

Whether that view or this architecture of the Internet itself persists has other members of the academy concerned as well. As Harvard computer science professor Jonathan Zittrain observes in the Scientific American, keeping the Internet open, distributed and free is not a certain outcome.

Attacks on Internet sites and infrastructure, and the compromise of secure information, pose a particularly tricky problem because it is usually impossible to trace an attack back to its instigator. This "attribution problem" is so troublesome that some law-enforcement experts have called for a wholesale reworking of Internet architecture and protocols, such that every packet of data is engraved with the identity of its source. The idea is to make punishment, and therefore deterrence, possible. Unfortunately, such a reworking would also threaten what makes the Internet special, both technologically and socially.

The Internet works thanks to loose but trusted connections among its many constituent parts, with easy entry and exit for new Internet service providers or new forms of expanding access. That is not the case with, say, mobile phones, in which the telecom operator can tell which phone placed what call and to whom the phone is registered. Establishing this level of identity on the Internet is no small task, as we have seen with authoritarian regimes that have sought to limit anonymity. It would involve eliminating free and open Wi-Fi access points and other ways of sharing connections. Terminals in libraries and cybercafes would have to have verified sign-in rosters. Or worse, Internet access would have to be predicated on providing a special ID akin to a government-issued driver's license—perhaps in the form of a USB key. No key, no bits. To be sure, this step would not stop criminals and states wanting to act covertly but would force them to invest much more to achieve the anonymity that comes so naturally today.

The history of the introduction of new communication tools is a reminder that most disruptive technologies have dual uses. In 1924, Calvin Coolidge was the first President of the United States to make a radio broadcast from the White House. A decade later, Hitler and Stalin were using the same tool to spread a different kind of message.

Nearly a century later, the current occupant of the White House is using YouTube, Facebook, Twitter, apps and live video on WhiteHouse.gov to communicate with citizens, both of the United States or in other countries. While the White House can claim some open source cred for running WhiteHouse.gov on Drupal, much of the rest world has long since becoming aware of the disruptive nature of a more wired society that is connected to the Internet.

The debate about the role of connection technologies in Internet freedom spans many audiences. Last month, the discussion came to the Cato Institute, where a debate on social media and revolutions was moderated by Jim Harper, Director of Information Policy Studies at Cato. The discussion featured Christopher Preble, Director of Foreign Policy Studies at Cato Institute, Tim Karr, Campaign Director, Free Press, and this correspondent.

The same platforms that can and are being used to transmit breathtaking moments of wonder, hear digital cries for help or lift up the voices of the citizens in oppressed societies to the rest of the world will also be used against them. Palfrey has further explored Middle East conflict and an Internet tipping point for the Internet at MIT's Tech Review. His conclusion is worth sharing again:

Today, we are entering a period that we should call "access contested." Activists around the world are pushing back on the denial of access and controls put in place by states that wish to restrict the free flow of information. This round of the contest, at least in the Middle East and North Africa, is being won by those who are using the network to organize against autocratic regimes. Online communities such as Herdict.org and peer-to-peer technologies like mesh networking provide specific ways for people to get involved directly in shaping how these technologies develop around the world.

But it would be a big mistake to presume that this state of affairs will last for long, or that it is an inevitable outcome. History shows us that there are cycles to the way that technologies, and how we use them, change over time, as Timothy Wu argues in his new book, The Master Switch. The leaders of many states, like China, Vietnam, and Uzbekistan, have proven able to use the Internet to restrict online discussion and to put people into jail for what they do using the network. We should resist the urge to cheer the triumph of pro-Western democracy fueled by widespread Internet access and usage. The contest for control of the Internet is only just beginning.

As the rest of the world watches the changes sweeping the Middle East through snippets of cellphone video uploaded to YouTube and curated by digital journalists like Andy Carvin, connected citizens have

March 4, 2011 by David Eaves

Are the Internet and Social Media 'Tools of Freedom' or 'Tools of Oppression?' March 8, 2011 by Alexander Howard

Workers vs. widgets: policing in the age of high tech

States worry over current year budget battles in Congress March 4, 2011 by Jeff Smith

March 5, 2011 by Christa Miller

Transit data as open government fuel for economic growth March 7, 2011 by Alexander Howard

