TIEDEMANN ADVISORS

TIEDEMANN INSIGHTS

Digital divides could disconnect the world

The world is evolving into three separate data governance zones – complicating flows and use of information for many companies and individuals

By Robert Hormats | Managing Director, Tiedemann Advisors

A version of this article originally pubished in *The Hill* on April 15, 2021

A world of seamless information flows, which many had forecast a decade or so ago — a world of full scale "information internationalism" — looks less and less likely today. We are moving ever closer to three "data-governance zones" (DGZs) characterized by three often sharply different sets of rules for regulating personal and business information and the enormous amounts of data flowing among nations: a world often referred to as one of "information nationalism." Differences among these zones and countries include: the role of government in obtaining access to data; limits of various types on the ability of companies to collect, store and utilize data; differing levels and rules of transparency required for obtaining and utilizing data; divergent rules and restrictions on localization of data storage; and sharp variations in the level and methods of user consent.

In many ways these rules and approaches reflect differences among histories and governmental systems, as well as public attitudes about individual rights in specific countries or zones. These sets of differences raise new challenges to cross-border interoperability of information-related technologies and the nature and degree of information flows and management among individuals, businesses and services.

These zones may be porous enough to continue to permit substantial international data flows across borders and to avoid imposing such tight restrictions that large numbers of individuals and companies are prevented from actively communicating internationally —but there will likely be a range of constraints in some key areas that will make some types of communications and certain categories of business requiring the flow, storage and use of data more difficult.

Compromises and resolutions of some differences are, of course, certainly possible in order to permit efficient cross border use of some new technologies and greater cross-border data flows in certain areas. But greater limits are also more likely in other areas. In some, divergences, could be quite stark, posing complicated challenges to flexibility and openness. And because some of these, as noted above, represent differences among histories, social values and government systems, many differences will be difficult to reconcile. Moreover, there is no international institution to establish common rules or norms, or to at least narrow them in key areas.

The zone that has focused most on data privacy and rules has been the European Union (EU). Its system is largely based on General Data Protection Regulation (GDPR). While Europe's system of regulations is continent-wide, including the United Kingdom after Brexit, the United States, largely because of its federal structure, is characterized more by rules promulgated by individual states. And China's system is nationwide, but in one major area takes a very different view from both Europe and the U.S. — its government's nearly complete access to all information and data. There are other countries with very different sets of policies and regulations, but these three are likely to be the ones that will set trends.

Europe: Protection of personal data in Europe is tied to the view that privacy is a fundamental right. This view has taken hold since World War II. Data privacy has become a major issue in many quarters. And European-wide nongovernmental organizations and collective governmental institutions have strongly advocated for privacy rights.

As Oxford Analytica has noted, the European Parliament has blocked the export of banking and travel data to the U.S. This was done in spite of U.S. pleas that this was needed for effective anti-terrorism measures. And the European Court of Justice established what is known as the "right to be forgotten" and then invalidated the U.S.-EU Privacy Shield arrangement. The GDPR includes such features as minimized data collection, increased transparency, greater localization and broad use of "user consent." It is enforced by the European Data Protection Commissioner and data protection institutions in member countries. Its provisions will need to be updated periodically as new technologies and business models emerge. EU member governments with stronger and more data-intrusive or authoritarian central governments may differ from the focus on privacy triggering intense internal disputes.

United States: America's leaders have not adopted the European view that there is a generalized "right to privacy" in this area — even though several cases in other areas have emphasized the need and priority for protection of privacy. Congress passed the Privacy Act in 1974, but it applies only to federal databases.

As Oxford Analytica notes, rather than sweeping rules and norms, much of the U.S. privacy and data protection at the national level is regulated by individual pieces of legislation related to such areas as consumer protection, health and financial information. Another difference is that in contrast to Europe, where rules are largely related to private companies, American rules and laws have been more focused on this country's history of limiting government power, which can mean limiting the amount and kind of information the government collects on citizens. But government-business frictions over private sector use of data have been growing and it is possible this will continue.

Much of the new movement in this area so far, as Oxford Analytica notes, is at the state level. The California Consumer Protection Act confers the right to know about how data is used, options to delete personal data, the choice to opt out of the sale of personal data, and non-discrimination vis-à-vis users. Then Virginia came in with its own set of rules — as have other states.

China: Until recently, China did not have broad data protection rules similar to those in Europe or the U.S. And the government has avoided anything that might interfere with its ability to obtain citizens' information of all sorts. But lately, as the digital economy expands, China has produced new legislation focused on the private sector.

Beijing has enacted laws on consumer protection, and is working on legislation on personal information protection in some sectors and some kinds of technology companies. Some language used in its legislation in this area even appears to be modeled from the GDPR.

The big difference, of course, is there are no protections of individual information and data from the state. China's Data Security Law, as described by Oxford Analytica, protects what is called "important data" —the destruction, distortion, alteration or disclosure of which, in the government's view, would affect China's national economic, social and cultural security. Beijing has developed a five-tiered system, with increasingly strict cybersecurity and data protection requirements for higher tiers. And there are strict provisions on inflows or outflows of certain types of information and certain date-driven companies and business models.

These three models reflect the different priorities for the zones/countries discussed. This tri-zone system, and the prospect of further regulatory policy divergence, presents formidable challenges for global communication and data management/flows of all sorts, with much of the impact likely to be on businesses and services dependent on cross-border data transfers or data-driven business models that differ from provisions laid out in regional or country laws and regulations.

More broadly, each of these zones/countries sees its system as a model for others. For example, China's system may be a model for other nations with strong or authoritarian central governments that want to maintain tight state control over information. Europe's approach to data protection is seen as a model for some other countries; several influential groups in the U.S. and elsewhere have argued for emulating regulatory features contained in it. So the three zones, in time, may have geographical scope and influence well beyond their borders.

Whether rules, norms and practices can be forged to avoid greater digital nationalism or divergence remains to be seen. But the global system clearly will be a lot less seamless and probably a lot more complicated to navigate than most of us had imagined a decade or two ago. In some cases, this will be a source of new types of 21st century international friction that will require new sets of policies and new types of "technology diplomacy" from Washington.