Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law. By Radim Polčák and Dan Jerker B. Svantesson. Northampton, MA: Edward Elgar, 2017. Pp. xvii, 268. ISBN: 978-1-78643-921-5. US$ 135.00.

Suppose criminals breach an international bank's database of customer accounts. The bank's datacenter is in the United Kingdom, the hackers are based in China (but worked through computers in Thailand), and the data is used to defraud customers in the United States, France, Japan, and Brazil. Which state(s) has jurisdiction to investigate and prosecute the criminals? In *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*, Radim Polčák and Dan Jerker B. Svantesson argue that international law's reliance on territoriality as the primary basis for jurisdiction is ill-suited to the information age.

The authors contend that territorial control makes little sense when applied to information that is routinely transmitted and processed in multiple sovereign states. As a pragmatic matter, territoriality prevents states from acting appropriately regarding cyber security, data privacy, and law enforcement investigations. Instead, the authors propose that jurisdictional doctrine should recognize that information is not a static object that sits exclusively in one state at a time, but rather a process that can be performed in multiple states. More than one state at a time should be able to have jurisdiction over an information process.

The authors propose that a state has jurisdiction when there is a substantial connection between the matter and the state, the state has a legitimate interest in the matter, and the exercise of jurisdiction is reasonable given the balance between the state's legitimate interests and other interests. Applying this framework to the example above, any of the states involved may have a valid claim to some kind of jurisdiction over the breach.

The authors distinguish between legislative, judicial, and enforcement jurisdictions, and add a new type, investigative jurisdiction. Using the authors' framework, perhaps the United States and China would have investigative jurisdiction and thus be empowered to collect evidence on the hacking, even if the datacenter through which the stolen data was routed is in the United Kingdom. Given that information processes, the technical infrastructure that carries the data, and the private corporations that own the cables and computers often cross national borders, the authors' framework offers a theoretical basis for exercising jurisdiction over those processes. The authors focus on jurisdiction over cyber security, evidence gathering by law enforcement, and data privacy, but the framework could be applied to other information matters such as intellectual property and international financial transactions. The framework could also be used for rethinking the foundation of cross-border jurisdiction in our interconnected world.

Information Sovereignty is a theoretical and specialized work most suitable for collections supporting researchers focusing on jurisdiction in international law and on global information policy. The authors have articulated portions of their argument in articles published in scholarly law journals. These articles may satisfy the needs of some researchers, while others may prefer the consolidated account in this book.

Benjamin J. Keele
Research and Instructional Services Librarian
Ruth Lilly Law Library
Indiana University Robert H. McKinney School of Law
Indianapolis, IN U.S.A.
doi:10.1017/jli.2018.28