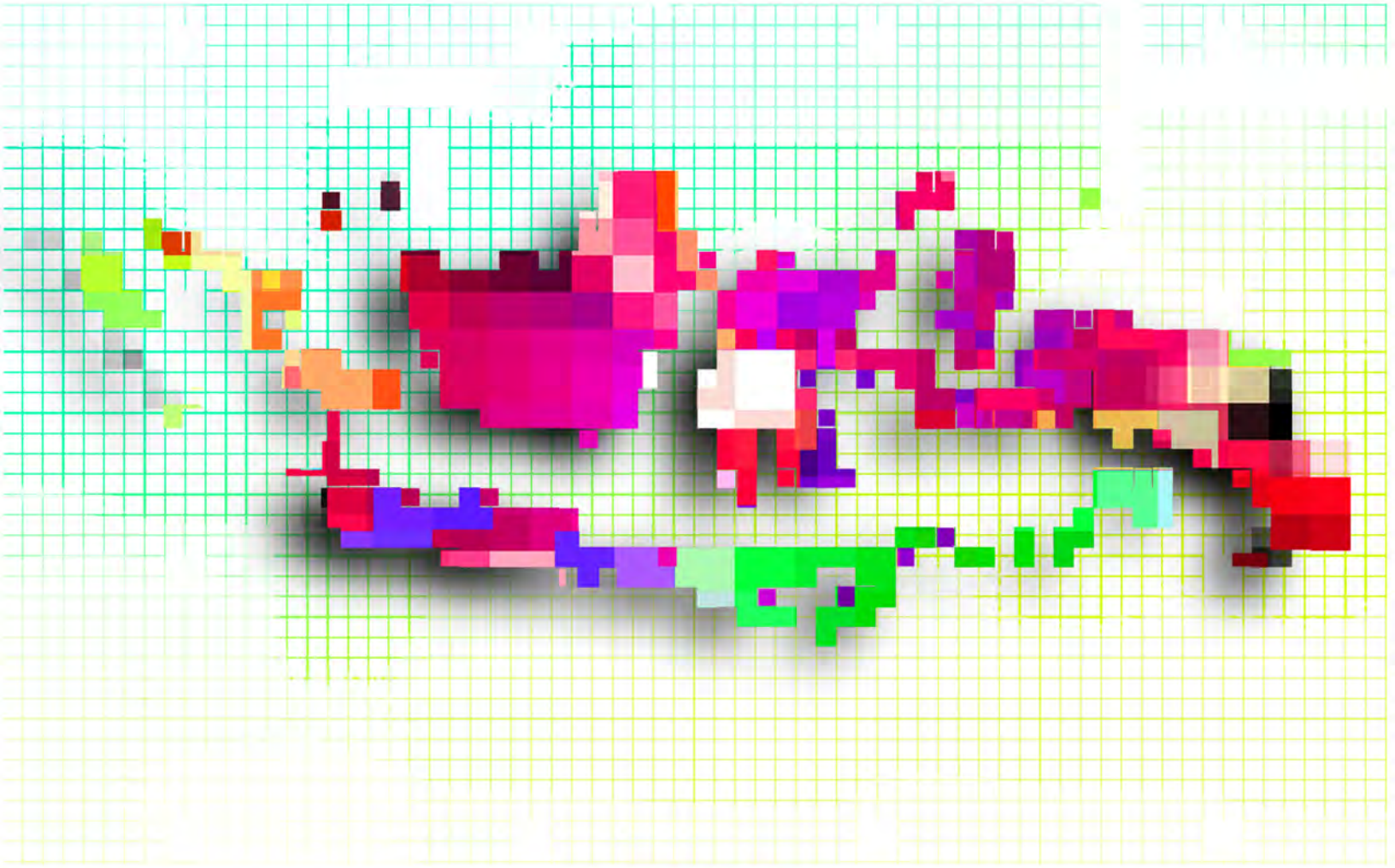
ISLANDS OF CONTROL, ISLANDS OF RESISTANCE:
MONITORING THE 2013 INDONESIAN IGF



NUMBER 29

JANUARY 20, 2014

CITIZEN LAB AND CANADA CENTRE FOR GLOBAL SECURITY STUDIES
MUNK SCHOOL OF GLOBAL AFFAIRS, UNIVERSITY OF TORONTO

UNIVERSITY OF TORONTO
MUNK SCHOOL OF GLOBAL AFFAIRS
Canada Centre for Global Security Studies

FOREWORD

Those who might wonder about the future of the Internet need look no further than Indonesia. Like many countries in the global South, Indonesia has swiftly entered into the universe of global digital communications. The nation's capital, Jakarta, is said to be the most active Twitter city in the world, and Indonesia now has the fourth largest number of Facebook users. From a baseline of almost zero only a decade ago, Indonesians are connecting at a rate of roughly 800,000 users every month. As is so often the case today among newly-connected countries, the primary means of communicating online in Indonesia is mobile devices—many Indonesians carry two of them—making the country's citizens highly wired and fully engaged.

But like many other countries in the global South, Indonesia has more than its share of governance challenges. As the world's largest majority Muslim country, concerns about religious and social issues are always percolating at the policy level, and spill over into Internet governance discussions. The archipelago continues to be strained by regional schisms and barely-contained insurgencies that occasionally burst out. Bombings in Bali in 2002 and 2005 remain imprinted on many minds and colour the Indonesian security landscape. Although Indonesia's three decade period of dictatorship has now passed, the country's democratic institutions are still nascent and there are many issues to resolve, including holding accountable the armed forces for past atrocities.

