UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 39 – May 2014

The Blocking of Vimeo in Indonesia

Baca laporan ini dalam Bahasa Indonesia: "Pemblokiran Vimeo di Indonesia."

"Op-ed: Toward an open, free and secure Internet," written by Irene Poetranto and published in The Jakarta Post, on May 24, 2014.

INTRODUCTION

The Citizen Lab has been conducting research on Internet censorship and surveillance in Indonesia since 2010. Indonesia is a country of interest because there is an absence of standardized laws and regulations that systematically regulate content-control practices and a lack of transparency and independent oversight over the government-mandated censorship regime, which means an increased risk for infringing on fundamental rights. Indeed, the country's Ministry of Communications and Information (MICT) has been criticized for the opaque nature of its censorship regime in general, and the recent wholesale ban of video-sharing site Vimeo in particular. The practice of wholesale blocking of websites like Vimeo, a video sharing site which is known for its high-quality and high-definition videos, could do more harm than good to the economy in the long run as the country's e-commerce market is growing rapidly and an increasing number of businesses are promoting themselves online. In order for the Internet to continue to be a key enabler of economic growth, the information controls framework must be consistent, greatly simplified, and harmonized to make it less burdensome and more transparent for business.

As part of our work of monitoring developments in the country's Internet governance agenda, this report seeks to outline information controls and explain the recent blocking of Vimeo in Indonesia.

INFORMATION CONTROLS IN INDONESIA

Information controls refer to efforts to manage the content accessible to a population, including information posted online. These controls can include laws and regulations that restrict free speech online or in certain media, as well as technical measures designed to limit access to information such as Internet filtering. We employ a mixed-methods approach to the study of information controls that includes technical testing of government-mandated Internet censorship policies and practices, field research by regional and country-level experts, as well as analyzing the legal and regulatory framework governing filtering. This multidisciplinary

effort is essential for understanding both how and why information controls are applied. We also investigate the specific techniques and, where possible, the products that are used to implement Internet content filtering. Using a mixed methods approach in our research on Indonesia has yielded important insight into the scope, scale, and character of content controls.

LEGAL AND REGULATORY FRAMEWORK

Despite the guarantees freedom of expression under article 28E(3) of the Indonesian constitution, a number of laws exist which limit freedom of expression online and restrict access to content considered dangerous or socially unacceptable. The penal code and the 1965 blasphemy law which prohibits religious blasphemy are used to limit free expression. But the most prominent laws are the 2008 Electronic Information and Transaction (EIT) Law and the 2008 Anti-Pornography Law. Our blog post on Indonesian Internet infrastructure and governance as part of the "Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesia IGF" report explains the nature of these laws in greater detail. Apart from specific invocations of the law, the Indonesian government also pressures ISPs to block websites with objectionable content.

IMPLEMENTATION OF INFORMATION CONTROLS

The Internet environment in Indonesia is broadly distributed across over 300 ISPs. As a result, the scope and depth of what content is actually filtered can vary between ISPs, leaving users with different Internet experiences depending on where they connect from. Recently, there is a growing push towards standardization, if not centralization. For example, a number of national-level systems have emerged which are promoted by the MCIT that offer filtering services. ISPs are encouraged to connect to these services as a way to subcontract out the job of Internet filtering and to ensure that ISPs comply with government "rules" and expectations. Additionally, ISPs have begun to purchase commercial filtering products, for example, those made by Western companies like Netsweeper Inc. and Blue Coat Systems, whose services include categorizing and controlling access to content online, thus taking the burden of maintaining content controls away from ISP administrators.

To assist in their implementation, the MCIT is currently drafting a Ministerial Decree on the Controlling of Internet Websites with Negative Content. As these developments are ongoing, the existing decentralized nature of information controls in Indonesia could in practice become more standardized. Our blog post on analyzing content controls in Indonesia as part of the "Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesia IGF" report discusses the the country's filtering policies and practices in greater detail.

TECHNICAL ANALYSIS OF INFORMATION CONTROLS

The MCIT endorses two DNS filtering projects that include configurations and URL lists to standardize content filtering, TRUST+ Positif and DNS Nawala. Currently, the implementation of these programs is optional and Indonesian ISPs use a number of other filtering systems and techniques. As a result, there are inconsistencies regarding what content is blocked.

DNS filtering

The Indonesian private sector has tried to standardize the criteria for content to be filtered and the techniques for DNS filtering since 2008, when the Association of Indonesia's Internet Cafés (AWARI) started an initiative to implement uniform filtering across Internet cafés and provide a means for users to report sites for blocking. Prior to 2008, filtering in Internet cafés was decentralized.

