“Securing the Internet Commons”

Anne-Marie Slaughter

Ever since Edward Snowden’s revelations about the National Security Agency’s spying on citizens and leaders around the world, a debate has raged in the United States about the proper balance between national security and individual privacy and liberty. Most recently that debate has focused on encryption: whether technology companies should be able to develop programs that encrypt their users’ messages so securely that no one but their intended recipients – not even governments – can read them. It is a debate to which governments and citizens everywhere should pay attention.

Not surprisingly, the US government’s national security officials oppose full encryption by American technology companies, arguing that the country will be less safe if the proper authorities have no “backdoor” – a piece of code that lets them in. Software engineers call backdoors “vulnerabilities,” deliberate efforts to weaken security. They regard a request for backdoors the same way an automobile manufacturer would view a request for a defective engine.

A large coalition of technology companies and civil-society organizations recently sent a letter to President Barack Obama arguing against backdoors. In addition to “undermining every American’s cyber security and the nation’s economic security,” the signers argued, “introducing new vulnerabilities to weaken encrypted products in the US would also undermine human rights and information security around the globe.”

What supporters of encryption recognize is that “if American companies maintain the ability to unlock their customers’ data and devices on request, governments other than the United States will demand the same access, and will also be emboldened to demand the same capability from their native companies.” The US government will not be able to object, given its own policies. The result “will be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes.”

What is at stake is nothing less than the health of the “global digital ecosystem.” The technology corporations that signed this letter understand that while they may be incorporated in the US, they are global players and have global responsibilities. They also understand, in a more self-interested vein, that if foreign consumers believe that using American social media and search engines exposes them to the scrutiny of US intelligence agencies, those consumers will turn to other providers.

The response of many foreign governments has been to focus on how to ensure and protect their “technological sovereignty.” Information may transcend borders, but servers and cables still have physical locations.
The Open Technology Institute at New America (which I head) is collaborating with the German Global Public Policy Institute (GPPI) on a series of transatlantic dialogues about “security and freedom in the Digital Age.” An initial report identifies 18 proposals from more than a dozen European governments on subjects including new undersea cables, encryption, localized data storage, domestic industry support, international codes of conduct, and data protection laws.

Many of these proposals will not actually achieve their goals. But the most important issues to sort out are less about feasibility than about desirability, from both a national and a global perspective. As with US companies, it is important to differentiate among corporate, economic, and public interests at the national and global levels. Citizens from around the world have a stake in getting this right.

For starters, digital protectionism should be as suspect as any other form of protectionism, albeit with exceptions for health, safety, and social solidarity. “Technological sovereignty” can easily be a pretext for insisting that citizens buy only homegrown tech products.

Moreover, rules should be formulated globally and implemented nationally. The Internet is essentially a country with both state and non-state actors as its citizens. It is our task to ensure that it is a free, open, and universally accessible country that advances and safeguards universal human rights.

The OECD adopted an excellent set of “Principles for Internet Policy Making” in 2011. Principle 1 requires that policymakers “promote and protect the global free flow of information”; Principle 2 insists on promotion of “the open, distributed, and interconnected nature of the Internet”; Principle 8 mandates “transparency, fair process, and accountability” across the Internet; Principle 11 promotes “creativity and innovation”; and Principle 13 “encourage[s] cooperation to promote Internet security.”

Other countries and regional organizations have come up with similar guidance. The point is less the specific wording or even content than the recognition that such principles are necessary for policymakers around the world.

From this perspective, it is not clear whether “technological sovereignty” is a helpful or harmful concept. It makes digital space sound like airspace or territorial seas, something that is somehow derived from or adjacent to physical territory. The New America-GPPI report is entitled “Technological Sovereignty: Missing the Point?” The authors conclude that “data privacy and security depend primarily not on where data is physically stored or sent, but on how it is stored and transmitted.” For data purposes, at least, we are in a post-territorial age.

Decoupling sovereignty from territory is hard to do, particularly after Snowden showed the world just how far one country’s technological tentacles can reach. Still, the larger lesson is that differentiating between national security and global security in the digital world may be both impossible and deeply counter-productive. We need new maps and mindsets and new coalitions of business, civic activists, and all those who understand that national security must include the protection of privacy and freedom of expression. And we need new ways to engage both governments and citizens in a new, exhilarating, dangerous, and still largely unexplored world.