Joining Zone Nine

REBECCA MACKINNON

A Global Voices Online blog entry written in the Ethiopian language of Amharic contains an update on jailed Ethiopian Journalist Reeyot Alemu.

"We want more openness, more transparency," Ethiopian writer Endalkchew Chala observes. "People deserve choice; people deserve access to the world's knowledge." For expressing views like these online, his friends were scheduled to go on trial for terrorism in early August—though the trial has since been adjourned to October 15. Perhaps because the absurd charges against them were getting more international attention than expected.

TERRORISTS' SOCIAL MEDIA CAMPAIGNS

World Policy Journal's Fall 2014 timeline tracks the phenomenon of terrorist organizations employing social media to recruit members, broadcast their messages, and wage online warfare.

Compiled by Lara Pham, Cami Tellez, and Marguerite Ward.

Two years ago Endalk (as his friends and colleagues like to call him) got together with several like-minded young Ethiopian writers and journalists to launch a hard-hitting blog called "Zone 9." The blog's name derives from Addis Ababa's infamous Kaliti prison, divided into eight zones with political prisoners confined to Zone Eight. Young bloggers believed that the entire nation was becoming a virtual prison—effectively a ninth zone. "All of Ethiopia is part of it," explains Endalk. In 2011, one inmate, journalist Eskinder Nega, was arrested for the seventh time after writing a column, which ironically criticized the Ethiopian government's habit of arresting journalists on terrorism charges.

Such edginess was too much for their government to take. Seven of the "Zone 9" bloggers were arrested this past April. Then, three months later, they were formally charged with terrorism and "related activities." Endalk, pursuing a graduate degree in Portland, Oregon when the arrests took place, is now their spokesperson, blogging and tweeting the latest developments. The group's alleged crimes include attending trainings by international technical experts on how to use software tools to shield themselves from electronic surveillance. They are also accused of clandestinely organizing themselves into a blogger collective—a bizarre accusation given that "Zone 9" is a public website.
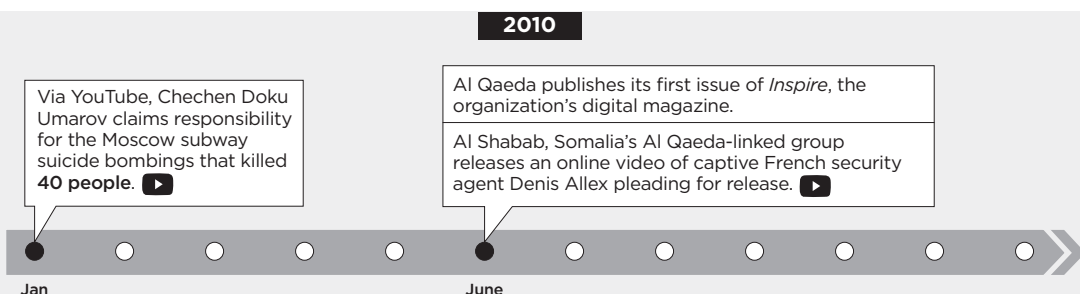
For the past two years, Endalk and four other "zone niners" also ran an Amharic edition of Global Voices Online, an international citizen media network that I co-founded nearly ten years ago with the media scholar and blogger Ethan Zuckerman. The Ethiopian branch translates blog posts written by contributors from around the world—particularly those related to activism, freedom of expression, and censorship— of strong relevance to an Ethiopian audience whose state-controlled media is heavily censored.

BARS AROUND THE WORLD

Disturbingly, the Zone 9 bloggers are not the only Global Voices contributors who recently found themselves behind bars, as governments in a disturbingly growing list of nations have recognized that modern-day connectivity can prove a lethal challenge to their legitimacy and very existence.

Bassel Khartabil, a Syrian-Palestinian computer engineer and open Internet advocate, has been imprisoned in Damascus

Rebecca MacKinnon directs the Ranking Digital Rights project at the New America Foundation. Author of Consent of the Networked: The Worldwide Struggle For Internet Freedom, *she is co-founder of Global Voices Online and a former CNN bureau chief and correspondent in Beijing and Tokyo.*

2010

Via YouTube, Chechen Doku Umarov claims responsibility for the Moscow subway suicide bombings that killed **40 people**.

