On 5 August 2020, the US State Department announced the expansion of the Clean Network, which includes a number of programs intended to safeguard US assets and protect US IT from interference by malicious actors. The document explicitly names the Chinese Communist Party (CCP) as one of these malicious actors, and enterprises with ties to the CCP are directly targeted. In particular, the Clean Network aims to protect the sensitive personal and business information of US citizens and covers areas such as clean carriers, stores, applications (apps), cloud and cable. The goal is to prevent malign apps, networks and equipment from being used to connect to systems containing US citizens’ information. It defines what is safe and what is not. This is one of many recent actions that signal an emerging techno-nationalism. Techno-nationalism is defined as mercantilist behavior that links technological innovation and enterprise directly to the security, prosperity and stability of a nation. Thus, if individuals and enterprises want to prosper in the United States, they must abide by its rules.

One of the key issues is the 2017 Chinese National Intelligence Law, which mandates that all Chinese individuals, organizations and institutions assist public and state security officials in performing national intelligence work. According to one interpretation of the law, when the state needs a Chinese enterprise or entity to perform intelligence work—more commonly known as spying—it must do so. This means that data stored in a Chinese cloud, passing through a Chinese network or stored on Chinese equipment may be subject to this law. The United States has its own law that gives law enforcement and intelligence agencies similar powers to obtain information, called the USA FREEDOM Act. The major differences between the two laws are the extent to which they limit these powers and their control and oversight mechanisms. Digital mass surveillance powers can be problematic if they are misused. However, in this context, they can be used to weaponize digital assets that straddle national borders. This concern is not limited to China and the United States; it exists in many other countries as well.

How is this relevant to censorship and privacy and IT practitioners? Censorship and legal intercept (which affect privacy) are two of the most powerful cybertools in a nation-state’s arsenal. The ability to
regulate communications (i.e., censorship) and collect information (i.e., privacy) can go a long way in fighting crime and preventing terrorist threats. However, when misused, these tools can suppress legitimate speech and violate personal privacy rights. Different countries have different legal standards regarding what kinds of speech may be censored and different standards of due process and oversight. This disparity is partly due to cultural differences. What is disallowed in one country might be allowed in another (e.g., hate speech, lèse-majesté). Practitioners who implement digital platforms and handle information security must be cognizant of this evolving legal landscape or risk being on the wrong side of the law. Different countries have different legislative frameworks (e.g., copyright laws, privacy laws, antiterror laws) that include safe-harbor provisions for platform and service providers. This creates additional challenges with respect to implementation.

These laws were written based on the assumption that physical boundaries impose limits on enforceability. However, with the pervasiveness of the Internet, these lines are no longer clear. For example, lèse-majesté laws historically applied to publishers within a given country. In the past, these publishers either printed or physically distributed materials within that country’s geographic boundaries, so censorship could be achieved through physical enforcement. But what happens when a citizen of a certain country posts content in violation of lèse-majesté in a blogging platform based in another country? Because this blogging platform is available on the Internet, it is possible for people in said country to read the banned content. The situation can become more complicated if the blogger is not a citizen of the country in question. In this case, service providers may be expected to enforce the country’s censorship standards, such as Thailand requiring Facebook to block certain content. Facebook, being a large, established platform with many resources, can do so, but what about smaller platforms? Enforcement can be a substantial burden. Do smaller platforms have to be cognizant of the many different laws in various countries? Does this requirement impose entry barriers to particular markets?

Consider legal intercept and the right to privacy. Each country has different rules with respect to legal intercept. Some require court orders (including from special courts, such as the US Foreign Intelligence Surveillance Court [FISA court]), some require only a request from a designated office (e.g., the anti-money laundering office) and some allow any law enforcement official to make a request. In addition, the criteria for obtaining information vary from country to country. Some require probable cause or just reasonable suspicion of wrongdoing, and some require no reason at all. The different platforms interpret these rules to the best of their abilities given the legal regimes with which they are familiar. Similar to the issue of censorship, when Internet platforms cross borders, they are subject to all the different laws related to legal intercept, which can lead to confusion. There are several questions that need to be asked, including:

- Which laws should platforms implement?
- Which standards should be used?
- Can countries with weaker privacy protections request data from global platforms more easily than those with stronger protections?
- What rules do small or emerging platforms use to ensure that they are compliant with the laws of different countries?

"SIMILAR TO THE ISSUE OF CENSORSHIP, WHEN INTERNET PLATFORMS CROSS BORDERS, THEY ARE SUBJECT TO ALL THE DIFFERENT LAWS RELATED TO LEGAL INTERCEPT, WHICH CAN LEAD TO CONFUSION."

