The Washington Post

Back to previous page

After Snowden, a lesser Internet?

By David Ignatius, Published: February 5, 2014

MUNICH

Edward Snowden's supporters have portrayed him as the champion of Internet freedom. But when senior European and U.S. experts privately discuss the future of cyberspace, their fear is that the Internet may be closing, post-Snowden, rather than opening. "We may be the last generation to take joy from the Internet," because of new boundaries and protectionism, as one American glumly put it.

Privacy advocates would argue that any dangers ahead are the fault of the pervasive surveillance systems of the National Security Agency, rather than Snowden's revelation of them. I'll leave that chicken-and-egg puzzle for historians. But it begs the question of how to prevent the anti-NSA backlash from shattering the relatively free and open Internet that has transformed the world — and which the NSA (and other security services) exploited. Unfortunately, the cure here could be worse than the disease, in terms of reduced access, cybersecurity and even privacy.

As a starting point, Americans need to understand just how angry Europeans are about the NSA's invasion of their personal space. Secretary of State John F. Kerry cheerily told the Munich Security Conference last weekend that he foresees a "trans-Atlantic renaissance," with new trade and diplomatic agreements. For now, such talk is just whistling past the NSA graveyard.

"People in Washington don't realize how serious feelings on this side of the Atlantic are," argued one prominent European politician at a high-level private dinner here, hosted by the Atlantic Council to discuss technology issues. He predicted flatly that U.S. companies would lose an estimated $28 billion to $32 billion in revenues to European cloud-computing companies that will market "NSA-proof" data storage.

This boom for Euro-cloud companies is understandable, in terms of corporate opportunism. But it could build fences around European servers that might turn the global information superhighway into a series of bottlenecks and on-off ramps.

The Internet governance issue is fraught, too. For the past several decades, basic standards and architecture have been managed by a private body known as the Internet Corporation for Assigned Names and Numbers. But this group, though passionate about privacy, is now seen as U.S.-dominated, and therefore contaminated. An alternative would give more oversight to the United Nations' International Telecommunication Union. The leading candidate to head the ITU next is a Chinese official, Houlin Zhao, the group's deputy secretary-general.

Protecting data networks may actually be harder in the post-Snowden environment, argued both Europeans and Americans. That's because sophisticated cyber-protection involves cooperation

between agencies such as the NSA (and its foreign counterparts) and private Internet service providers. Such contacts are now anathema.

Another paradox is that indignation about U.S. snooping might make it easier for Russian and Chinese security services to spy on their own people and conduct cyber-espionage. "The Russians and Chinese will talk about sovereignty and non-interference in cyberspace, which is a proxy for their control agenda," argued one technology expert.

"The Snowden disclosures are being used to renationalize the Internet and roll back changes that have weakened government control of information," argues Stewart Baker, a former NSA lawyer who writes an influential blog on cybersecurity issues.

Many Europeans told me President Obama made a good start with his speech last month outlining new rules for the NSA, especially in his willingness to provide some version of a global Fourth Amendment. One European argued that privacy rights should be reciprocal — the United States should offer protections to countries that grant such rights to their own citizens, as well as Americans.

But one senior European politician warned that if his fellow citizens can't sue in U.S. courts to enforce their new privacy rights, then the European Union will withdraw its so-called "safe harbor" protection for U.S. technology companies. This provision allows U.S. companies to operate in European cyberspace by quickly certifying that they comply with stringent European Union privacy rules. Closure of this safe harbor could sink U.S. companies and stall e-commerce.

The NSA revelations have tapped what another top European official called "a fundamental anti-Americanism and mistrust of the U.S." He noted that if Europeans question the new post-Snowden call for limits and boundaries, they are accused of being the NSA's lackeys. "Where's the pushback from the U.S.?" he asks plaintively.

In this tempest of anti-NSA feeling, one of the bravest speeches at Munich was given by German President Joachim Gauck. "We rightly complain when allies overstep the mark when they use electronic surveillance to detect threats. And yet we prefer to remain reliant on them and hesitate to improve our own surveillance capacities," he said.

A loose interpretation of his underlying message would be: Get real, fellow Europeans. Protecting cyberspace is more complicated than bashing the NSA.

Read more from David Ignatius's archive, follow him on Twitter or subscribe to his updates on Facebook.

Read more about this issue: Peter Swire: Why tech companies and the NSA diverge on Snowden Robert J. Samuelson: The hidden consequences of Snowden's NSA revelations John McLaughlin: The NSA's surveillance programs keep us safe Eugene Robinson: The NSA is collecting too much information The Post's View: Improving transparency without harming security