

## Munk Debate on State Surveillance Summary

By Alexis Ohanian

We Americans and Canadians have many shared values -- though we may never settle who's really to blame for Justin Bieber -- an inalienable right to privacy is something secured in our Bill of Rights and Canadian Charter of Rights and Freedoms, respectively. Our democratic societies balance this right to privacy with security, but the technological leap we've made in the last decade that has made possible my career as a tech entrepreneur and investor has also enabled a surveillance state that is simply unacceptable.

The NSA has immense capabilities now and the only thing controlling it is secret law. There's precedent of far less efficient surveillance technology being abused -- even Dr. Martin Luther King and many more US citizens involved in the Civil Rights and Anti-War movements were surveilled. Democracy needs sunlight to thrive.

Our reputation has attracted the world's best and brightest, as well as their money, for our highly-regarded global tech industry, but now [Forrester estimates US companies alone stand to lose \\$180 billion to non-US cloud providers](#). The NSA's insatiable appetite for data and mass surveillance has polluted the network. We're all connected online, governments, companies, the very infrastructure of the Internet is no longer healthy because of our brazenness.

From a technological standpoint, the world wide web works best when it's "world wide" and yet we're faced with countries like Brazil and Germany now discussing balkanizing the Internet to guard against intrusion. Steve Huffman and I can't possibly start reddit (a site that now is one of the most popular in the world with 150 million visitors a month, 42% of whom are non-US) and expect it to become a truly global platform without every potential customer having both access and trust in our servers.

We're not just talking about law, we're talking about keeping technology *insecure* so that governments can do mass surveillance. That has a huge impact on user trust, policy debates about privacy, data protection, data localization, and gives comfort to oppressive governments that want to surveil the Internet. This is important, because what we're doing in the name of counterterrorism is actually

undermining security elsewhere -- finding security flaws and leaving them for anyone to exploit later is not sound policy.

A rising tide really does lift all boats -- or in this case, lock all doors -- when it comes to online security.

Speaking of which, that word, security, means different things to my opponents. I'm not talking about trading security for privacy, I'm talking about trading one kind of security for another kind of security. First, these tools aren't just being used for counter-terrorism. Second, the things done in the name of counter-terrorism are *hurting* other kinds of security.

I was lucky enough to get a 33.6 modem in my home while I was still in grade school. It changed my life. Today I'm a serial tech entrepreneur and an investor in over 100 startups thanks to the open Internet. I've built and backed international corporations run from laptops because the greatest privilege of entrepreneurship in countries like the USA and Canada is the benefit that comes from the values of our free societies.

They must be defended, but thoughtfully, because we need to lead the world by example when it comes to ensuring the Internet -- a fundamentally democratic global platform -- embodies all the values we as democracies hold so dear and mass surveillance undermines the very security it purports to protect.