The Christian Science Monitor presents:

Passcode

Modern field guide to security and privacy

TODAY'S BIG IDEA

Ethiopia's web crackdown

Ethiopia has issued a six-month state of emergency in the country following months of citizen protests. Government forces have killed more than 500 people since November 2015 and authorities have already shut down access to social media in the Oromia region four times this year. Now the situation is escalating, with the government cutting mobile internet in the capital Addis Ababa for more than a week.

Internet shutdowns do not restore order. They hamper journalism, obscure the truth of what is happening on the ground, and stop people from getting the information they need to keep safe. Further, shutdowns harm the local economy; by June 2016, Ethiopia had already lost $8.5 million due to internet disruptions, according to a recent report by the Brookings Institution.

It will take effort from many corners to restore Ethiopia from its human rights crisis and protect privacy and free expression in the long term. Ethiopia should to immediately restore full internet access in the country and repeal sections of a proposed computer crime law that threatens human rights. Digital rights organizations globally must draw attention to what is happening so Ethiopians can exercise their rights and freedoms, and above all, stay safe from harm. **Read more.** // Ephraim P. Kenyanito

WHAT WE'RE WRITING

Report finds racial bias in facial recognition technology

More than 40 rights groups asked the Department of Justice to launch a probe examining whether systems used by police to investigate crimes disproportionately identify blacks as criminal suspects. // Jeff Stone

PASSCODE EVENTS

Security of Things Forum // Washington

On **Thursday, Oct. 27**, Passcode and The Security Ledger will host the Security of Things Forum-DC for a daylong exploration into IoT security issues facing industry.
Code **PCREADER** will give you a 20 percent discount. **Register here**

TODAY: Cyber Risk Wednesday: Hacking the Vote // Washington

E-voting could expose the US electoral process to an unprecedented scale of vulnerabilities. Join the Atlantic Council's Cyber Statecraft Initiative today **from 4:00 to 5:30 p.m.** for an examination of threats facing our election systems. **Register to attend here or watch live here**

WHAT WE'RE READING

Ever heard of Solar Sunrise?
As the US prepared for a series of bombings against Iraq in 1998, Defense Department computer networks containing medical, personnel, and logistics records came under attack from hackers from the United Arab Emirates, France, Germany, and Taiwan. New FBI memorandums sent soon after the attacks, and released Wednesday by the National Security Archive, show that the bureau quickly investigated the hacks, worried they could disrupt US military deployments. But when the probe concluded, investigators found out that teenagers in California and Israel, not nation-state hackers, were behind the attack. Today, you can credit the so-called "Solar Sunrise" attack with changing US views on cybersecurity: it led the Pentagon to establish a 24-hour emergency watch for digital attacks. // National Security Archive

WHAT'S TRENDING

The most influential topics and stories, as curated by Passcode's social media mining algorithm.*

Did British security agencies unlawfully collect data?

British intelligence practices are under the microscope. On Monday, the investigatory powers tribunal, which hears complaints against British spy agencies, says MI5, MI6, and GCHQ illegally operated schemes to scoop up users' communications, including phone and web use that included sensitive personal information. // The Guardian

Stuxnet leaker found

If you know anything about Stuxnet, the software virus almost certainly developed by the US and Israel to cripple Iranian nuclear centrifuges, it's probably because of former Joint Chiefs of Staff Vice Chairman Gen. James E. Cartwright. According to court documents, Mr. Cartwright lied to Justice Department investigators about leaking the program to a New York Times reporter. // Washington Post

Did trolls kill Twitter deal?

Salesforce CEO walked away from a potential acquisition of social media giant Twitter last week, saying the deal wasn't a good fit for the cloud computing company. But according to CNBC host Jim Kramer, another factor might have helped nix the deal: Twitter's difficulty stopping abuse and hate speech on the platform. // Business Insider

Hillary Clinton's not the only one with an insecure email server

Donald Trump said at the last presidential debate that Hillary Clinton should be prosecuted for using a private email server during her time as Secretary of State. But according to security experts, Mr. Trump's email servers use out of date Windows software that could be easily exploited by hackers. // Motherboard

*About this section: The Passcode algorithm tracks more than 100,000 Twitter accounts followed by prominent people in security and privacy to determine which arguments, ideas, and stories are the most influential. We unravel their social media conversation in every newsletter. We're watching Twitter so you don't have to.

Know someone who would like Passcode?

Forward our newsletter along. Anyone can subscribe for free.

See full Passcode coverage on The Monitor's website and our long form storytelling platform.

PASSCODE

BOSTON | WASHINGTON, D.C.

By Mike Farrell, Sara Sorcher, Jeff Stone, and Jack Detsch

www.csmpasscode.com

You signed up to receive Passcode's digest of global cybersecurity news and analysis.

View this email as a web page

Send us news tips, event notices and comments to passcode@csmonitor.com

Click here for a special Monitor subscription offer for Passcode readers.

The Christian Science Monitor

210 Massachusetts Ave

Boston, MA 02115

Add us to your address book

Unsubscribe from this list. | Update your profile