Data is often conceptualized through metaphor. Some compare data to oil, insofar as data is an asset that must be refined to have value. But the oil metaphor has its limits—after all, data does not have a fixed value irrespective of who possesses it. More recently, data has been compared to sunlight because it is “everywhere and underlie[s] everything.” The sunlight metaphor is particularly attractive to those who ascribe to the open-data movement. But like the oil metaphor, it also runs into problems because data, unlike sunlight, is increasingly subject to borders and political power. Others view data as infrastructure, akin to roads and railways. Understanding data in this way, however, presumes a level of government involvement in its management that is largely missing.

None of these metaphors perfectly encapsulates all data’s qualities, but each is helpful in understanding certain aspects of data in today’s digital world. First, like oil, data has value. It is valuable to companies that primarily generate revenue through targeted ads. Further, data about a living individual is valuable to that person—an interest recognized in emerging privacy-protecting regimes, like the GDPR. Second, like sunlight, data is everywhere. Digital technology “challenges basic assumptions about what is ‘here’ and ‘there.’” Data can cross borders in a moment, and it is often located in a physically distinct location from the individual using or manipulating it. What’s more, data can reside in numerous places simultaneously. Third, data often is infrastructure, suggesting a natural role for government regulation. This is how the United Kingdom’s National Infrastructure Commission characterizes data—as a critical resource that can improve how “infrastructure is built, managed, and eventually decommissioned.”

Understood together, these metaphors suggest that data is simultaneously a valuable, intangible, elusive, and ubiquitous resource. For the purposes of this Paper, data’s intangible and elusive qualities—it’s non-territoriality—play a central role because data’s ability to subvert borders presents numerous challenges in a world premised on Westphalian sovereignty. Recent cases dealing with data sovereignty cut to the core of these challenges, and conundrums abound: If a national court issues a delisting order to a digital company like Google, does that company have to globally delist the data in question? What should a state do when digital evidence—necessary to investigate a serious crime that occurred on its territory—is held abroad? Can states require data be stored within its national borders as an end run around this problem? How can states tax sales and advertising revenues in the digital economy? What role should digital companies play in solving data-sovereignty challenges? These questions do not have easy or clear answers, and consequently, data-regulation scholars are increasingly concerned with sovereignty.

This Paper endeavors to describe key flashpoints that typify the clash between sovereignty and data’s non-territoriality, including: (1) the reach of local and national law and courts in a digital world, (2) cross-border access to data in investigations of serious crime, (3) data protectionism efforts, (4) digital trade and taxation, and (5) the evolving role of technology companies and multistakeholder internet governance efforts. Together these flashpoints paint a picture of a world that is struggling and at times succeeding to address the myriad collective-action problems
posed by data in a Westphalian system. In each instance, there is interplay among states, multilateral organizations, and private companies, highlighting how data’s non-territoriality is altering the world as we now it. What’s more, these examples indicate that sovereignty still has a strong grip on the international order. This is most evident in efforts by states like China and Russia to localize citizen data within its borders, but even liberal democratic states are reluctant to forfeit sovereignty in the digital world. Slowly but surely, data flows are being manipulated and altered to conform to sovereign demands, and often these demands are in conflict.

Local Law with Global Reach

States enacting privacy-protecting regimes like the EU’s General Data Protection Regulation (GDPR) are testing the territorial reach of such laws—in some cases going so far as seeking global injunctions against companies like Google and Facebook. At issue in these cases is the delicate balance of data privacy and freedom of expression. Because states have varied data-privacy and free-speech protections, global injunctions requiring Google, for example, to delist personal data could place the U.S.-based entity in conflict with the First Amendment and other U.S. laws. In sum, global injunctions to delist or remove personal data can create conflicts of law and infringe on state sovereignty.

Concerns regarding the efficacy of global injunctions animate a number of recent cases in domestic and regional courts. In 2015, France’s data-protection regulator (CNIL) ordered Google to globally remove links or pages that violated a user’s right to be forgotten; Google blocked the relevant content in Europe but refused to do so globally. The Court of Justice of the European Union (CJEU) ultimately ruled that Google did not have to globally delist the data, emphasizing that, “numerous third States do not recognise the right to de-referencing or have a different approach to that right.” However, the CJEU did not reject the possibility of global injunctions in the future, and in 2019, the CJEU ruled that Facebook could be forced to globally remove defamatory or illegal content. Similar disputes will continue to arise as states enact laws protecting the right to be forgotten and seek to regulate online data. For example, when the Canadian Supreme Court issued an order that required Google to delist search results globally in the patent-infringement trial Google Inc. v. Equustek Solutions Inc., Google challenged this ruling in U.S. court.