These moves toward standardization were further enhanced with the development of DNS Nawala, an initiative that the MCIT started in November 2009 with the support of AWARI, PT Telkom, and Indonesian political parties in a response to pressures to implement the 2008 Anti-Pornography Law and the introduction of the "Healthy and Safe Internet" (INSAN) program.

TRUST+ Positif

TRUST+ Positif is another attempt to standardize content filtering which is maintained and endorsed by the MCIT. The system consists of a database of both blacklisted and whitelisted domains, URLs and keywords, as well as configuration information to allow administrators to implement filtering using the open-source Squid-Cache HTTP proxy/caching system and the SquidGuard add-on, which is an open source implementation of URL access control lists for Squid. The content of these lists and information about the restricted content are publicly accessible.

The TRUST+ Positif website includes a submission page that encourages users to participate in the development of URL lists (to blacklist websites for filtering or whitelist for accessibility) by forwarding pages to an e-mail address or filling in a submission form (at the time of publication, this form is described as "currently under development"). The site also contains a search form which allows searching for the presence of keywords, URLs or domains in the content database. However, how this submission process operates in practice is unclear and the MCIT ultimately decides what to block.

The blacklist database is split into 3 sub-categories: "study results" (*kajian*), "public submissions" (*pengaduan*) and "international pornography". The 'study results' database contains 1366 domains, the 'public submissions' database contains 12,643 domains and the 'international pornography' database contains 745,030 domains. As of May 25, 2014 there are no URLs in any of the three sub-category databases.

Searching the available search form for 'vimeo' shows a match with the domains list on the 'public submissions' (*pengaduan*) database:

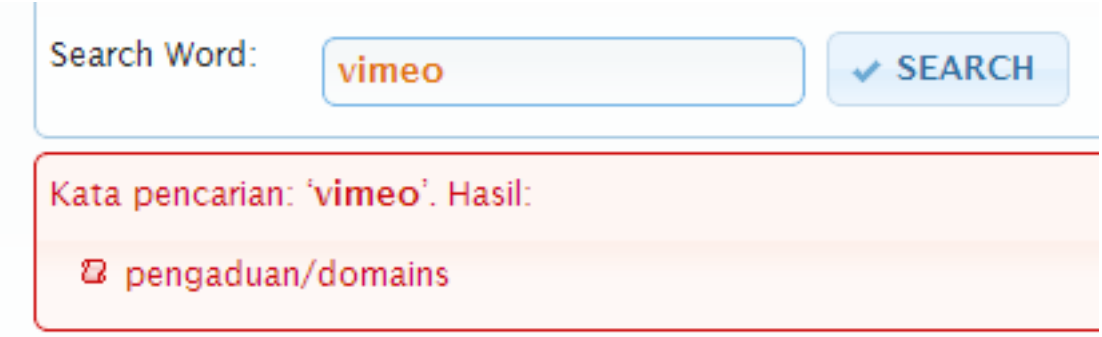

Figure 1: Search results showing Vimeo is present in TRUST+ Positif public database

Further investigation shows that 'vimeo.com' is present in this database, which as of writing is timestamped May 21, 2014.

It is unclear how domains or URLs submitted for review are vetted before being added to the submissions blacklist. It is also unclear how ISPs differ in their use of these blacklist databases, from blocking all of these sub-categories or being more selective. In addition, these databases are not free from errors and miscategorizations. Our previous research examined such miscategorizations in the TRUST+ Positif database, finding numerous examples of sites incorrectly categorized as pornography. From that small sample we found

that the websites of the government of Gibraltar and the University of Rochester library, amongst others, were incorrectly labeled as pornography. As of May 26 2014 these domains remain on the pornography blacklist.

THE BLOCKING OF VIMEO

In May 2014, Indonesian netizens took to social media to express their frustrations over the blocking of Vimeo, a video sharing site. Telkomsel's customersfirstnoticed the block, but soon two other major ISPs (Indosat and XL Axiata) reported on it, though the site remained accessible to customers of smaller ISPs. Indra Utoyo, Director of IT Solutions & Strategic Portfolio of PT Telkom (Telkomsel's operator) said on Twitter that the directive to block Vimeo was based on the instructions of TRUST+ Positif team, mailed to Indonesian ISPs on Friday, May 9, 2014, along with dozens of sexually-oriented websites that were to be blocked. However, the chairman of the Indonesian ISP Association, Semmy Pangerapan, said that the organization never received the instruction letter and that not every ISP has received it by Sunday, May 10, 2014. Adding to the confusion, the MICT through its official Twitter account denied that it had ordered to block Vimeo and attached a screenshot of the website, but the statement has since been deleted.