Al Qaeda publishes its first issue of *Inspire*, the organization's digital magazine.

Al Shabab, Somalia's Al Qaeda-linked group releases an online video of captive French security agent Denis Allex pleading for release.

Jan
June

since March 2012. Alaa Abd El Fattah, an Egyptian activist and blogger arrested in November 2013 for violating Egypt's new Protest Law, was dealt a 15-year jail sentence along with 25 other activists this past June. Tajik author Alex Sodiqov—a Ph.D. student at the University of Toronto—was arrested while carrying out academic research in the Gorno-Badakhshan Autonomous Region of Tajikstan. Eventually he was accused of espionage. While he has since been released, he has yet to be cleared of the charges.

The idea for the Global Voices network came out of a 2004 meeting of bloggers from around the world. It was a time of heady optimism, when bloggers seemed poised to break down barriers and help create a better world. We created a website with the tagline "The world is talking. Are you listening?" As our manifesto put it:

"Thanks to new tools, speech need no longer be controlled by those who own the means of publishing and distribution, or by governments that would restrict thought and communication. Now, anyone can wield the power of the press. Everyone can tell their stories to the world."

We recruited a set of editors and volunteers from across the globe who helped to curate, translate, and contextualize what bloggers were saying about their countries and regions—what they were observing in their communities, and how people around them were reacting to world events. Eventually, the site came to be translated back
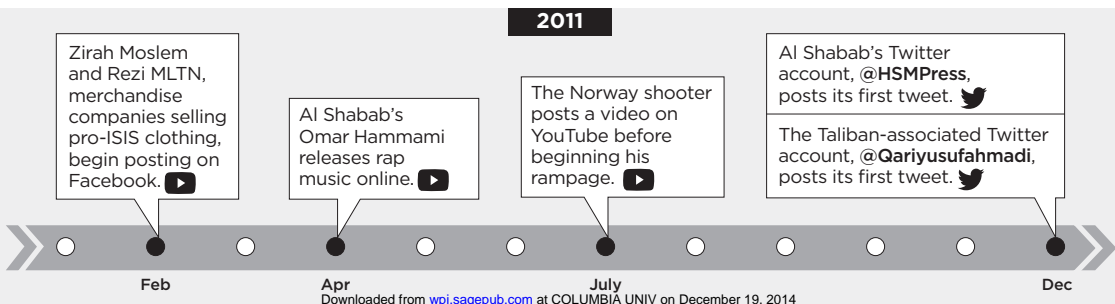
and forth in over two dozen languages, mainly by volunteers like the Zone 9ers.

Digital connectivity can indeed be revolutionary. In the 21st century, networked technologies are a necessary condition for social and political change. But over the past decade we've learned they are insufficient on their own to prevent widespread and systematic human rights violations— let alone bring about a more democratic and just world.

BATTLING EMPOWERMENT
Governments are fighting back against the Internet's empowering, decentralized character. They are upgrading their own institutional, military, and technical power. They are passing laws criminalizing various forms of online speech and enforcing those laws with police, security, and intelligence forces. Law enforcement and intelligence services of democracies, as well as dictatorships, are pushing their powers of surveillance to the limit. Many governments are also finding new and creative ways to control through their legal and technical powers what people can and especially cannot do on the Internet and with mobile devices.

The Ethiopian government is a case in point. It has revised the law so that practically anybody who uses the Internet to build a movement around a common ideal, or conduct independent journalism, can potentially be charged with terrorism. Internet access is available only through the state controlled monopoly, Ethio Telecom, which keeps

2011

Zirah Moslem and Rezi MLTN, merchandise companies selling pro-ISIS clothing, begin posting on Facebook.

Al Shabab's Omar Hammami releases rap music online.

The Norway shooter posts a video on YouTube before beginning his rampage.

