE

The marked increase in economic nationalism and protectionism in the United States has resulted in heightened national security review of transactions involving foreign investors and which involve critical infrastructure, such as submarine cables. Combined with the recent reversal on net neutrality rules in the United States and regulatory changes in the EU, international and intercontinental submarine cable owners and operators must navigate an increasingly complex legal and regulatory landscape.

National Security Review. As many of you may already know, the Federal Communications Commission, or FCC, regulates submarine cable landings in the United States. Operators of submarine cables must obtain an FCC license pursuant to the Submarine Cable Landing License Act of 1921 and Section 1.767 of the FCC's Rules. Although the application process for a submarine cable license may theoretically be completed in as little as 45 days from the date the application is put on public notice; in practice, the FCC licensing process tends to take significantly more than 45 days, largely due to the national security review process conducted by "Team Telecom", an *ad hoc* task force comprised of the Departments of Defense, Homeland Security, and Justice, including the Federal Bureau of Investigation. Because most subsea cable applications have some level of foreign ownership or participation, submarine cable landing license applications are subject to such national security reviews. In addition to these reviews, acquisitions of submarine

cables and other U.S. telecommunications networks may also be subject to potential review by the Committee on Foreign Investment in the United States, also known as CFIUS.

As the specter of cyberterrorism increases internationally and the United States becomes increasingly more protective of its critical infrastructure, the process for obtaining national security approvals has become more onerous. The Team Telecom review process involves more scrutiny in recent years and has become even more time consuming during the Trump Administration. This national security review adds significant time concerns and uncertainty to the process of landing a new cable or obtaining control of a cable touching the United States. The FCC will rarely grant a submarine cable landing license in fewer than six months where Team Telecom review is required, and in recent years a twelve-plus-month review period has not been uncommon. If you add delays due to the recent U.S. government shutdown or any future shutdowns, the timeline for approval may be even longer.

National security issues have become more complex in recent years with the increase in globalized supply chains and the increase in the number of transactions involving emerging technologies and sensitive data of U.S. citizens. For example, U.S. sensitivities to Chinese investments in sensitive technologies such as semiconductors have resulted in certain transactions being blocked on the basis of national security concerns. This can be seen percolating into the telecommunications arena as well, for example, in the form of the recent rejection of applications by Chinese carriers (*e.g.*, China Mobile) or in projects otherwise involving use of Chinese equipment (e.g., Huawei or ZTE).

Historically, for a new submarine cable system, Team Telecom would conduct a review if (1) the system will connect the United States to a foreign point, or (2) the system will have aggregate direct or indirect foreign ownership of 10 percent or more. However, in the recent past, submarine cable applications by 100% American investors have also been subject to Team Telecom scrutiny.

As part of the process, Team Telecom asks the applicants a series of questions, commonly known as "triage questions," pertaining to issues such as equipment type, storage and security of network data and other physical security information, encryption key usage, and entities with access to the applicant's network and data. Where particular ownership, operational, or financing arrangements raise concerns, Team Telecom will typically make additional inquiries and information requests. This process normally results in the removal of the application from streamlined processing at the FCC and the withholding of FCC approval until Team Telecom's review is complete.

Team Telecom review often results in required letters of assurances or network security agreements as a condition for FCC license approval. These agreements are viewed as critical to facilitating surveillance programs conducted by U.S. national security and law enforcement agencies, for example, the National Security Agency, as well as for preventing foreign governments from gaining visibility into U.S. telecommunications networks. Provisions of such agreements frequently include limitations on equipment types used, or requirements to establish a network operations center ("NOC") located

domestically and operated by screened U.S. citizens.

While there are few reported cases of applications denied based on Team Telecom and CFIUS concerns, applications often languish for months without progress, given that Team Telecom is not constrained by any statutory timeframes for review. In an open proceeding, the FCC proposed a 90-day shot clock on Team Telecom review in a recent reform proceeding, but this process is moving at glacial pace in Washington D.C.

In addition, legislation to revise CFIUS regulations was signed into law. The legislation expanded the scope of CFIUS reviews to include matters that are currently only considered by Team Telecom, smaller minority investments, or arrangements involving the contribution of intellectual property or certain types of services with sensitive implications. This has resulted in a wider range of transactions falling within CFIUS's jurisdiction. Among other things, the law also requires the executive branch to prepare regular reports on foreign direct investment made by Chinese entities, and provides that CFIUS may consider whether a covered transaction involves a "country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology."