This report, *Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesian IGF*, is the first in a series of Citizen Lab reports that apply a mixture of methods, from technical interrogation to field research and social and legal analyses, to study information controls in and around particular events. Our interest in event-based monitoring of information controls is an evolution in the Citizen Lab's approach to research of cyberspace and global politics. During the period of our involvement in the OpenNet Initiative,[1] the approach of that project was to undertake country-by-country comparative studies with little consideration given to timing apart from the availability of researchers inside the country. Meanwhile, we noticed, the most interesting dynamics around information controls were happening "in time" and around political events such as elections, anniversaries, global conferences, and sporting events. It is during political events that information has its greatest value and power, and is most highly contested. Moreover, events are episodes that mark turning points, perhaps creating a plateau of standards and regulations to follow, a kind of punctuated equilibrium of practices that become normalized after the event is over. For those reasons, Citizen Lab has embarked on a new project

1 The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet and Society at Harvard University; and the SecDev Group (Ottawa).

examining event-based monitoring of information controls, of which this report is the first.

The Citizen Lab chose to focus on information controls in and around Indonesia's hosting of the United Nations Internet Governance Forum (IGF), running from 20 October to 25 October 2013. While Citizen Lab researchers, staff, and associates have had many memorable IGF and World Summit on the Information Society (WSIS) experiences, including having book launches and other presentations disrupted by host government and IGF official security, our participation in the Indonesian IGF proceeded without interference. Unlike prior IGFs, we also came properly equipped not just to attend and present, but also to undertake applied research during the course of the event. We worked closely with Indonesian civil society partners for many months leading up to the IGF, which gave us unique insight into the political processes surrounding the planning and preparation. With the help of the same Indonesian partners, some of whom wish to remain nameless, we undertook in-country and remote network measurements aiming to document Internet content filtering and surveillance practices, and interviewed officials attending the IGF. Independent researcher Collin Anderson contributed data from OONI probe tests[2] he undertook during the IGF. Parts of this report were written *in situ*, some of us working from the IGF conference venue or from the conference hotel, while other Citizen Lab staff and researchers in Toronto undertook technical analysis and contextual research. Our preliminary findings were presented at a press conference and a panel session at the IGF. The final section of the report was written after the IGF had wrapped up, and provides a series of reflections on the overall process.

Islands of Control, Islands of Resistance was researched and written in a collaborative fashion, by the Citizen Lab's (in alphabetical order) Matt Carrieri, Masashi Crete-Nishihata, Jakub Dalek, Ron Deibert, Bennett Haselton, Saad Khan, Marianne Lau, Helmi Noman, Irene Poetranto, Adam Senft, and Greg Wiseman. Prior research of the Citizen Lab's Morgan Marquis-Boire, Bill Marczak, and John Scott-Railton also informed the report. The Citizen Lab's Irene Poetranto translated this report into Bahasa Indonesian. Special thanks to Collin Anderson, Harijanto Pribadi (Department Head of Indonesia Internet Exchange, Indonesia Internet Service Provider Association), Professor Sinta Dewi Rosadi (Faculty of Law, Padjadjaran University, Bandung, Indonesia), and several Indonesian civil society partners who contributed to the report but wish to remain anonymous.

Ron Deibert
Director, Canada Centre for Global Security Studies and the Citizen Lab
Munk School of Global Affairs, University of Toronto

2 OONI-probe is a client based Internet censorship measurement tool developed by the Tor project.

TABLE OF CONTENTS

INTRODUCTION

Between 22 and 25 October 2013, Indonesia hosted the eighth annual Internet Governance Forum (IGF), a multistakeholder dialogue on the issues and policies of Internet governance. The main theme of the 2013 IGF was "Building Bridges: Enhancing Multistakeholder Cooperation for Growth and Sustainable Development."

This report explores online freedom of expression and the state of information controls in Indonesia in the context of its role as host of the IGF, comparing Indonesia's information controls with similar practices in the region, the rest of the world, and in events similar to the IGF. We also analyze how these practices are driven by Indonesia's social, political, and cultural context, and the role that international norms play in influencing information controls.

Major global events are frequently a focal point for the exercise of and contests over information control, including Internet censorship and surveillance, disruptions to mobile and other communications systems, and tampering with Internet connectivity. Such information controls are often highly dynamic, responding to the changing situation on the ground when information can have the greatest impact. We call such practices "just-in-time" information controls—denying, disrupting, manipulating, or monitoring access to information during important political moments.[3] High-profile global events can have significant political, social, and economic consequences for host countries, and may come with new security and surveillance measures as a result.[4]

Several Citizen Lab researchers and associates who attended the IGF participated in the research for this report, including those who have been situated in Indonesia for some time as part of the civil society stakeholder preparations for the 2013 IGF. Additionally, we capitalized on the expertise and input of Indonesian colleagues, including those who are part of the

3 For more background on "just-in-time" content controls, see Masashi Crete-Nishihata and Jillian C. York, "Egypt's Internet Blackout: Extreme Example of Just-in-Time Blocking," OpenNet Initiative, 28 January 2011, https://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking; and Ronald Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, eds. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-6.pdf.

4 Russia's Surveillance State, a joint project between Citizen Lab, Agentura.Ru, and Privacy International, has documented the growth of surveillance measures in preparation for the 2014 Sochi Winter Olympics. See Irina Borogan and Andrei Soldatov, "Surveillance at the Sochi Olympics 2014," Agentura.ru, October 2013, http://www.agentura.ru/english/projects/Project_ID/sochi.

Cyber Stewards Network,[5] to provide much-needed context and nuance around the analysis presented here. Citizen Lab staff working remotely provided input into and support for network measurement and legal and policy analysis.