Al Shabab's Twitter account, @**HSMPress**, posts its first tweet.

The Taliban-associated Twitter account, @**Qariyusufahmadi**, posts its first tweet.

Feb   Apr   July   Dec

prices artificially high and beyond the reach of most. Those who can access the Internet do so through heavily monitored cybercafés. They must navigate censorship blocking overseas dissident websites, and face pervasive surveillance thanks to technologies purchased not only from Chinese companies but from European firms like FinFisher, a German company that sells remote monitoring systems, and Hacking Team, an Italian firm specializing in spyware.

Anything the Zone 9 bloggers ever did online can potentially be used against them without constraint.

The attack by governments on Internet freedom is by no means limited to authoritarian dictatorships. This year, alongside the usual suspects like North Korea, Cuba, and China, Reporters Without Borders listed the Indian government's Centre for Development of Telematics as one of the 20 biggest "enemies of the Internet," thanks to its role in developing a clandestine mass electronic surveillance and data mining program for deployment on nationwide networks.

The United Kingdom also made the list, winning the title "world champion of surveillance," due largely to the work of the Government Communications Headquarters (GCHQ), which has developed the world's largest data collection and communications-monitoring system. Last month the British authorities invoked emergency powers to pass a new law allowing th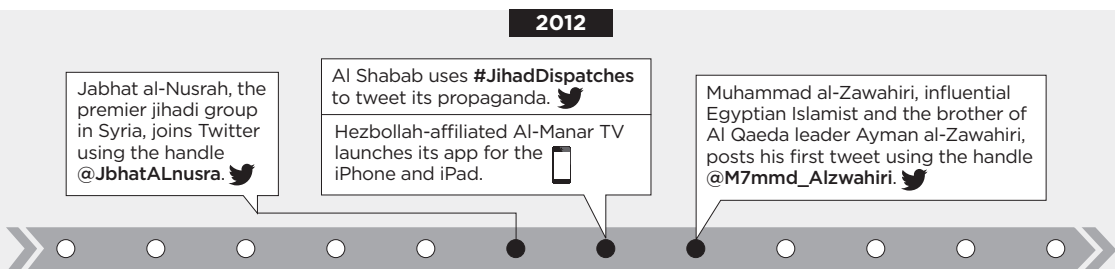e government to issue warrants to companies for data stored outside UK jurisdiction—effectively legalizing its already sweeping technical power to spy on much of the world. As former NSA contractor Edward Snowden put it, "they are worse than the U.S."

The problem has been compounded by Internet and telecommunications companies pursuing short-term business interests without considering the impact of their behavior on Internet users' rights. We have all unfortunately allowed companies to track, collect, and sell vast amounts of personal information without even realizing what was happening. As American security guru Bruce Schneier likes to say: "Surveillance is the business model of the Internet."

> WE HAVE ALL UNFORTUNATELY ALLOWED COMPANIES TO TRACK, COLLECT, AND SELL VAST AMOUNTS OF PERSONAL INFORMATION WITHOUT EVEN REALIZING WHAT WAS HAPPENING.

How convenient for the NSA, which, until Snowden blew the whistle, had relatively easy access to the communications and stored data of U.S. Internet companies. Now many of these companies have recognized that this situation is not actually sustainable for their business in the long run. Without basic levels of trust from individuals and businesses that rely on the

2012

Jabhat al-Nusrah, the premier jihadi group in Syria, joins Twitter using the handle @**JbhatALnusra**.

Al Shabab uses **#JihadDispatches** to tweet its propaganda.

Hezbollah-affiliated Al-Manar TV launches its app for the iPhone and iPad.

Muhammad al-Zawahiri, influential Egyptian Islamist and the brother of Al Qaeda leader Ayman al-Zawahiri, posts his first tweet using the handle @**M7mmd_Alzwahiri**.