Net Neutrality. Net Neutrality – the concept that Internet service providers must treat all data on the Internet the same, regardless of content – is an issue of broad and current interest vis-à-vis access to broadband networks, including ultra-high broadband networks, such as submarine cables. The United States has recently taken a step back with respect to the paradigm of open network access, despite adoption of EU-wide net neutrality rules, which prohibit blocking, throttling or discrimination with respect to online content, applications and services.

In December 2017, the FCC reversed the landmark Obama-era net neutrality rules, which aimed to establish a level playing field on the Internet by preventing broadband companies from slowing down or providing paid-for priority for certain types of traffic. This controversial decision in a highly contentious proceeding has sent the message that under the current Trump Administration, there is more of a free market, less regulatory approach; although its ultimate impact on the regulatory environment remains up for debate through legislative efforts in Congress and the states as well as ongoing appeals in the U.S. courts.

The ongoing debate regarding net neutrality in the U.S. and resulting impact it could have on other regulatory frameworks over time remains an issue to watch given that the divergent treatment of Internet content delivery could influence the demand for capacity on submarine cables. While the inconsistencies between the U.S. and EU net neutrality regulatory schemes and potential effects on price structuring and other business decisions will, in large part, be borne by last mile and Internet Service Providers, the impact could also trickle down to content transport mechanisms. A laissez-faire capitalistic mechanism that allows parties to sell priority access to those with the means to pay a premium for increased speed and lower latency on one end of a network and a protectionist prohibition on discrimination with respect to content provision on the other, could make it difficult for a trans-Atlantic cable operator to set consistent pricing rules and expectations.

3. EU TELECOMMUNICATIONS REGULATION

The European Union has set a number of regulatory frameworks that impact the telecommunications sector. Most notably, the General Data Protection Regulation, also known as the GDPR, is a significant overhaul to EU data protection legislation and aims to protect its residents' personally identifiable information and "right to be forgotten." In December 2018, the EU has also adopted a unified Electronic Communications Code providing EU-wide telecommunications regulation, and has made political agreements on both a framework for screening foreign direct investments into the EU and a Cybersecurity Act to address security issues impacting critical infrastructure across the EU. On one hand, the unification of EU regulations addressing data protection, electronic communications, and foreign investment are welcome changes for international and intercontinental submarine cable owners and operators, simplifying the number of regulatory regimes touching a cable system. On the other hand, however, some of these regulations impose onerous requirements and harsh penalties for noncompliance, reaching new technologies and services not contemplated under prior regulatory frameworks.

Finally, similar to the United States, the EU has recently begun moving toward more protectionist measures with respect to critical infrastructure and access to these networks by foreign nationals. Adoption of new EU-wide national security rules will be a significant consideration of submarine cable operators when designing new networks and acquiring existing systems touching Europe.

Let's explore some of these issues at a high level and discuss how they intersect with regulations across the pond.

GDPR. The GDPR, which is intended to unify data privacy requirements across the EU, took effect May 25, 2018. The GDPR establishes a technology neutral, uniform framework for data protection legislation across the EU, replacing individual countries' separate data protection laws. This framework levels the playing field with respect to data protection regulation in the European Union, easing the burden for entities that offer services in multiple countries, which will no longer need to comply with multiple regulatory regimes but instead only need to interface with a single data protection authority in most cases.

The GDPR applies widely to organizations that collect and process data for their own purposes, which are called "controllers", as well as to organizations that process data on behalf of others, which are called "processors". Specifically, with respect to entities domiciled in the EU, the GDPR applies to the processing of anyone's personal data collected in the context of the activities of such organization. In addition, entities established outside the EU are also subject to the GDPR with respect to the processing of personal data that applies to EU residents.

Under the GDPR, companies may only collect and process personal data that has not been rendered irreversibly anonymous for specified legitimate purposes and processing must be limited to the data necessary to fulfil such purpose, only for as long as necessary. Companies that collect "sensitive information" that pertains to, for example, an individual's health, race, sexual orientation, religion, political beliefs or trade union membership, are subject to additional processing constraints and may need to implement additional safeguards, such as encryption, to protect the data.