We frame our analysis with the following topics and questions:

INFRASTRUCTURE AND GOVERNANCE

The application of information controls in a country is highly influenced by the domestic political, economic, and social context in which they are applied. Each country's communication infrastructure is unique, differentiated by factors such as the number of Internet service providers (ISPs), telecommunication companies, the degree of market competition among them, and the overall level of Internet penetration and growth. In some countries numerous ISPs and a highly competitive market environment can act as a constraint on state-driven information controls, whereas in other countries with fewer ISPs and less democratic regimes, state regulations can be more centrally implemented and sometimes more constraining. International connectivity and upstream arrangements with peers can also shape the nature of information controls, as do regional and international governance regimes of which the country may be a member. Most importantly, the regime type of the country in question can have a major influence over the nature of information controls.

The Indonesian government has traditionally been supportive of ICT development. Internet penetration has increased since the beginning of the century, from less than 1 percent in 2000 to 15.36 percent in 2012. Cellular phone penetration has increased at an exponential rate over the same time period, from 1.72 to 115.20 cellular phone subscriptions per 100 inhabitants. The government is planning to increase basic telephone services to thousands of villages across the country and is trying to increase Internet penetration to the country's easternmost islands.

Indonesia has over 250 ISPs. The two largest telecommunications operators, PT Telekom and PT Indosat, were partially privatized in the mid-1990s after years of state control, although the government continues to own shares in both companies. As ICT penetration in Indonesia has increased, so have the regulations and laws, some having the perceived necessities of dealing with growing cybercrime issues as their impetus while others have to do with content controls. ISPs and telecommunications companies have voiced their concerns that these laws lack clarity and may place burdens on their services.[6]

5 The Cyber Stewards program is a global network of organizations and individuals that use evidence-based research for policy advocacy to ensure and promote a secure and open Internet. We are building bridges between researchers and activists in the Global North and South to form a space of peers for collaboration and organization at local, regional, and international levels.

6 Mariel Grazella, "ICT Businesses to Tackle Policy at Global Internet Forum," *The Jakarta Post*, 2 March 2013, available at http://www.thejakartapost.com/news/2013/03/02/ict-businesses-tackle-policy-global-forum-bali.html.

This section examines the following questions:

- How is cyberspace constituted in Indonesia?
- What is the political economy of Internet governance and use in the country?
- How are laws and regulations over the Internet implemented?
- What autonomy do ISPs have to implement laws and rules, and what practices inform implementation of controls in Indonesia? How do these practices compare to other countries?
- Is the Indonesian government developing a cybersecurity strategy? What policies does it include, and how will these affect information controls? How have issues of cybercrime been perceived in Indonesia and what have been the institutional and legal responses?
- Does the Indonesian government have a "regional" or "foreign policy" for cyberspace?

CONTENT CONTROLS

Information controls involve control over what content is accessible to a population, including information posted online. Content 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–otherwise known as "Internet filtering." Since 2003, the Citizen Lab, as a founding member of the OpenNet Initiative,[7] has tested Internet filtering in seventy-four countries, and found that forty-two of these seventy-four countries engage in some form of content filtering. The type of content being filtered varies across countries, and depends on local political, legal, social, and cultural contexts. We employ a multidisciplinary approach that includes technical testing of government-mandated Internet censorship policies and practices, field research by regional and country-level experts, as well as analysis of the country's legal and regulatory filtering framework. The combination of technical investigation with political, social, and legal contextual work is essential for understanding both how and why information controls are applied.[8] We also aim to determine the specific techniques and, where possible, which products are used to implement Internet content filtering.

OpenNet Initiative testing in 2010 on four Indonesian ISPs found that pornographic content, which is illegal under the country's 2008 Anti-Pornography Law, is heavily filtered. Testing also revealed that Internet filtering across ISPs is unsystematic and inconsistent, with some ISPs blocking more than others and targeting a wider range of content such as anonymizer and circumvention websites, and websites containing controversial political or religious content. In 2011, smartphone maker BlackBerry began censoring pornographic content on their networks

7 The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet and Society at Harvard University; and the SecDev Group (Ottawa).

8 See Masashi Crete-Nishihata, Ronald J. Deibert, and Adam Senft, "Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls," *IEEE Internet Computing* 17, no. 3 (2013): 34-41.

in the country following demands by the Indonesian government.

Our research on content controls is guided by the following questions:

- What content controls are applied in Indonesia?
- How are those content controls implemented or carried out?
- What do network measurements of Internet accessibility reveal about the scope, scale, and character of information controls in Indonesia?
- What restrictions are placed on free expression, both off and online, in Indonesia?
- What steps have civil society groups taken in response?
- What Internet users, if any, have been targeted for arrest and on what grounds?

SURVEILLANCE AND CONTROL

Surveillance is one of the most effective, if less obvious, forms of information control. Governments and private companies engage in surveillance for a wide range of reasons, many of them beneficial for society. For example, surveillance is an essential component of government responses to health crises and natural emergencies, and is a critical component of effective large-scale network management and law enforcement. However, surveillance can also be used to target dissidents and undermine privacy. If surveillance is undertaken without proper accountability, it can lead to the abuse of power. Surveillance of the Internet and other communications is now a huge growth industry, with many companies supplying governments with passive and targeted surveillance products and services.

Past Citizen Lab research has documented the use of surveillance technologies, products, and services in Indonesia. For example, command-and-control servers for the commercial malware product FinFisher were identified on the Indonesian ISPs PT Telkom, PT Matrixnet Global, and Biznet, as were devices that can be used for filtering and surveillance which were manufactured by the US-headquartered Blue Coat Systems. Indonesia's Ministry of Defence recently signed a USD 6.7 million contract with Gamma TSE to provide undisclosed "wiretapping equipment" for use by the ministry's Strategic Intelligence Agency. Gamma TSE is part of the Gamma Group, which includes Gamma Group International, the developer of FinFisher, a "lawful interception" product. Smartphone maker BlackBerry has come under pressure from Indonesian authorities to locate infrastructure within the country as a means of facilitating surveillance of users, although it is not clear what, if any, arrangements have been made between the company and the Indonesian government.