A number of users voiced their concerns by sending tweets directly to the Minister of Communications and Information, Tifatul Sembiring, asking for an explanation. Mr. Sembiring explained that the blocking occurred due to pornographic content on Vimeo and and therefore a notice to all ISPs and telecommunications providers was sent out, informing them that Vimeo has been included in the ministry's list of blacklisted URLs. He also mentioned that the ministry has sent a letter to Vimeo, asking them to remove the offending content. Several days later, Vimeo said through its official Twitter account that they have received the letter and, as of May 19, was looking into the request. The acting ministry spokesman Ismail Cawidu has since said that the ban is "not permanent."

Mr. Sembiring argued that the action taken by the ministry is in accordance with stipulations in Law No. 44 of 2008 on Pornography. "Pornographic content" is often used as justification for the government's decision to block specific URLs or websites, and most of these decisions are not publicly disputed. However, blocking Vimeo is controversial because not only has the website gained a reputation for its high-quality and high-definition videos, but the site also forbids users from uploading sexually explicit material or pornography. These developments are consistent with the pattern of blocking and filtering that we have seen previously in Indonesia.

In 2012, we found evidence of Internet filtering on Indosat, Telkomsel, and XL Axiata. All three ISPs filtered pornographic content and displayed block pages with varying degrees of transparency as to the reason behind the filtering. However the filtering was highly inconsistent in other respects, with Indosat and XL Axiata blocking far more content than Telkomsel did. For example, content relating to circumvention tools and free speech issues were blocked by Indosat and XL Axiata, while Telkomsel only showed evidence of blocking pornographic content.

Part of our research on the 2013 IGF includes a report on content control in Indonesia. This research compared content accessibility within the IGF venue to that elsewhere in the country. We found that the primary wireless network provided for the IGF event, which is mandated by the UN host agreement to offer unfettered access, showed no evidence of blocking. However, alternate networks that were provided within the venue by Telkomsel and Indosat, as well as a 3G network provided by Tri Indonesia tested from elsewhere in Bali, had evidence of filtering.

TESTING RESULTS

Following reports of Vimeo's blocking, we conducted client-based network measurement tests from within Indonesia. Data was collected by performing synchronized HTTP requests from within Indonesia and from a lab location (at the University of Toronto) using customized measurement software written in Python in a client-server model. The lab network acts as a control and is located at a site that does not censor the type of content tested by the measurement software.

During tests the client attempts to access a pre-defined list of URLs simultaneously in the Indonesia (the "field") and in a control network (the "lab"). Tests were conducted on URL lists that consisted of locally sensitive URLs that are specific to Indonesia's social, political, and cultural context, including content from Vimeo.

A number of data points are collected for each URL access attempt: HTTP headers and status code, IP address, page body, traceroutes and packet captures. A combined process of automated and manual analysis attempts to identify differences in the results returned between the field and the lab to isolate instances of filtering. Because attempts to access websites from different geographic locations can return different data points for innocuous reasons (such as a domain resolving to different IP addresses for load balancing, or displaying content in different languages depending on where a request originates from) a manual inspection of results is often necessary to verify whether inaccessibility is caused by deliberate filtering or mundane network errors

Tests were conducted on the ISP Telkom Indonesia from May 13 to May 20, 2014. A total of 191 unique URLs were tested during this period, with each URL tested 10 times. A total of 86 of the 191 URLs were found to be blocked during at least one test. Attempts to access these 86 URLs saw the DNS lookup resolve to an incorrect IP (118.98.97.100) which redirected towards http://internet-positif.org/site.block?d=STRING, where STRING is a base64 encoding of the blocked domain. The IP (118.98.97.100) is hosted by Telkom Indonesia and hosts the Internet Positif blockpage:

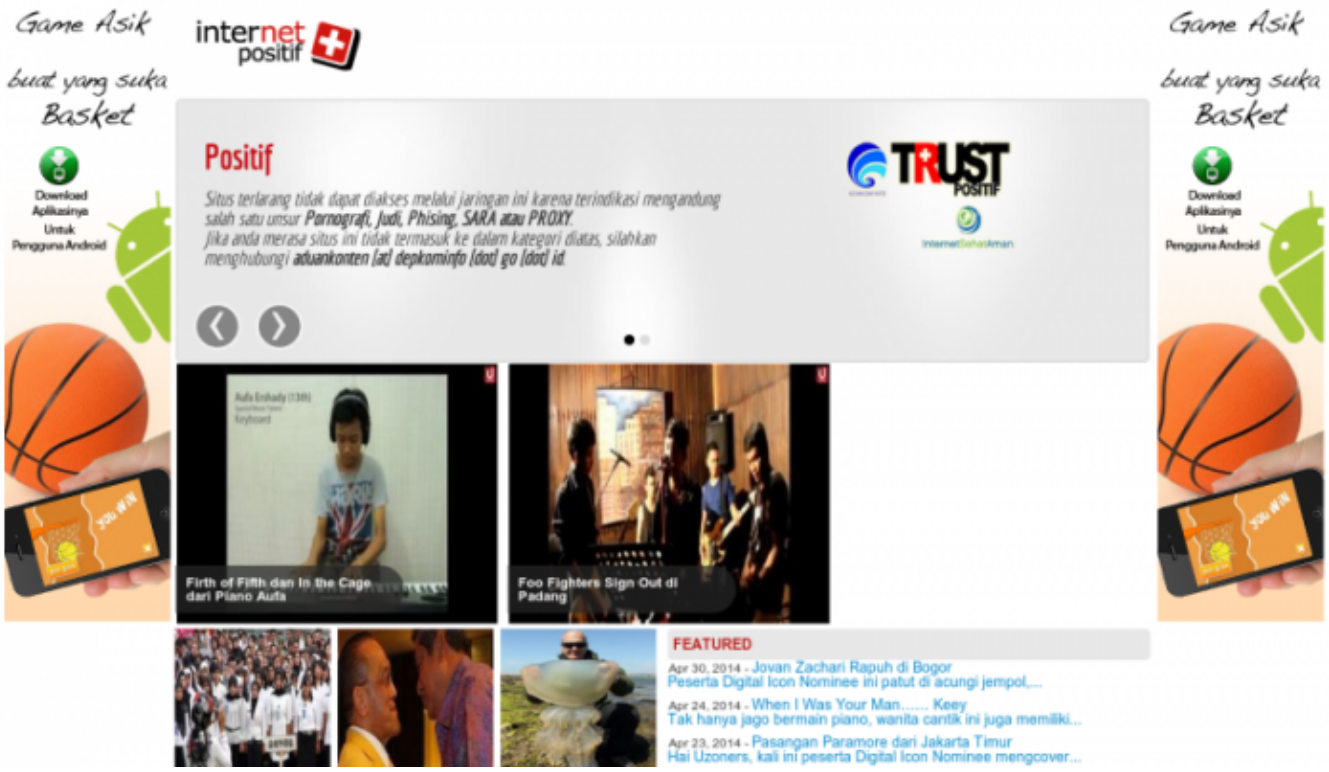

Figure 2: The TRUST+ Positifblockpage found at 118.98.97.100

From this sample of 86 URLs found blocked, the most commonly blocked content categories were pornography, gambling and proxy/circumvention tools. Links to the full list of URLs found blocked can be found in the Data section below.

During the 10 tests run between May 13 and 20, there were 2 tests in which no blocking was documented. During these tests, DNS resolution occurred normally and all content tested was accessible. It is not clear if this intermittent accessibility of otherwise blocked content was the result of a misconfiguration of the censorship infrastructure or an issue with the testing setup. The earliest and most recent tests both showed evidence of filtering, so these two tests appear to be anomalies.

We tested a sample of 12 Vimeo URLs, including specific channels and groups identified by an MICT press release as containing pornographic content. All 12 Vimeo URLs tested were found to be blocked during at least one test, although this was also intermittent, with some Vimeo URLs blocked on some tests but not others. The only exception we found was the HTTPS version of Vimeo (https://vimeo.com) — although it did incorrectly resolve to the IP 118.98.97.100 (like other blocked content), tests of this URL were never redirected to the TRUST+ Positif website. Instead, the initial HTTPS connection was rejected. This may be the case with all HTTPS versions of blocked URLs, however we do not have sufficient data to confirm this.

SUMMARY AND LOOKING AHEAD

Understanding information controls without considering the broader social, political, and legal context and the ICT environment within which they are embedded is essentially impossible. This difficulty is due to the nature and character of information controls largely depend on a variety of factors: the market structure of ISPs and telecommunication companies; the informal relations and practices among stakeholders, especially a diverse

and politically active civil society; and the legal and policy structures which frame them all. The blocking of Vimeo is but one example illustrating the challenges in Indonesia's existing information control regime.

