George Orwell was an optimist

“Who controls the past, controls the future: who controls the present controls the past”

— George Orwell, Nineteen Eighty Four, 1949
Internet Censorship Is Everywhere

Internet censorship map.

Blue: No censorship
Yellow: Some censorship
Red: Under surveillance
Black: Internet black holes (most heavily censored nations)
Dear User,

Sorry, the requested page is unavailable.

If you believe the requested page should not be blocked please click here.

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa
Internet Censorship Is Everywhere
Internet Censorship Is Everywhere

This domain name has been seized by ICE - Homeland Security Investigations, pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981 and 2323.

Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C § 506, 18 U.S.C. § 2319). Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution (18 U.S.C. § 2320).
Censoring the ’net is all the rage

China increases Internet control, takes down hundreds of websites
Censoring the ’net is all the rage

“more than 700 pornographic and copyright infringing websites have been shut down"
Censoring the 'net is all the rage

Exclusive: Top ISPs poised to adopt graduated response to piracy

by Greg Sandoval

Some of the country’s largest Internet service providers are poised to leap into the antipiracy fight in a significant way.

After years of negotiations, a group of bandwidth providers that includes AT&T, Comcast, and Verizon are closer than ever to striking a deal with media and entertainment companies that would call for them to establish new and tougher punishments for customers who refuse to stop using their networks to pirate films, music and other intellectual property, multiple sources told CNET.

The sources cautioned that a final agreement has yet to be signed and that the partnership could still unravel but added that at this point a deal is within reach and is on track to be unveiled sometime next month.
In the future everyone will be anonymous for 15 minutes
Internet Surveillance is getting more advanced

If You Can See It
You Can Monetize It

Evolved DPI – See what’s flowing through your network
Internet Surveillance is getting more advanced
'Comodo Hacker' Says He Acted Alone

The plot thickens: In an effort to back up his claims, alleged hacker dumps apparent evidence of pilfered database from breached Comodo reseller, as well as Mozilla add-on site certificate

By Kelly Jackson Higgins InformationWeek
April 09, 2011 12:00 AM

Comodo, a website certificate authority, revealed that nine SSL certificates were issued for fraudulent websites posing as domains for high-profile sites. Security researchers hope the incident will call attention to a certificate process they say is riddled with holes.
US company 'helped' Egypt block web

Egypt's crackdown on web users allegedly aided by US company's product.

Last Modified: 06 Feb 2011 03:23 GMT

When Egypt's uprising began nearly two weeks ago, there was a near-total internet blackout.

But exactly how was access cut off?

An American advocacy group called Free Press says it has uncovered a link to a California-based technology company that allegedly sold the Egyptian government equipment allowing it to track online activity.

Al Jazeera's Rob Reynolds reports.
Internet Surveillance is getting more advanced
DigiNotar Damage Disclosure

Posted September 4th, 2011 by ierror in ca certificates, https, ohdiginotaryoudidnt, ssl certifications, tor client safety, tor network safety, tor project website

About an hour ago I was contacted by the Dutch Government with more details about the DigiNotar Debacle. It seems that they're doing a great job keeping on top of things and doing the job that DigiNotar should've done in July. They sent a spreadsheet with a list of 531 entries on the currently known bad DigiNotar related certificates.

The list isn't pretty and I've decided that in the interest of defenders everywhere without special connections, I'm going to disclose it. The people that I have spoken with in the Dutch Government agree with this course of action.

This disclosure will absolutely not help any attacker as it does not contain the raw certificates; it is merely metadata about the certificates that were issued. It includes who we should not trust in the future going forward and it shows what is missing at the moment. This is an incomplete list because DigiNotar's audit trail is incomplete.

This is the list of CA roots that should probably never be trusted again:

DigiNotar Cyber CA
DigiNotar Extended Validation CA
DigiNotar Public CA 2025
DigiNotar Public CA - G2
Koninklijke Notarieele Beroepsorganisatie CA
Stichting TTP Infos CA

The most egregious certs issued were for *.com and *.org while certificates for Windows Update and certificates for other hosts are of limited harm by comparison. The attackers also issued certificates in the names of other certificate authorities such as "VeriSign Root CA" and "Thawte Root CA" as we witnessed with ComodoGate, although we cannot determine whether they succeeded in creating any intermediate CA certs. That's really saying something about the amount of damage a single compromised CA might inflict with poor security practices and regular internet luck.
Internet Surveillance is getting more advanced

“The most egregious certs issued were for *.abc.com and *.xyz.org while certificates for Windows Update and certificates for other hosts are of limited harm by comparison. The attackers also issued certificates in the names of other certificate authorities such as ”VeriSign Root CA” and ”Thawte Root CA” as we witnessed with ComodoGate...”

— Tor Project blog, https://blog.torproject.org/blog/diginotar-damage-disclosure
The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy
Tor hides communication patterns by relaying data through volunteer servers

Diagram: Robert Watson
Tor hides communication patterns by relaying data through volunteer servers

Diagram: Robert Watson
Tor hides communication patterns by relaying data through volunteer servers
Tor hides communication patterns by relaying data through volunteer servers.

Diagram: Robert Watson
Thanks!

Visit https://www.torproject.org/ for more information, links, and ideas.
Copyright & Sources

- Internet censorship is everywhere, first image: Reporters without Borders, http://www.rsf.org
- censoring the ’net is all the rage,
- censoring the ’net is all the rage,
- Internet surveillance, second image: 
- Internet surveillance, third image: Al Jazeera, February 2011
- spring is in the air, Paco Pomet, http://pacopomet.wordpress.com/