Our research on surveillance and control is guided by the following questions:

- What type of surveillance is undertaken by Indonesian authorities?
- What oversight and accountability is associated with that monitoring?
- What range of equipment, products, services, etc., does Indonesia use to implement surveillance? And how is that surveillance targeted?
- Were any special security and surveillance measures put in place for the IGF? And if so, what type of surveillance, and for what purpose?

IGF CONTROLS

Major global events like the IGF are often a significant focus of international attention and can have important political, economic, and social consequences for host countries. Information controls are customarily loosened during the hosting of the IGF event – particularly at the venue itself. The 2005 World Summit on the Information Society (WSIS) in Tunis, for example, provided unfettered access within the conference venue, while filtering remained in place elsewhere in the country.

Citizen Lab staff and associates have participated in every IGF since the first meeting was held in Athens in 2006 (as well as the WSIS meetings that preceded it in 2003 and 2005). At the 2005 WSIS meeting in Tunis, Citizen Lab researcher Nart Villeneuve's presentation on Internet filtering was disrupted by Tunisian authorities and nearly cancelled. Our participation in the 2009 IGF in Egypt included having our book launch for the OpenNet Initiative's *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* disrupted by United Nations' officials, following complaints by Chinese government representatives concerning our reference to Tibet and the Great Firewall of China in our published material.

This section focuses on the dynamics surrounding the IGF itself:

- What were the interests of the various Indonesian stakeholders (government, private sector, civil society) in hosting the IGF? What did different stakeholders hope to accomplish? Where did these interests clash? What value does the Indonesian government place in the IGF relative to other international forums, such as ICANN, the ITU, or non-cyberspace-related forums like APEC and ASEAN?
- To what extent were Indonesian stakeholders able to influence and shape the agenda and outcomes of the IGF? How did they prepare for the meeting, and what were the obstacles to overcome in making it happen (e.g., budgetary issues)?
- What impact did the forum have, if any, on Indonesian information controls and related practices?
- How did Internet accessibility in the forum's venue, or in any other area where attendees

congregated (i.e., hotels, Internet cafés, etc.), compare to what the average Indonesian user experiences?

- How did stakeholders in Indonesia organize themselves to host the IGF?
- What were the political dynamics of the IGF meeting itself?
- What were the processes to develop the agenda and program for the meeting–e.g., how did the multistakeholder advisory committee develop the key topics, agenda, and structures of the IGF? Which stakeholders held which positions, and who had input?
- What were the outcomes?

AN OVERVIEW OF INDONESIAN INTERNET INFRASTRUCTURE AND GOVERNANCE

Indonesia, an archipelagic country with a population of over 240 million people, is involved in many regional and international debates on integrating information and communication technology (ICT) in national development. As the largest economy in Southeast Asia, the country's steps toward ICT development and regulation will have a significant influence on the trajectory of similar efforts in other countries within the region. This section seeks to map out the infrastructure and governance of ICTs in the country, and explores the trends and challenges regarding the right to freedom of expression and access to information that are grounded in the universal human rights framework.

Internet penetration in Indonesia has increased since the beginning of the century from less than 1 percent in 2000 to just over 15 percent in 2011 (or roughly 45 million people). At the end of 2012, that figure was 10 million more, or equivalent to an increase of over 800,000 users every month. A predicted 80 million Indonesian users will be online by the end of 2013. This means that Internet penetration will grow to 33.3 percent. The value of the Internet in Indonesia, as calculated from the amount it will deliver to the gross domestic product (GDP), according to Deloitte Access Economics, is at 1.6 percent of GDP, bigger than liquefied natural gas exports, and it is growing rapidly. Deloitte Access Economics expects it to grow at three times the pace of the economy, from 1.6 percent of GDP in 2010 to at least 2.5 percent of GDP over the next five years.

Cellular phone penetration has increased at an exponential rate over the same period, from 1.72 to 115.20 cellular phone subscriptions per 100 inhabitants (See Figure 1). A 2011 market report found that 48 percent of users connect to the Internet through mobile devices. Mobile phone subscription in Indonesia reached 290 million in 2012 because people frequently carry two or more devices. The Indonesian government aims to push mobile broadband penetration to 22 percent in 2013, higher than the 8 percent penetration target for fixed broadband.