If platforms decide to use the strictest privacy laws, then countries that give strong legal intercept powers to law enforcement will complain. If platforms decide to use more lenient privacy laws,
then countries with stricter laws will complain. It becomes even more complicated when considering what data are covered: the data of citizens within a country’s borders vs. citizens outside its borders vs. noncitizens within its borders. Do they use some form of *jus in bello*’s noncombatant immunity definition?5

The effect on platforms is a complex regulatory regime that requires constant adjustment. The majority of platforms will start by enforcing legal standards and laws based on their home country and primary target markets, treating all cases from other countries on a case-by-case basis. If governments react negatively as these platforms gain popularity in their countries, platforms will be forced to adjust to these government demands or leave the market. This is the genesis of the Great Firewall of China6 (or any other country). It creates a barrier to trade under the guise of regulatory compliance. The complexity will only get worse. Similar to global tax as a service,7 will there be a time when censorship and legal intercept as a service become popular? It is possible that natural language processing (NLP) tools will be developed to study content by users, and a database of different censorship schemes by different territories will be created. Or a service could be contracted that processes take-down requests on behalf of the platform.

One of the negative consequences of legislation is the purposeful weakening of encryption by regulating it and limiting its use (i.e., anti-encryption laws). There are cases where law enforcement is unable to obtain information due to the use of strong encryption.8 The purposeful weakening of encryption comes in various forms, such as the mandatory use of a class of encryption that can be easily broken by legal intercept systems or the introduction of a backdoor or master key for access to information.9 This has the undesired effect of weakening the system overall, which, in many cases, defeats the purpose of encryption in the first place. If more countries pass anti-encryption laws or platforms use weak encryption to comply with them, there will likely be a substantial increase in cybercrime.

The primary issue is that each country has different standards when it comes to privacy rights and free speech. Therefore, they have different laws and regulations with respect to legal intercept and censorship. But with the Internet and the pervasiveness of global platforms holding personal information, there is a real concern about how that information will be treated. As the world becomes more interconnected, enforcement based on physical boundaries will get harder and harder.

This is a quickly evolving situation; however, there are some actions that platform owners and providers can take to prepare:

- **Ensure proper audit trails are created and retained**—This is essential, as the majority of legal intercept regulations require service and platform providers to keep metadata of activities on their systems to take advantage of safe harbors. It is critical to ensure that platforms properly log and archive this information for the retention period defined by the relevant regulator or applicable law. For example, anti-child pornography laws in some countries require that metadata be kept for at least six months, but tax authorities normally ask that transaction information be retained for three years.

- **Ready necessary systems**—If a platform has been advised that major requirements will be imposed on its systems, such as the ability to record transactions and retain them for court purposes, the system must have these capabilities ready. Other capabilities include the tapping into an existing transaction, live monitoring, removing or filtering content,
preventing activities, and rolling back transactions. This is particularly important for service providers, but it is increasingly expected of other platform providers.

- **Enable frontline workers**—Legitimate takedown and investigation requests from the government will become more frequent as digital platforms become the norm. Therefore, it is important that enterprises be prepared with policies and procedures for handling such requests. Frontline workers should be armed with the proper responses to each request (e.g., Does it require a subpoena? Should it be handed over to another group?). This can be quite tricky with respect to takedown requests. Frontline workers must be aware of the rules that allow takedowns aligned with the markets in which the enterprise operates. If an enterprise is large enough, it can dedicate a team for this purpose. In some cases, this function can be outsourced.

- **Be responsive, drill and practice**—It is not sufficient just to have the proper processes or procedures; they must be practiced as well. There have been many breaches, such as the 2016 data leak of the election authority in the Philippines (COMELEAK). In that case, a contact in the organization was notified of the vulnerability but was unable to act on it in a timely manner. With more time, it might have been possible to mitigate the problem or even prevent the major data loss.

- **Know the regulatory and legal requirements**—It is essential to consult lawyers about the regulations and laws applicable to the specific enterprise in the countries where it operates. Adhering to key requirements, such as what capabilities to provide, what information to retain and how long to retain it, is essential for keeping complaints to a minimum.

Although most of these capabilities are already available in many platforms, some policies (e.g., retention periods), procedures (e.g., takedowns) and systems (e.g., monitoring) may need to be adjusted or enabled.

A longer-term approach is to advocate for globally acceptable standards for the protection of speech and privacy rights. Having a common standard that all countries follow would allow people to have a reasonable expectation of privacy. It would also provide uniformity and consistency in enforcement. Regarding privacy rights, there are multiple frameworks, such as the Organisation for Economic Co-operation and Development (OECD) Privacy Principles and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Freedom of speech is a little trickier because it deals with content. What is the solution? This is an open question.

"A LONGER-TERM APPROACH IS TO ADVOCATE FOR GLOBALLY ACCEPTABLE STANDARDS FOR THE PROTECTION OF SPEECH AND PRIVACY RIGHTS."

**Conclusion**

Advocating for a Clean Network by the United States can be seen as an attempt to separate those entities that do not conform with its standards for free speech and privacy. Similar to the situation during the age of mercantilism, a subject can benefit from the bounty of the homeland by buying into the system. This effectively divides the Internet into many different silos governed by different laws and regulations—the US Clean Network being one of them. Currently, approximately 30 countries and territories have signed up to be “clean” countries. If the world cannot agree on global standards, is it better to break it apart so that each country is on its own? The best thing practitioners can do is ensure that they design processes, systems and platforms with these considerations in mind. It is ideal to take advantage of the many safe harbor provisions while also staying within the lines of compliance. It would truly be difficult to ensure compliance with different regimes in a highly interconnected world.
Endnotes