Case law dealing with global delisting orders often hinges on the relevant company’s willingness to comply rather than a third-party government’s assertions that its sovereignty might be infringed. For example, Google challenged the Canadian Supreme Court’s global delisting order in Equustek Solutions Inc. by invoking the First Amendment of the U.S. Constitution, U.S. law, and U.S. sovereignty. However, it is unclear what sovereign interest the United States has in allowing Google to link to pages selling illegal goods, which was at issue in the case, and Canada’s Supreme Court found Google’s argument “theoretical.” Google then filed a case in U.S. federal court to create a conflict of law. Thus, while global injunctions necessarily raise questions of sovereignty, they do not always create material conflicts of law that an issuing court will recognize.

Cross-border Access to Data in Criminal Investigations
Jennifer Daskal has succinctly described the problems data and borders pose to law enforcement: “Increasingly, users in State A contract with or use email or social media services that are based in State B. Meanwhile, technology companies often store users’ data across international borders.” However, international law has long prohibited State A from unilaterally searching and seizing property—including data—located in State B without State B’s consent. Consequently, when conducting a criminal investigation that requires extraterritorially located data, State A must first ascertain which state has jurisdiction over the data in question. This inquiry might turn on a number of factors, including where the data is located; where the company that manages the data is headquartered, has physical presence, or provides services; or the location or nationality of the target of the search. Second, if the data is located in State B (or any State that is not State A), State A must obtain permission to access the data pursuant to established rules. State A could also demand access, though this is a sub-optimal outcome.

Implementing a system that allows State A to access data stored in State B is far more complicated than the foregoing summary suggests. One need look no further than the Microsoft Ireland case to understand how states are struggling to adapt to a world where digital evidence is both increasingly critical to law-enforcement investigations and increasingly likely to be located outside the jurisdiction where a crime has occurred. The rules governing cross-border access to data are far from cemented, and we are at an inflection point: the danger is that “governments demand[] access to all information anywhere and everywhere,” but there is also a unique opportunity to collectively set “baseline standards and clear jurisdictional rules.”

The United States, the European Union, and Australia have all taken different approaches to law-enforcement access to extraterritorially located data. The U.S. Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act in 2018 to codify that U.S. warrants issued pursuant to the Stored Communications Act reach all data within possession, custody, or control of a U.S.-based provider. The CLOUD Act leaves in place blocking provisions that require states to make a mutual legal assistance (MLA) request to the United States for U.S.-held communications content “even if they are seeking their own citizens’ data in the pursuit of a domestic criminal investigation.” The MLA request process is notoriously inefficient, and the CLOUD Act allows states to bypass it by signing a bilateral executive agreement with the United States. The first of these agreements—between the United States and United Kingdom—was sent to Congress for approval in October 2019, and agreements between with the EU and Australia are underway. However, if foreign governments want to access data of U.S. persons (U.S. citizens, permanent residents, and people located inside the United States), they still have to make an MLA request.

The European Union’s draft e-Evidence proposal is distinct from the CLOUD Act in that it allows one EU member state to compel production of data held by a service provider established or represented by another member state. This gives EU member states extraterritorial warrant authority, albeit within the EU. Further, the EU proposal restricts the grounds on which a provider can object to a disclosure order. In these ways, the EU proposal is distinct from the CLOUD Act. Australia took a different approach when it enacted a law in December 2018 that allows law enforcement to issue search warrants that bypass companies and directly access data. When the government knows data or a device is extraterritorially located, a foreign government must consent before a search warrant will be issued. However, consent is not required when the location of the data or device is unknown.
None of the current approaches to e-evidence are perfect, but they demonstrate a clear government interest in accessing data quickly and efficiently in the course of the investigation of serious crime. In the absence of solutions that balance privacy interests with the government interest in accessing such information, the international community risks the rise of data localization laws that seek to sidestep international engagement entirely.

**Data Protectionism and the Chinese Approach**

Numerous states have adopted or are considering data-protectionist policies, in part, as a response to the law-enforcement challenges discussed in Part II. Such efforts are an attempt to apply borders to data. States like China and Russia have enacted laws to ensure that their citizen’s data is stored inside their territory, thereby facilitating surveillance, minimizing foreign influence, and maximizing sovereignty. Data-localization efforts are spreading, but there is some indication that states are hesitant to adopt regimes as strict as China’s. For example, in early 2020 the Indian government introduced a revised Personal Data Protection Bill that included relaxed data-localization requirements than had previously been contemplated.

China’s approach to data is one of forced localization, and it provides a model for states that want to exercise maximal sovereignty over their citizens’ data. For example, Article 37 of China’s Cybersecurity Law requires that “important data” concerning Chinese citizens be stored and processed locally.” However, China’s control over its citizen’s data is not complete. As of now, multinationals in China can still send some data abroad, but it is unclear how long such allowances will last. Furthermore, Chinese government at this moment does “not necessarily have unfettered real-time access to all [Chinese] companies’ data.” China’s stringent regulation of cross-border data transfers is rapidly evolving.