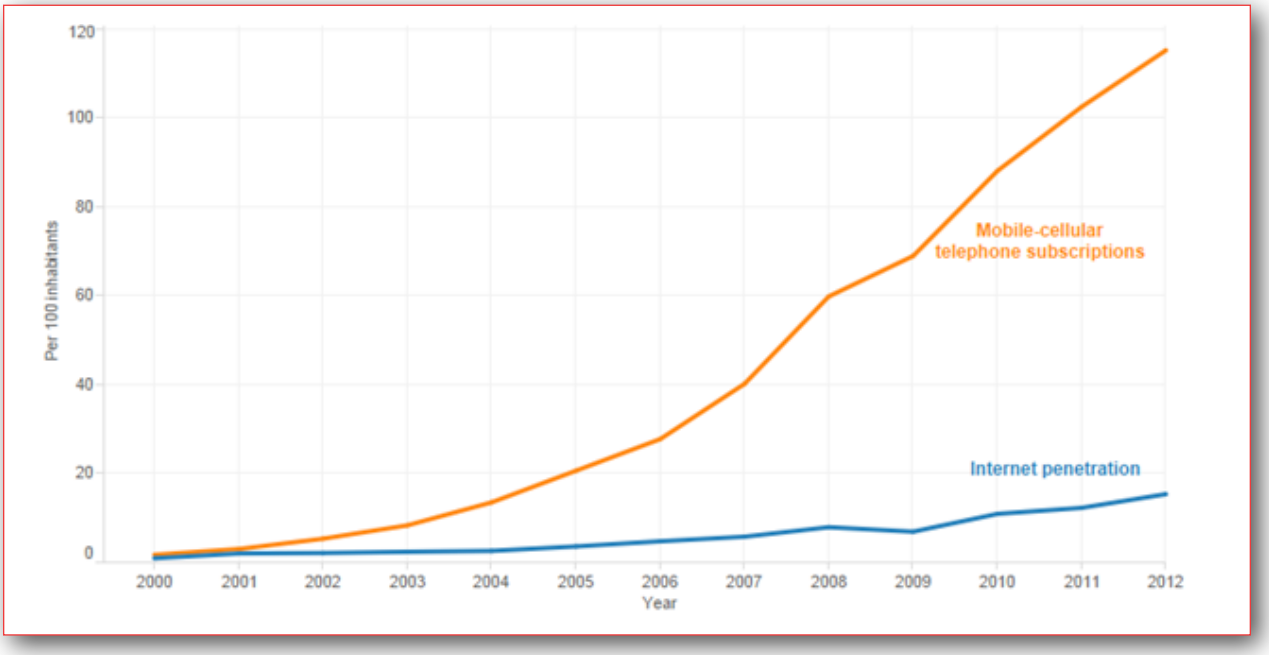


FIGURE 1: Indonesian Internet penetration and mobile subscriptions per 100 inhabitants.

Indonesia has over three hundred Internet service providers (ISPs), thirty-five of which own network infrastructure. PT Telkom is Indonesia's largest telecommunications company, with 8.6 million fixed-wire-line customers, 14.2 million fixed-wireless customers, and 107 million cellular customers as of December 2012. PT Indosat is Indonesia's second-largest cellular operator, with more than 55 million cellular subscribers. Both PT Telkom and PT Indosat were partially privatized in the mid-1990s. The government retains shares in both companies, including over 50 percent ownership in the case of PT Telkom.

In contrast to the agglomeration of ISPs, the growth of Indonesia's media industry has led to a media oligopoly and the concentration of ownership in the hands of a small number of corporations. Twelve large conglomerates control nearly all of the country's media channels, including broadcast, print, and online media. For instance, Berita Satu Media Holding, a new media company under the Lippo Group, has established an Internet-Protocol Television (IPTV) BeritasatuTV, online media channel www.beritasatu.com, and also owns a number of newspapers and magazines. A number of these media groups are owned by individuals involved in politics. For example, Aburizal Bakrie is both the chairman of Golkar, one of the country's biggest political parties, and owner of Visi Media Asia (also known as VIVA), which owns TV stations such as ANTV, tvOne, Vivasky, and Sport One, as well as the online news website VIVA.co.id. Surya Paloh, the founder of a new political party, Nasional Demokrat (NasDem), is the owner of Media Group, which operates the MetroTV station and publishes

the newspapers *Media Indonesia*, *Lampung Post*, and *Borneonews*, as well as the tabloid, *Prioritas*. Such monopoly in the media is made possible by the 2002 Broadcasting Law (Undang-undang Penyiaran), which sets vague limitations on private broadcasting ownership (and, as we will explain, the People's Representative Council and the Indonesian government are currently drafting a revision to the Broadcasting Law). Ahead of the 2014 general elections, there are concerns that this "conglomeration" may affect the media's independence.

The Ministry of Communication and Information Technology, recognizing the importance of high-speed Internet to economic and social development, launched the Indonesia Connected program to boost connectivity in border and remote areas. The fiber-optic Palapa Ring network is being implemented throughout Indonesia to accommodate this growth. The ministry estimates that construction of the Internet backbone has reached 80 percent, covering Nangroe Aceh Darussalam (Sumatera) Ring, Java-Kalimantan-Sulawesi-Denpasar-Mataram Ring, and Mataram-Kupang Ring. Several companies are involved in this project, including PT Telkom and PT Indosat. Recently, Lippo Group announced that it is partnering with JSAT, Japan's largest telecommunications company, to increase Internet connectivity in Papua, specifically through the installation of VSAT (very small aperture terminal). The stretch from Manado (Sulawesi) to Papua (5,194 kilometres) will be connected to the fiber-optic network when the project is completed.

The Palapa Ring project contains 35,280 kilometres of undersea cable. Many of these cables connect to Singapore (see Figure 2), which sits at the crossroads between Asia Pacific and Europe and serves as a major hub for submarine cables used for Internet and telecommunications infrastructures. Citizen Lab's partner organization, Privacy International, has conducted research on surveillance technology providers, whose systems include subsea cable-tapping technology. According to the *Sydney Morning Herald* (SMH), information disclosed by US whistleblower Edward Snowden revealed that the British Government Communications Headquarters (GCHQ) collects all data transmitted to and from the United Kingdom and Northern Europe via one of Indonesia's submarine cables, the SEA-ME-WE-3, which is the longest optical submarine cable in the world with landing points in Medan and Jakarta, Indonesia. Australian intelligence sources also told Fairfax Media, which owns the SMH, that Singaporean intelligence cooperates with Australia in accessing and sharing communications carried by the cable.

