

Global Policy Weekly - June 27, 2013

by [Emily Barabas](#) [1]
June 27, 2013



CDT's Global Policy Weekly highlights the latest Internet policy developments and proposals from around the world, compiled by CDT's [Global Internet Freedom Project](#) [2].

FREE EXPRESSION

The government of the UK will expect all Internet Service Providers (ISPs) to [begin providing](#) [3] content filters as a default setting before 2014. The filters are intended to reduce children's exposure to pornographic content on the Internet. Governments expect ISPs to participate voluntarily without any additional regulations. The plan is part of a broader UK initiative to reduce children's exposure to inappropriate content. It follows an announcement from the government that public Wi-Fi networks will be expected to [block pornographic content](#) [4].

The annual Freedom Online Coalition conference was held in Tunis, convening governments, civil society, and companies to discuss issues related to the open Internet and human rights. In the days leading up to the conference, a hacker space called #404Lab launched in the former home of the country's ousted dictator, Ben Ali. #404Lab participants [installed an open Wi-Fi network](#) [5] for use by the community. The Tunisian Internet Agency also [invited hackers](#) [6] to decrypt censorship technologies once used in the building's basement.

PRIVACY

Protestors in Turkey have [relied heavily](#) [7] on Twitter to spread information about demonstrations in Gezi Park. In response, the Turkish government has [announced that is cracking down on social media](#) [8] in the country. Deputy Prime Minister Bekir Bozdağ said that people using "fake" accounts have incited protests and spread misinformation. Bozdağ told reporters that the government will be drafting new laws to prevent the use of "fake" social media accounts in Turkey.

SECURITY AND SURVEILLANCE

Researchers at [Citizen Lab](#) [9] reported that they found Internet filtering tools [installed on a network](#) [10] belonging to the Pakistan Telecommunication Company Limited (PTCL), the country's largest telecom provider. The technology, called Netsweeper, can be used to limit user access to independent media, as well as websites related to human rights and religion. In 2012, the government of Pakistan requested proposals for a national URL filtering system. Bytes for All [criticized the adoption](#) [11] of Netsweeper and raised concerns about human rights implications of the tool.

The OECD [agreed to consider a complaint](#) [12] against Gamma International, a company that allegedly sells surveillance technologies to governments that violate human rights. The complaint, filed by [Privacy International](#) [13], the [European Center for Constitutional and Human Rights](#) [14], the [Bahrain Center for Human Rights](#) [15], [Bahrain Watch](#) [16], and [Reporters without Borders](#) [17], argues that the UK-based company acted against recommendations in the OECD Guidelines. Gamma responded by saying the company "would not supply the product identified in the complaint in a situation where it believed it would be used for the purpose of repressing civil rights."

[Access](#) [18], [Article 19](#) [19], [PEN International](#) [20], and [English PEN](#) [21] wrote a [joint submission](#)

[22] to the United Nations Universal Periodic Review (UPR) expressing concern about human rights violations in Vietnam. The UPR reviews the human rights record each UN member state every 4.5 years. Vietnam is up for review in January 2014. The organizations expressed particular concern about cyber attacks taking place against Vietnamese civil society. The statement describes how pro-government actors are targeting independent media with Denial-of Service attacks, using fake domains to mirror media sites and then infect visitors with malware, and taking over user accounts to access private information. The NGOs discusses the implications of these attacks on privacy and freedom of expression.

The Spanish Minister of Justice has [proposed revisions](#) [23] to the Criminal Procedural Code that would allow police to install malware as part of criminal investigations. The draft changes would permit “the installation of a software that allows the remote examination and without knowledge of the owner of the content in computers, electronic devices, computer systems, instruments of massive storage or databases.” Such actions would require the approval of a judge. EDRI [discussed the privacy implications](#) [24] of the proposed regulations and raised concerns about the possibility of law enforcement abusing these new powers.

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://cdt.org/blogs/emily-barabas/2706global-policy-weekly-%E2%80%93-june-25-2013>

Links:

- [1] <https://cdt.org/personnel/emily-barabas>
- [2] <https://www.cdt.org/issue/international>
- [3] http://arstechnica.com/tech-policy/2013/06/isps-to-include-porn-filters-as-standard-in-uk-by-2014/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+arstechnica%2Findex+%28Ars+Technica+-+All+content%29
- [4] <http://www.wired.co.uk/news/archive/2013-04/24/public-wifi-porn-block>
- [5] <https://www.eff.org/deeplinks/2013/06/open-wi-fi-comes-tunisia-ex-dictators-house-turned-openwi-relessorg-hotspot>
- [6] <http://observers.france24.com/content/20130624-tunisia-internet-censorship-hackers-servers>
- [7] <http://www.theatlantic.com/international/archive/2013/06/these-charts-show-how-crucial-twitter-is-for-the-turkey-protesters/276798/>
- [8] <http://www.hurriyetdailynews.com/fake-social-media-accounts-to-be-prevented-deputy-pm.aspx?pageID=238&nID=49189&NewsCatID=338>
- [9] <https://citizenlab.org>
- [10] <https://citizenlab.org/2013/06/o-pakistan>
- [11] <http://content.bytesforall.pk/node/104>
- [12] <http://en.rsf.org/bahrein-oecd-complaint-filed-by-human-24-06-2013,44797.html>
- [13] <https://www.privacyinternational.org/>
- [14] <http://www.ecchr.de/>
- [15] <http://www.bahrainrights.org/>
- [16] <http://bahrainwatch.org/>
- [17] <http://en.rsf.org/>
- [18] <https://www.accessnow.org/>
- [19] <http://www.article19.org/>
- [20] <http://www.pen-international.org/>
- [21] <http://www.englishpen.org/>
- [22] <https://www.accessnow.org/blog/2013/06/19/access-submits-upr-report-on-vietnam-cyber-attack-s-on-civil-society-a-key-c#When:19:57:17Z>
- [23] <http://www.neurope.eu/article/spanish-police-might-use-trojans-spy-computers>
- [24] <http://www.edri.org/edrigram/number11.12/spain-use--trojans-to-spy>