The most prominent laws used to justify content controls in Indonesia are the 2008 Electronic Information and Transaction (EIT) law and the 2008 Anti-Pornography law. These laws, however, have been controversial. Article 27(2) of the EIT law, which covers defamation, is of particular concern. Gatot S. Dewa Broto, the spokesperson for the MCIT, has acknowledged that many have judged the penalty of up to six years' imprisonment and fines of up to IDR 1 billion (approximately USD 106,000) as being too harsh, especially because it is more severe than the provisions contained in the Penal Code, which specifies a penalty of up to nine months' imprisonment. Despite calls to revise the EIT Law, the MCIT has yet to produce a revised draft to submit to parliament.

The Anti-Pornography Law has been criticized because the definition of pornography under the law is considered to be too broad and has been opposed by minority groups who argue it runs counter to Indonesia's tradition of diversity and pluralism. Enforcing content controls using the EIT law and Anti-Pornography law is also problematic because to this day the government has yet to issue a Government Regulation (Peraturan Pemerintah) to operationalize the laws. Our previous blog post on content control in Indonesia elaborates on how these laws, in conjunction with other laws, such as those which prohibit blasphemy or "defamation of religions," are used for content regulation.

The MCIT's latest effort in standardizing content regulation is the drafting of a Ministerial Decree on the Controlling of Internet Websites with Negative Content. However this draft has also been criticized for its vague and overly broad provisions which allow authorities to criminalize free expression. The absence of laws and regulations that systematically regulate and narrowly define content-control practices mean that the authorities are at liberty to enforce them through their own interpretations of legislations and that ISPs may implement their own filtering devices and practices.

The sheer number of Indonesian ISPs and the decentralized nature of Indonesian Internet infrastructure also make uniform content control practices challenging. With regard to the recent blocking of Vimeo, for example, the MICT-issued directive to block the website did not reach all ISPs at the same time, and neither did it reach the Indonesian ISP Association (Asosiasi Penyedia Jasa Internet (APJII)). As a result, there was confusion as to why the website was accessible on some ISPs, but not others. This incident led to APJII's chairman, Semmy Pangerapan, calling out the Minister of ICT as "arrogant" for the ministry's unilateral decision to block Vimeo in a wholesale manner, as opposed to blocking specific accounts or URLs with objectionable content, without consulting other stakeholders. Due to this controversial decision, Mr. Pangerapan suggested that a content advisory board, which consists of government, civil society, and private sector, should be established, to avoid the consequences of having a concentration of power within one institution.

TRUST+ Positif's reliance on lists of blacklisted URLs is also problematic. Our research into the list of URLs labelled as "porn" — it is publicly available on TRUST+ Positif's website — has found that there are numerous URL miscategorizations that result in erroneous blocking. Our 2013 content control in Indonesia study found that the UK government's website on Gibraltar, as well as the University of Rochester's library's website are on the TRUST+ Positif blacklist and are thus blocked. These examples illustrate a key issue with blacklist-based filtering methods – the difficulty in accurately identifying and targeting content for blocking without errantly blocking unrelated content. Many blacklists are generated through a combination of manually and automated searches, and thus, they often contain websites that have been incorrectly classified. In addition, blunt filtering methods such as IP blocking can knock out large swaths of unrelated websites simply because they are hosted on the same IP address as a site with restricted content.

The Internet expands access to information beyond traditional media. This feature is perceived by many as important in Indonesia, where there is the concentration of media ownership in the hands of a small number of individuals. Twelve large conglomerates control nearly all of the country's media channels, including broadcast, print, and online media, and therefore there are concerns that this "conglomeration" may affect the media's independence.

During the leadup to the July 2014 general elections, the Internet has provided a platform for social mobilization and civic action. Jakarta is said to be the most active Twitter city in the world and Indonesia has the fourth largest number of Facebook users. Indonesian netizens use these social networking sites to communicate directly with political parties' candidates and discuss them amongst each other, while Indonesian political parties have been quick to adopt these communications platforms to market their candidates and policies.

The public uproar that ensued following the blocking of Vimeo has shown that Indonesian netizens are increasingly more aware not only of the value of the Internet as a tool to promote growth and development, but also their right to access, receive and impart information and ideas. The MICT has since backpedalled by saying that the ban is "not permanent," and that it is merely "waiting to see a minimum effort to remove the pornographic content." Considering Vimeo's response that it "will not change its policies or censor any content in response to Indonesia's decision to ban," it is not yet clear how this situation will be resolved. This incident has shown that more than just a source of information, the Internet also plays an important role in facilitating citizen participation and engagement, and therefore must be kept open and accessible.

DATA

A full list of URLs tested and those identified as blocked can be found here.