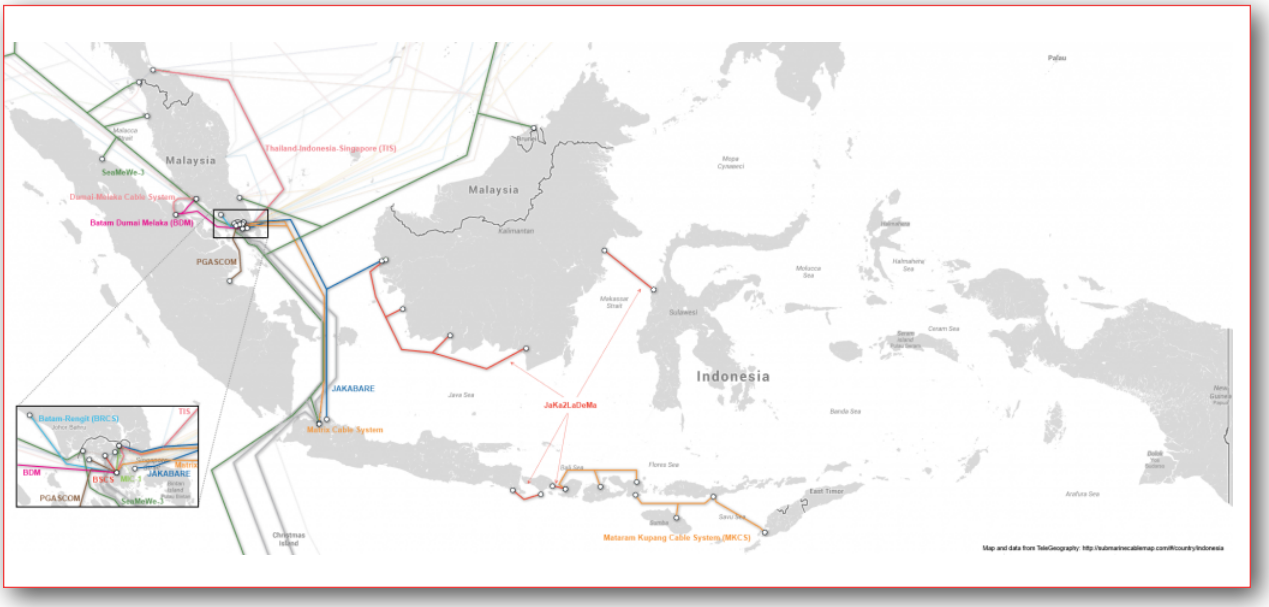


FIGURE 2: Currently active Indonesia-connected submarine cables (international and domestic) (Source / interactive version: http://submarinecablemap.com/#/country/indonesia).

Indonesia does not have a centralized Internet infrastructure and has several links to overseas networks. The Indonesia Internet Exchange (IIX), the country's first Internet exchange point (IXP), is maintained by the Association of Indonesian Internet Service Providers (APJII) (See Figure 3). The country's second IXP, OpenIXP, is operated by the Indonesia Data Center (IDC). Indonesian government regulation mandates that ISPs must subscribe their IP transit from the network access provider (NAP) as global upstream. The IXPs, therefore, serve only local/ domestic function between Indonesian ISPs.[9]

9 PowerPoint presentation by Harijanto Pribadi, Department Head of IIX APJII, https://citizenlab.org/wp-content/uploads/2013/10/IIX-APJII2012-APNIC34-Final.pptx.

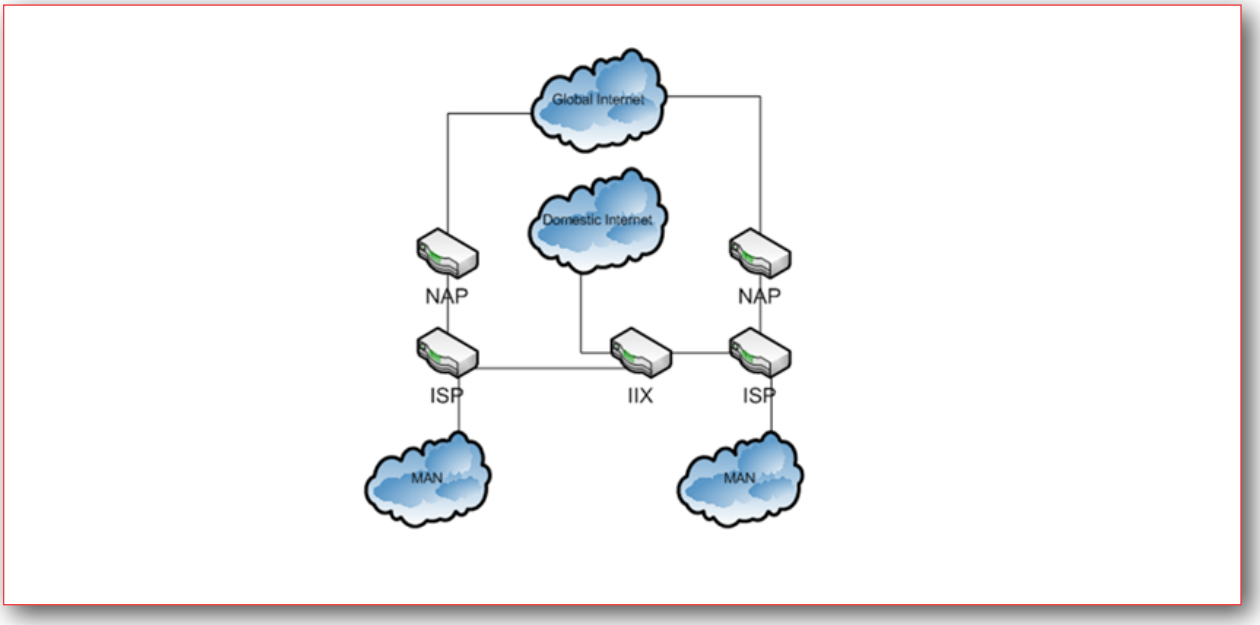


FIGURE 3: The schema of the Indonesian Internet Industry according to IIX.

Figure 4 shows various Indonesian, as well as foreign, Autonomous Systems (ASes): networks that are under the administration of a particular entity or authority. The middle layer of nodes in the diagram (with both names and numbers) represents Indonesian networks that have upstream connectivity to foreign networks. The variety of networks and number of links to these foreign networks indicates a lack of centralization. This dispersed decentralized network may be what caused Renesys, an Internet intelligence provider, to classify Indonesia in 2012 as "likely to be extremely resilient to Internet disconnection."

