Don’t gerrymander the internet

by Leslie Harris [1]
November 4, 2013 Originally appeared as Don’t gerrymander the internet [2] in Index on Censorship

Originally published on Index [2].

We can partially blame gerrymandering for the current gridlock in the U.S. Congress. By shaping the electoral map to create politically safe spaces, we have generated a fractious body that often clashes rather than collaborates, limiting our chances of resolving the country’s toughest challenges. Unfortunately, revelations about the global reach of American security surveillance programs under the National Security Agency (NSA) are leading some to propose what amounts to gerrymandering for the internet in order to route around NSA spying. This will shackle the internet, inherently change its technical infrastructure, throttle innovation, and likely lead to far more dangerous privacy violations around the globe.

Nations are rightly upset that the communications of their citizens are swept up in the National Security Agency’s pervasive surveillance dragnet. There is no question the United States has overreached and violated human rights in its collection of communications information on innocent people around the globe; however, the solution to this problem should not, and truly cannot, be data localization mandates that restrict data storage and flow.

The calls for greater localization of data are not new, but the recent efforts of Brazil’s President, Dilma Rouseff, to protect Brazilians from NSA spying [3] reflected the view of many countries suddenly faced with a new threat to the privacy of the communications of their citizens. Rouseff has been an advocate for internet freedom, so undoubtedly her proposal is well intentioned, though the potential unintended repercussions are alarming.

First, it’s important to consider the technical reasons why data location requirements are a really bad idea. The Internet developed in a widely organic manner, creating a network that allowed data to flow from all corners of the world – regardless of political boundaries, residing everywhere and nowhere at the same time. This has helped increase the resilience of the internet and it has promoted significant efficiencies in data flow. As is, the network routes around damage, and data can be wherever it best makes sense and take an optimal route for delivery.

Data localization mandates would turn the internet on its head. Instead of a unified internet, we would have a fractured internet that may or may not work seamlessly. We would instead see districts of communications that cater to specific needs and interests – essentially we would see Internet gerrymandering at its finest. Countries and regions would develop localized regulations and rules for the internet to benefit them in theory, and would certainly aim to disadvantage competitors. The potential for serious winners and losers is huge. Certainly the hope for an internet that promotes global equality would be lost.

Data localization may only be a first step. Countries seeking to keep data out of the United States or that want to exert more control over the internet may also mandate restrictions on how data flows and how it is routed. This is not far-fetched. Countries such as Russia, the United Arab Emirates, and China have already proposed this [4] at last year’s World Conference on International Telecommunications.

As internet traffic begins to demand more bandwidth, especially as we witness more real-time multimedia applications, efficient routing is essential to advance new internet services. High capacity applications like Apple’s FaceTime may slow to the painful crawl reminiscent of the dial-up days of the internet.

This only begins to illustrate the challenges internet innovators would face, but big established players like Facebook, Google and Microsoft, would potentially have the resources to abide by localization mandates – of course, only if the business case supports working in particular locales. Some countries with local storage rules may be bypassed altogether. For small or emerging businesses, data localization requirements would be a greater challenge. It would build barriers to markets and shut off channels for innovation. Few emerging businesses could afford to locate servers in every new market, and if local data server requirements become ubiquitous, it will be

businesses in emerging markets that are most disadvantaged. The reality for developing nations is that protectionist measures such as data localization will further isolate local business from the global market, depriving them of the advantages for growth that are provided by the borderless internet.

Most important though, is the potential for fundamental harm to human rights due to data localization mandates. We recognize that this is a difficult argument to accept in the wake of the revelations about NSA surveillance, but data localization requirements are a double-edged sword. It is important to remember that human rights and civil liberties groups have long been opposed to data localization requirements because if used inappropriately, such requirements can become powerful tools of control, intimidation and oppression.

When companies were under intense criticism for turning over the data of Chinese activists to China, internet freedom activists were united in theirs calls to keep user data out of the country. When Yahoo! entered the Vietnamese market, it placed its servers out of the country in order to better protect the rights of its Vietnamese users. And the dust up between the governments of the United Arab Emirates, Saudi Arabia, India, and Indonesia, among others, demanding local servers for storage of BlackBerry messages [5] in order to ensure legal accountability and meet national security concerns, was met with widespread condemnation. Now with democratic governments such as Brazil and some in Europe touting data localization as a response to American surveillance revelations, these oppressive regimes have new, albeit inadvertent, allies. While some countries will in fact store, use and protect data responsibly, the validation of data localization will unquestionably lead to many regimes abusing it to silence critics and spy on citizens [6]. Beyond this, data server localization requirements are unlikely to prevent the NSA from accessing the data. U.S. companies and those with a U.S. presence will be compelled to meet NSA orders, and there appear to be NSA access points around the world.

Data localization is a proposed solution that is distracting from the important work needed to improve the Internet’s core infrastructural elements to make it more secure, resilient and accessible to all. This work includes expanding the number of routes, such as more undersea cables and fiber runs, and exchange points, so that much more of the world has convenient and fast Internet access. If less data is routed through the U.S., let it be for the right reason: that it makes the Internet stronger and more accessible for people worldwide. We also need to work to develop better Internet standards that provide usable privacy and security by default, and encourage broad adoption.

Protecting privacy rights in an era of transborder surveillance won’t be solved by ring fencing the Internet. It requires countries, including the U.S., to commit to the exceedingly tough work of coming to the negotiating table to work out agreements that set standards on surveillance practices and provide protections for the rights of privacy and free expression for people. Germany and France [7] have just called for just such an agreement with the U.S. This is the right way forward.

In the U.S., we must reform our surveillance laws, adopt a warrant requirement for stored email and other digital data, and implement a consumer privacy law. The standards for government access to online data in all countries must likewise be raised. These measures are of course much more difficult in the short run that than data localization requirements, but they are forward-looking, long-term solutions that can advance a free and open internet that benefits us all.

-- Read the full text of as Don’t gerrymander the internet [2] in Index on Censorship

Copyright © 2013 by Center for Democracy & Technology.
Source URL: https://www.cdt.org/commentary/don%E2%80%99t-gerrymander-internet

Links:
[1] https://www.cdt.org/personnel/leslie-harris
[2] http://www.indexoncensorship.org/2013/11/dont-gerrymander-internet/
[3] http://bigstory.ap.org/article/brazil-looks-break-us-centric-internet
[4] https://www.cdt.org/blogs/emma-llanso/1012wcit-watch-day-8-quite-ruckus-over-internet-proposals
[5] http://abcnews.go.com/Technology/blackberry-butterfly-effect/story?id=11461691
[6] http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance
[7] http://www.bbc.co.uk/news/world-europe-24665554