Telecommunications companies with capacity on international submarine cable routes must take measures to ensure the security, integrity and confidentiality of personal data and must maintain detailed internal records of processing activities to ensure compliance with the GDPR. In particular, providers must assess whether they would fall within the broad purview of the GDPR, even if their networks do not directly touch the EU, and must understand the types of data that may be collected and must be protected in their roles as data controllers or providers. Failure to comply with the GDPR may result in significant fines of up to EUR 20 million or 4% of a company's global turnover. In addition, consumers may bring civil litigation against entities for breach of the GDPR.

The tension between the cybersecurity and privacy frameworks established in the United States and Europe is readily apparent. On the U.S. side, the government has a significant national security interest in gaining additional visibility into networks, particularly those involving critical infrastructure with foreign ownership, and seeks access to information and content that flows through networks touching U.S. territories. Conversely, European regulators have declared long-arm jurisdiction to protect the individual liberties and fundamental privacy rights of their residents, in particular with respect to the processing of their personal data.

Submarine cable operators thus find themselves in a difficult position having to simultaneously comply with incongruent regulatory requirements, which could, in turn, lead to an increase in litigation. For example, issues involving the recently-passed Cloud Act in the U.S. (which may provide U.S. law enforcement agencies access to data stored outside of the U.S.) and compliance with the EU's GDPR are directly at odds. It follows that the increased risk of litigation associated with cybersecurity, privacy requirements and legal compliance issues in multiple jurisdictions requires additional resources to be allocated within an organization, which could thereby drive up the cost of bandwidth.

EU Electronic Communications Code. In addition to a harmonized data protection framework under the GDPR, the EU recently adopted a unified Electronic Communications Code, an EU-wide telecommunications regulation aimed at promoting investment, competition and innovation and preparing Europe for 5G services and ultra-high broadband connectivity. The Electronic Communications Code includes measures such as: introducing new provisions to support the roll-out of very fast networks capable of gigabit per second speeds; broadening the scope of the legislative framework to cover new communications tools, such as 'over-the-top services;' proposing changes to radio spectrum management; and providing affordable functional Internet access to end-users. As with the GDPR, the Electronic Communications Code subjects submarine cable operators with multiple landing points within the EU to a single regulatory regime, where they would otherwise have to comply with the regulations of each individual member state in which they intend to land. The Code must be implemented in national legislation by December 21, 2020.

National Security Review in Europe. For acquisitions of telecommunications network assets by non-EU nationals, countries such as Germany, Italy and France are increasingly requiring critical infrastructure national

security filings similar to those required by CFIUS in the United States. As with the CFIUS process, these reviews have the potential of exacerbating nationalism and potentially blocking network acquisitions by foreign investors on the grounds of cybersecurity.

Moreover, late last year, the EU reached a political agreement on an EU framework for screening foreign direct investment. The new framework creates a cooperation mechanism where Member States and the European Commission will be able to exchange information and raise specific concerns, and allows the European Commission to issue opinions in cases concerning several EU Member States, or when an investment could affect a project or program of interest to the whole EU. However, it will not affect the Member States' ability to maintain their existing review mechanisms, to adopt new ones or to remain without such national mechanisms, and the Member States have the last word whether a specific operation should be allowed or not in their territory.

In addition, the EU reached a political agreement on the proposed EU Cybersecurity Act, which aspires to address and prevent network and information security incidents, provide guidance on security of critical infrastructure across the EU, and create a framework for European Cybersecurity Certificates for products, processes and services that will be valid throughout the EU. While the proposed measures do not impede further national actions in terms of national security matters, the Cybersecurity Act would likely provide greater uniformity and predictability for telecommunications companies in terms of compliance with a cybersecurity framework and transaction review process.

These additions of potential European reviews will likely to inject additional uncertainty and delay into transactions involving the acquisition of telecommunications networks and critical infrastructure in Europe, including submarine cables landing in EU member countries.

4. CONCLUSION

As you can see, the demand for international and intercontinental submarine cable capacity shows no sign of abating in the near term. The recent changes in national security review procedures as well as data protection and content delivery regulations in the U.S. and EU are just a few examples of the complex legal and regulatory environment that must be navigated by entities that own or operate international submarine cables as well as those providing content or services over the cable systems.