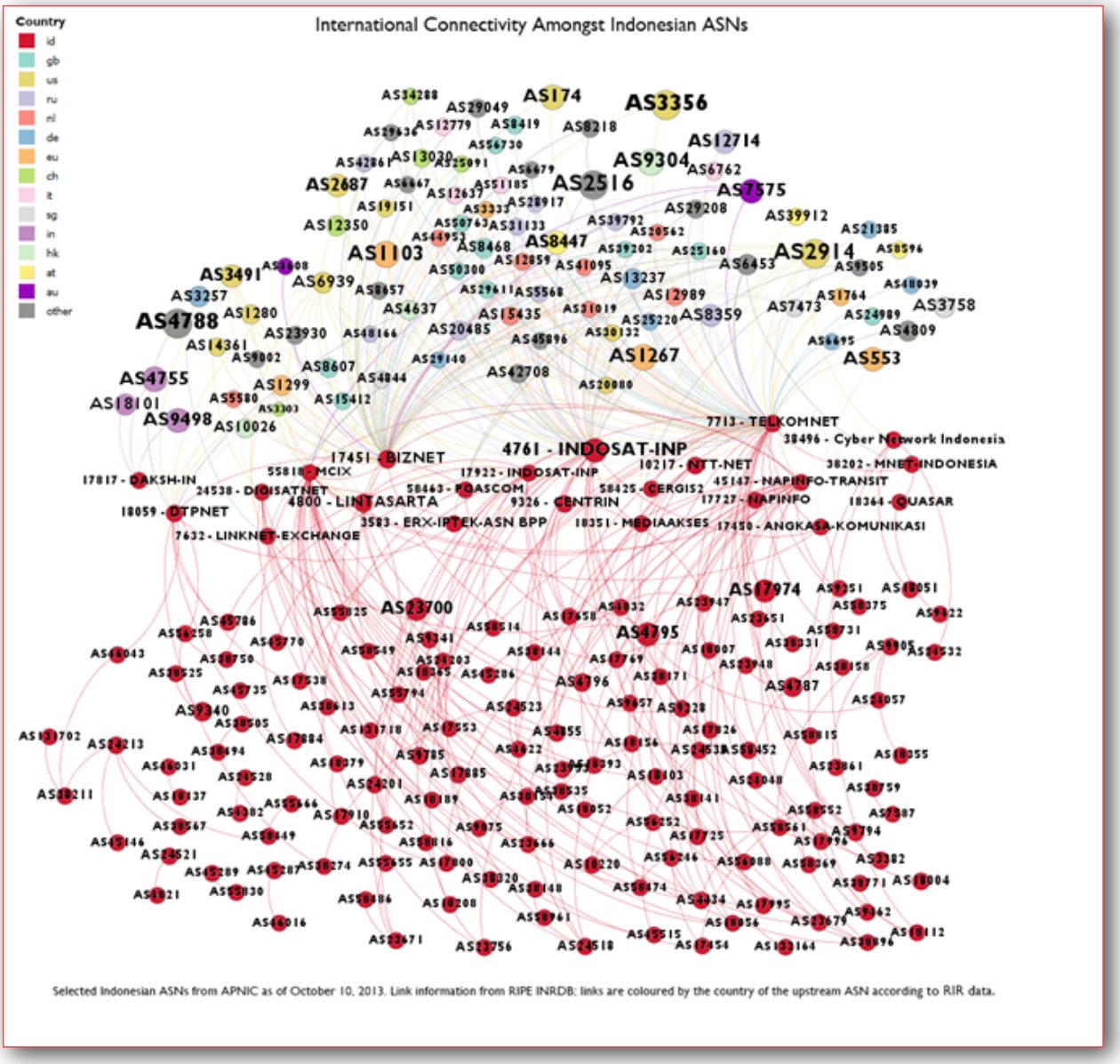


FIGURE 4: International connectivity among Indonesian Autonomous System Numbers.

Despite its impressive growth and numerous small and large ISPs, Indonesia's ICT development has lagged behind many of its regional neighbours' ICT growth. For example, Malaysia's Internet penetration rate was close to 66 percent in 2012, while the percentage of individuals using the Internet in Singapore was 74 percent in the same year. LIRNEasia, a regional think tank focusing on ICT policy and regulation in the Asia-Pacific region, places this technological development gap in the context of political instability and Indonesia's economic stagnation during the Asian financial crisis of the late 1990s. LIRNEasia further names the limited use of English in Indonesia, a lack of access to telecommunication infrastructure in rural areas, the high cost of connectivity to the international backbone, and inadequate government regulation as contributing factors to Indonesia's low ICT use. In addition, according to the Indonesian Internet Governance Forum (ID-IGF), the low level of bandwidth and computer penetration in Indonesia has contributed significantly to the challenge of increasing Internet penetration in the country.

REGULATORY BODIES

Ministerial duties associated with the regulation of information technology fall under the auspices of the Ministry of Communication and Information Technology (MCIT). The ministry defines part of its function as the "formulation of national policy, policy implementation, and technical policies in the field of communication and informatics, including the postal, telecommunications, broadcasting, information technology and communications, multimedia services and the dissemination of information." In 2005, the MCIT took control of the Directorate General of Post and Telecommunication (DGPT). According to its website, the DGPT has three functions:

> The first covers all general and operational aspects, which are implemented through licensing and other requirements. The second function covers all aspects of surveillance and scrutiny to make sure that posts and telecommunications are conducted within the legal framework, while the third function deals with supervision of the operators as well as enforcement of law regarding their operations.