June   July   Aug

Internet, its platforms, and networks, the economic value of the Internet (along with its political and social value) will diminish over time. That is precisely why major companies like Google, Microsoft, and Facebook are now calling publicly for legal limitations on the NSA's powers, as well as increased government transparency on matters of surveillance.
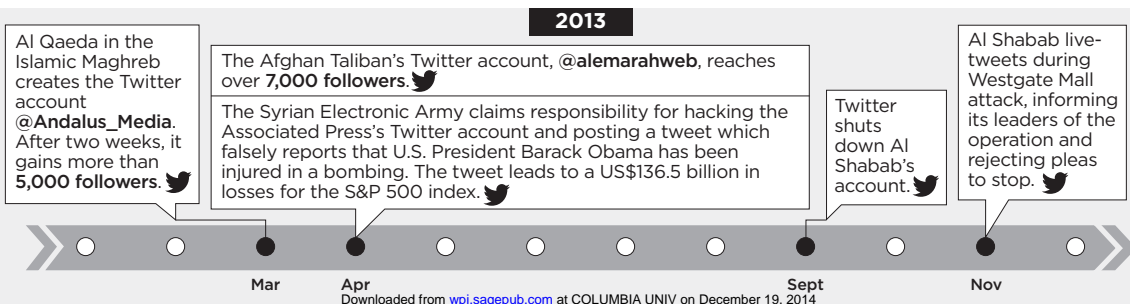
CYBER SOVEREIGNS

These sovereigns of cyberspace—an apt term because of the rules and parameters they set on their services, on which we have come increasingly to depend—have become a form of trans-national private governance. The Internet is replete with corporate and government gatekeepers. It's patrolled by a variety of virtual police seeking to enforce government laws and company terms of service. These gatekeepers and police must be held publicly accountable in a way that can constrain them from abusing their power.

It is up to all of us, as citizens of nations and as denizens of a globally interconnected Internet, to keep pushing for accountability in how our digital lives are shaped and governed by all who wield power over us. If digital connectivity is to fulfill its clear potential, nations' legal frameworks governing Internet companies, as well as users, must embrace the protection and exercise of basic human rights. The technical standards and business practices of companies must be compatible with the kind of open, democratic world we seek to create.

We are far from reaching that goal, but some important steps are being taken in the right direction. Legal reform efforts to curb government surveillance powers in the United States are making headway. Initiatives are being built to hold tech companies to basic human rights standards, including freedom of expression and privacy. Global Voices is working with a worldwide community of people ready to fight for their online freedoms, working with other trans-national groups advocating an open Internet.

As we think globally, those of us lucky enough to live in democracies must not forget that Internet freedom starts at home. If we cannot figure out how to constrain government and corporate power over digital networks people depend on, prepare to join our Ethiopian friends in Zone 9. ●

2013

Al Qaeda in the Islamic Maghreb creates the Twitter account @**Andalus_Media**. After two weeks, it gains more than **5,000 followers**.

The Afghan Taliban's Twitter account, @**alemarahweb**, reaches over **7,000 followers**.

The Syrian Electronic Army claims responsibility for hacking the Associated Press's Twitter account and posting a tweet which falsely reports that U.S. President Barack Obama has been injured in a bombing. The tweet leads to a US$136.5 billion in losses for the S&P 500 index.

Twitter shuts down Al Shabab's account.

Al Shabab live-tweets during Westgate Mall attack, informing its leaders of the operation and rejecting pleas to stop.

Mar   Apr   Sept   Nov

2014

Al Qaeda announces via video its launch of its first digital English magazine, *Resurgence.*

ISIS's app, The Dawn of Glad Tidings or simply Dawn, goes live on Google Play.

Boko Haram claims responsibility via viral video for the kidnapping of nearly **250 schoolgirls** in Nigeria.

Posting activity through ISIS's app reaches an all-time high of almost **40,000 tweets** as group storms the city of Mosul, Iraq.

Twitter suspends six accounts affiliated with ISIS.

ISIS begins using the hashtag **#AllEyesOnISIS** to build grassroot support on Twitter.

Israel and Hamas clash on social media, denouncing each other on Twitter and Facebook.

Mar   Apr   June   July