INTERACTIVE SESSION ORGANIZATIONS

Digital Nationalism

The Internet began as a network of networks designed to foster the free and open exchange of information anywhere in the world. It has been a major driver of globalization, embodying a public sphere beyond the control of sovereign governments. Today, this is no longer the case. All over the world, nation-states have been asserting their authority over Internet use and claiming various forms of digital sovereignty. The Internet now has become subject to firewalls, shutdowns, and data-localization laws that have fundamentally changed its character as a unified global infrastructure.

Authoritarian governments have long sought to rein in the Internet, China being one of the first. Its Great Firewall, which restricts what people can read and do online (see the chapter-ending case), has served as a model for promoting Chinese "digital sovereignty." China's efforts have demonstrated to other authoritarian regimes that the Internet can be effectively controlled.

Several countries are trying to follow the Chinese example. To control contact with the outside world and suppress dissident content, Iran has set up a so-called "halal net," and North Korea set up its Kwangmyong network. In 2019, Vladimir Putin signed a "sovereign Internet bill" to set up a self-sufficient Runet. The bill also includes a "kill switch" to shut off the global network to Russian users. According to the *New York Times*, at least a quarter of the world's countries have temporarily shut down the Internet over the past four years.

In recent years, digital nationalism has also taken the form of data localization (or data protectionism) laws in countries such as Vietnam, India, Argentina, Venezuela, and Nigeria. Some countries require that data on their citizens (or certain types of data, such as medical or financial data) be physically stored on servers within their borders. Others allow the data to leave their borders but insist on a copy remaining domestically.

These laws have legitimate uses, including privacy protection and national security. Unfortunately, hate speech expressions and disinformation on the Internet have been co-opted to justify laws enabling repressive governments to monitor online activity and speech. At least 45 countries now have some version of data localization requirements in place—and they are not limited to authoritarian states. Australia, Canada, New Zealand, South Korea, and Switzerland are among the countries that now restrict cross-border flows of data.

Russia now requires a copy of data on Russian citizens to be stored in the country. The country has banned LinkedIn for defying the rules and fined Facebook and Twitter $63,000 each for failing to comply with a national data law.

The European Union's General Data Protection Regulation (GDPR—see Chapter 4) is not specifically about localization, but it imposes stringent restrictions that make it difficult for companies to move data across borders. There is growing sentiment among EU nations to further strengthen data protections and that EU privacy regulation should call for European data to be physically stored in Europe. Data produced in Europe should be processed in Europe.

Many of these laws are ostensibly targeted at Western multinationals, but larger companies are generally better able to meet these requirements than smaller ones, which lack the necessary resources. Developing countries, often at the forefront of digital nationalism, might also suffer. For example, India and the Philippines have large numbers of outsourcing firms that rely on a unified global information network. These countries' efforts to set up roadblocks on that network could come back to haunt them.

The great risk is that digital nationalism will Balkanize the Internet, breaking it up into a patchwork of incompatible and irreconcilable fiefdoms. This scenario, sometimes referred to as Splinternet, is already affecting Internet-based content and services. China's population does not have access to Wikipedia, Facebook, and most of Google. When the EU's GDPR first came into effect, many American media companies were ready to stop offering their content to European consumers, at least temporarily.

Balkanization could also reshape the Internet's underlying technical infrastructure. Over the last decade, several countries, citing cultural sensitivities, have considered banning or otherwise restricting the .xxx top-level domain name (generally used

for pornography), raising the prospect that the Internet's naming system could eventually fracture. After Edward Snowden's revelations about U.S. spying, Brazil moved to build a separate undersea cable link to the EU to bypass existing Internet infrastructure. At the Engineering Task Force, a key Internet standards committee, representatives who wanted to maintain a backdoor for government agencies clashed with those pushing for more robust encryption.

What can be done to curb digital nationalism? Experts recommend finding ways to restore a sense of inclusiveness and fair play among Internet users and to remind them of the original principles of universality and inclusiveness that made the network so effective in the first place. Another recommendation is to develop "zone"-based approaches for running the Internet, where interconnecting blocs of member-nations would commit to uphold liberal principles such as free trade, privacy, and freedom of expression. This approach would not produce a single global network, but a "coalition of the willing" might be the best way to counter growing Internet fragmentation and keep the network relatively open and free.

Sources: Vincent Manancourt, "Europe's Data Grab," *Politico*, February 19, 2020; Akash Kapur, "The Rising Threat of Digital Nationalism," *Wall Street Journal*, November 1, 2019; Fang Kecheng, "Is Cyber-Nationalism on the Rise in China?" *Echo Wall*, September 25, 2019;

CASE STUDY QUESTIONS

1. What is digital nationalism? Give two examples.
2. What problems does digital nationalism pose for conducting business globally?

Software Localization

The development of core systems poses unique challenges for application software: How will the old systems interface with the new? Entirely new interfaces must be built and tested if old systems are kept in local areas (which is common). These interfaces can be costly and messy to build. If new software must be created, another challenge is to build software that can be realistically used by multiple business units from different countries given that business units are accustomed to their unique business processes and definitions of data.

Aside from integrating the new with the old systems, there are problems of human interface design and functionality of systems. For instance, to be truly useful for enhancing productivity of a global workforce, software interfaces must be easily understood and mastered quickly. When international systems involve knowledge workers only, English may be the assumed international standard. But as international systems penetrate deeper into management and clerical groups, a common language may not be assumed and human interfaces must be built to accommodate different languages and even conventions. The entire process of converting software to operate in a second language is called **software localization**.

Most of the world's population accesses the Internet using a mobile device, so apps must be built for mobile platforms, tiny screens, and low bandwidth. Since many mobile Internet users cannot read or write, special interfaces using video and audio need to be built to serve this group.

What are the most important software applications? Many international systems focus on basic transaction and management reporting systems. Increasingly, firms are turning to supply chain management and enterprise resource planning systems to standardize their business processes on a global basis and to create coordinated supply chains and workforces. However, these cross-functional systems are not always compatible with differences in languages, cultural heritages, and business processes in other countries. Company units in