Decrypting the Web

Siva Vaidhyanathan - October 18, 2010

HERE IS how it works.

Step 1: Bad guys use encryption to mask their communications from snooping intelligence and law enforcement officials.

Step 2: Frustrated with the hassles of deploying that dependable eighteenth-century technology, the court-issued warrant, to combat the bad guys, officials call for radical changes in the architecture of computer and communication technology, yet try to sell proposals as a modest "updating" of the law for the digital age.

Step 3: Steadily, officials face withering criticism from encryption experts, civil libertarians, computer engineers, and representatives of firms that wish to do business globally. They all make the strong case that these measures would do little to stop the real bad guys but could do significant damage to the good (or at least innocent) people and firms using encryption technology.

We witnessed these steps in the mid-1990s under the Clinton administration, in response to the proliferation of encrypted mobile phone communication among al Qaeda leaders and organized crime figures. Despite the fact that the security breeches that enabled the attacks of September 11, 2001 were completely analog in nature, we heard similar calls for technological overhaul in the aftermath of those attacks from UK Foreign Secretary Jack Straw and Richard Clarke, terrorism chief (later cyberterrorism czar) in the early days of the George W. Bush administration.

And now, according to the *New York Times*, some officials in the Obama administration are once again exploring restrictions on the use of strong encryption—or at least a key to the back door of secure commercial communication systems such as BlackBerry networks and Skype, the brilliant voice and video communication service.

The silly thing about this proposal is that federal officials are actually trying to regulate math. More precisely, they want to outlaw some kinds of math. Encryption is just a mathematical

system by which computers hide information, rendering it unreadable to unauthorized humans. Under a proposal outlined in September, the government would determine what sorts of encryption algorithms would be legal—those that left a spare key with federal law enforcement, for instance—and what sorts would be illegal. These officials actually think they can stop small strings of computer code from flowing around the electronic networks of the world simply by making a law against them.

It sounds absurd, but the consequences for a service like Skype would be quite grave. If the new proposal goes through, Skype would be illegal as it currently operates. Skype is a distributed network, much like the old Napster music downloading service—it merely connects one user to another. The actual data carrying voice and video travels circuitous routes around the Internet without running through Skype's own servers. The entire communication stream is encrypted, so that only the two users on the endpoints of the conversation can understand the data stream. Skype is free to use and has been widely adopted by those with friends, family members, or business associates in other countries. Some of these countries, of course, are authoritarian and censorious. So Skype is particularly valuable to those who hope to challenge oppressive regimes—or at least let emigrants from those countries speak to each other without fear of repercussions, such as imprisonment or torture. Under the current proposal, if the *New York Times* account is accurate and complete, Skype would have to build itself from the ground up as a centralized service so that it could monitor activity and offer law enforcement access to the content that flows through it. That would make Skype expensive, inefficient, vulnerable, undependable, slow, and insecure.

It's possible that proposals like this might have had limited success or given meager aid to law enforcement in the early 1990s, but U.S. officials are acting twenty years too late. The widespread availability and use of "off the shelf" encryption services makes such a proposal in 2010 laughable. All it would do is turn "off the shelf" encryption into "black market" encryption. What would this look like? If companies doing business within the United States had to submit their keys to U.S. officials, small firms from the former Soviet republics or the Philippines (two major sites of hacker training and activity) would jump at the chance to sell black-market encryption protections to organized crime or terrorist syndicates. Even legitimate global corporations might find comfort in an extra layer of black-market protection here and there. Certainly, many bad guys use Skype, which is encrypted well enough for their needs. But if this proposal becomes policy, bad guys simply would switch to some non-U.S.-based services, which the FBI can't threaten or control. However, immigrants who use Skype could find themselves spied upon as they discuss events back in their countries of origin.

The full futility of this proposal becomes clear as soon as one looks at its most obvious implications. In short: for three decades the U.S. government has been trying to make encrypted communication subject to surveillance. And through three administrations it's been clear that really bad people would still be able to hide their plans from law enforcement and intelligence. Rather than stopping these bad people, these efforts would subject innocent people to massive surveillance of their communications—not only by the United States, but by Egypt, Pakistan, India, China, Russia, Iran, or the United Arab Emirates. So such policies would be intrusive to the innocent, a slight hassle for the guilty, expensive for all, and would give us a false sense of security—a description that applies to many post-9/11 policies.

But the current proposal could have even greater adverse effects. If, by government order, encrypted information becomes easier to decrypt, it's not just the U.S. government that would have greater access: any hole in an otherwise secure system could be exploited by nefarious elements far more hostile to commerce or privacy than the NSA or FBI. Corporate

espionage—even state-sponsored corporate espionage—is certain to increase in scope if its agents know that BlackBerries are now insecure.

As civil liberties advocate Julian Sanchez has explained, this move puts the United States in the distinguished company of Saudi Arabia and the United Arab Emirates. All of these countries have tried in recent months to snoop on BlackBerry users.

Yet just ten months ago U.S. Secretary of State Hillary Clinton gave a stirring speech about the commitment the United States has made to keep the Internet free and open for the sake of those struggling for freedom against governments very much like Saudi Arabia and the United Arab Emirates. The State Department even helped launch failed (and perhaps fraudulent, as Evgeny Morozov reported at *Slate* in September) efforts to roll out encryption technologies for use by dissidents in China and Iran. "Governments and citizens must have confidence that the networks at the core of their national security and economic prosperity are safe and resilient," Clinton said in her speech in January 2010. "This is about more than petty hackers who deface websites. Our ability to bank online, use electronic commerce, and safeguard billions of dollars in intellectual property are all at stake if we cannot rely on the security of information networks." In other words: according to Clinton, the United States supports the proliferation of strong encryption for the purposes of keeping governments from snooping and criminals from stealing.

THE INTERNET doesn't mean to be bad. Like Jessica Rabbit, it's just drawn that way. The problem is, if we want a technological solution to complex, vexing human problems, we would have to radically re-engineer the Internet and all the devices that interact with it. We let the Internet be the Internet back in the 1990s, when we assumed a peaceful world would use it for learning, exploring, and (most of all) shopping. We reveled in its decentralized architecture. We celebrated its alleged (and largely unrealized) power to "route around censorship." And president after president after president has proclaimed Internet freedom the key to pushing the consciousness of the globe toward the noble goals of democracy, human rights, and powerful markets. Oddly, the security tentacles of U.S. government keep pushing for policies that run directly against U.S. diplomatic and commercial efforts.

At some point, U.S. leaders are going to have to confront this clear contradiction in American policy and principles. Everyone else sees it. One White House official has assured me that even within the administration, there is substantial doubt that policies such as this are feasible and beneficial. So for the third decade in a row, it might not emerge as real legislation or regulation.

We are steadily learning that the Internet is neither a panacea for our species' ills nor the source of them. The "network of networks" is hard to govern, but it's not radically free either. We have only just begun to understand the consequences of ubiquitous, constant, global human communication. Radical plans and proclamations about the nature, potential, or dangers of digital networks should be greeted with healthy skepticism.

Siva Vaidhyanathan is a professor of media studies and law at the University of Virginia and the author of the forthcoming book, *The Googlization of Everything (And Why We Should Worry)* (University of California Press).

Homepage image: Mark Pellegrini/Wikimedia Commons/2007

encryption, national security, wiretapping