Russia followed China’s lead when the State Duma enacted a data-localization law in 2014. While this law has not always been strictly enforced, the Russian government appears to be taking enforcement more seriously as of late. For example, when LinkedIn refused to transfer Russian user data to servers in Russia, Roskomnadzor, the Russian state agency that oversees media and telecommunications, announced that the company would be blocked in Russia. Apple, on the other hand, has complied with Russia’s data-localization demands. Thanks to a new counterterrorism law, which came into force in 2018, companies operating in Russia are required to retain data for six months, and Russian security services can now access data without a court order. The Kremlin appears to be tightening its grip on the internet and moving toward strict enforcement of its data laws.

The U.S. Congress is also considering a data-localization bill that was introduced by Senator Josh Hawley (R-Mo.) in November 2018. This proposal, which was originally introduced by Senator Tom Cotton (R-Ark.), would “combat the flow of Americans’ sensitive personal data to China and countries that similarly threaten America’s national security.” But this bill could set a dangerous example. While states might be hesitant to follow China’s lead, a U.S. data-localization law could spark similar efforts around the world. For example, Indian officials have cited Senator Hawley’s proposal to support their own data-localization efforts.
As more countries consider and adopt data localization laws, the internet will become increasingly fragmented and filtered. What’s more, erecting borders around data will make AI innovation more difficult and thereby affect economic growth because “large, diverse, international datasets are core to building AI applications that work across a variety of geographies, languages, cultures and demographics.” Thus, if the United States and its partners are committed to the free flow of data and innovation, they must work to create baseline regulations governing cross-border data flows to counteract the rise of data-localization efforts.

**Digital Trade and Taxation**

The digital economy presents novel challenges to international taxation schemes, which have traditionally been based on an entity’s physical location (their “permanent establishment”). However, digital companies can now have customers in a country without having physical presence and derive significant profit from user data. The French government, for example, argues that the “structure of the global economy has shifted to one based on data, rendering 20th century tax systems archaic.” Further, new technology can facilitate novel ways to avoid taxation and can thus exacerbate base erosion and profit shifting (BEPS) issues. Consequently, taxation of digital goods or services is a live public-policy issue that national governments and regional organizations are working to address.

Both the Organization for Economic Cooperation and Development (OECD) and United Nations are working to craft solutions to the challenge of digital taxation. The EU is also creating new taxation rules for the digital age. These efforts are meant to create a standardized approach to digital taxation and to ensure digital companies “pay tax wherever they have significant consumer-facing activities and generate their profits.” They are also meant to head-off unilateral efforts by national governments to create new digital taxation schemes. If multilateral organizations are unable to successfully implement new digital taxation schemes, states will fill the void with national-level policy leading to a fragmented system.

**The Evolving Role of Digital Companies**

In discussing the numerous ways in which data complicates traditional ideas of sovereign power and authority, it becomes clear that states are not the only major players. Each example explored above implicates interactions among states and digital companies like Google, Microsoft, Facebook, and Amazon. These digital companies lack sovereignty, territory, and statehood, but they wield an enormous amount of power in modern society. Bearing this in mind, should digital companies be understood as equal to states or as subordinate to them? This question then raises a natural corollary: what role should digital companies play in the international system?

Experts answer this question and its corollary in numerous ways. Lucas Kello, for example, argues in his book *The Virtual Weapon and International Order* that the rise of non-state actors, including digital companies, does not threaten the state’s primacy in international affairs but dilutes the state’s role; in other words, the rise of non-state actors in the digital age creates a “sovereignty gap.” Kristen Eichensehr argues in a recent article that tech companies should be understood as “digital Switzerland”—a term she borrows from Microsoft President Brad Smith—insofar as they are equal to states and neutral actors in the international system. Other
scholars have suggested thinking of technology companies as information fiduciaries, surveillance intermediaries, and public utilities. All these proposals recognize digital companies’ ascendant power and influence and thereby suggest the attendant need to shift from multilateral to multistakeholder models of internet governance. Multistakeholder models incorporate multiple types of actors (e.g., states and digital companies), and the precise contours of multistakeholder internet governance—like the role of digital companies—is still developing. In the digital world, multistakeholderism is both necessary and inevitable.

***

In conclusion, data presents numerous challenges to a world premised on sovereignty and territoriality, and the international community is only beginning to grapple with the challenges presented in this Paper. One lingering question is whether in this process, the world will become more interconnected or borders will become further entrenched. It seems that the answer could very well be both.

Recommended Readings:

- The Data Economy, Special Report, ECONOMIST (Feb. 2020).
  - Pay special attention to the articles titled Are data more like oil or sunlight? and Governments are erecting borders for data.
  - For a longer treatment of the issues presented in Privacy and Security Across Borders, see Jennifer Daskal, The Un-Territoriality of Data, 125 YALE L.J. 326 (2015). Pay specific attention to Part II.
- Samm Sacks, Data Security and U.S.-China Tech Entanglement, LAWFARE (Apr. 2, 2020, 8:00 AM).