Another key government department is the Indonesian Telecommunications Regulatory Body (Badan Regulasi Telekomunikasi Indonesia, BRTI). The BRTI is responsible for issuing licenses, resolving disputes, and advising government on telecommunication policy issues. However, its responsibilities vis-à-vis DGPT are not clearly defined. Although the BRTI was intended to be an independent regulator, the agency has been criticized for its lack of independence because it is chaired by the DGPT, which is part of MCIT.

LAWS AND REGULATIONS

THE INDONESIAN CONSTITUTION (UNDANG–UNDANG DASAR (UUD) 1945

The 1945 constitution was amended four times between 1999 and 2002. Before these amendments, the constitution did not explicitly affirm human rights. For instance, articles 27 (1 and 2) and 28 asserted only the *existence of the principle* of equality before law, freedom of assembly, and freedom of speech. It was after the amendments were made that the constitution stipulates a number of articles that explicitly affirm human rights are honoured and guaranteed. Ten articles were incorporated into the constitution (articles 28A, 28B, 28C, 28D, 28E, 28F, 28G, 28H, 28I and 28J), proving that Indonesia has adopted the Universal Declaration of Human Rights (Deklarasi Universal tentang Hak Asasi Manusia).[10]

DECREE NO. 17/MPR/1998 AND LAW NO. 39 OF 1999 ON HUMAN RIGHTS

This is how the Decree of the Consultative Assembly (TAP MPR) No. 17/MPR/1998 concerning human rights protects the right to freedom of expression:

- Everyone shall have the right to freedom to express his/her opinions and convictions based on their conscience (article 14);
- Everyone shall have the right to freedom of association, assembly, and expression opinion (article 19);
- Everyone shall have the right to communicate and receive information for his/her personal development and social environment (article 20);
- Everyone shall have the right to seek, obtain, possess, keep, process, and convey information by utilizing all kinds of available channels (article 21); and
- The right of citizens to communicate and obtain information is guaranteed and protected (article 42).

Furthermore, Indonesia adopted Law No. 39 of 1999 on Human Rights. The preamble to this law states that Indonesia, as a United Nations (UN) member state, has moral and legal responsibilities to honour and implement the Universal Declaration of Human Rights and other international instruments on human rights. The law also stipulates that everyone has the right to express his or her opinion in public (article 25).

10 Persandingan UUD 1945, 2002, 49-57; and Totok Sarsito, "The Indonesian Constitution: Why It Was Amended," *Journal of International Studies* 3 (2007), http://www.myjurnal.my/public/issue-view.php?id=2125&journal_id=217.

RELIGION

Religion is a key factor affecting the regulation of freedom of expression in Indonesia. As the world's largest majority Muslim country, the voices of those who believe in a more conservative brand of Islam have influenced discussions ranging from the social to political arenas and have given rise to strict legislation governing what is considered acceptable content or speech.

Passing laws with harsh, punitive legal measures and demanding telecommunication companies like BlackBerry and ISPs to filter out pornographic content indicates increasing pressure from conservative groups, and the lack of protection of peoples' right to freedom of expression and freedom of information, despite these rights being included in the Indonesian constitution.

Indonesia's free press, dynamic political process, and vibrant civil society have exerted pressure on the government to respect these rights (and will continue to), but there needs to be sustained international support to ensure that the government works in as transparent and accountable a manner as possible.[11]

LAW NO. 36 OF 1999 ON TELECOMMUNICATIONS

Telecommunications services in Indonesia used to be provided by a string of state-owned companies. But recent reforms have attempted to create a regulatory framework that promotes competition and accelerates the development of telecommunications facilities and infrastructure. The enactment of Law No. 36 of 1999 on Telecommunications, which replaced Law No. 3 of 1989 on Telecommunications, provided the framework for a major deregulation of the Indonesian telecommunications sector to unfold. These deregulation measures are reflected in its commitments under the WTO Agreement on Basic Telecommunications that entered into force in February 1998, which means that the country committed itself to review its current policy.

This law does not regulate e-commerce or other specific receiving or sending information through the Internet. However, in the definition of telecommunication, one can see that although it is not explicitly mentioned, the transmission of information through the Internet is covered by the law. The definition of telecommunication in article 1(1) of the law is "any broadcasting, sending and or receiving from any information in the form of sign, code, word, picture, sound, and tone through cable system, fiber optic system, radio, or other electromagnetic system."[12] Furthermore, article 4(1) mentions that "the state has authority on telecommunication and the government has power to its development,"[13] and therefore, the development of the Internet can be expected to fall under the government's purview.

11 Kikue Hamayotsu, "The Limits of Civil Society in Democratic Indonesia: Media Freedom and Religious Intolerance," *Journal of Contemporary Asia* (2013), http://dx.doi.org/10.1080/00472336.2013.780471.

12 Article 1(1) of Law No. 36/1999, http://dittel.kominfo.go.id/wp-content/uploads/2013/06/36-TAHUN-1999.pdf.

13 Article 4(1) of Law No. 36/1999, http://dittel.kominfo.go.id/wp-content/uploads/2013/06/36-TAHUN-1999.pdf.

LAW NO. 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTIONS LAW

Law No. 11 of 2008 on Electronic Information and Transactions (EIT) was adopted on 21 April 2008. It is the first cyber law in the country and the main instrument for the regulation of online content.

Chapter 7 of the EIT law lists all prohibited acts, which include knowingly and without authority distributing, transmitting, or causing to be accessible in electronic form records containing:

- Material against propriety (article 27(1));
- Gambling material (article 27(2));
- Material amounting to affront and/or defamation (article 27(3)); and
- Extortion and/or threats (article 27(4)).

In 2013, the MCIT said that they will prioritize a revision of the law. Of particular concern is article 27(2) regarding defamation. Gatot S. Dewa Broto, the spokesperson for the MCIT, said 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,[14] especially because it is more severe than the provisions contained in the penal code, which specified the penalty of up to nine months' imprisonment. The section on content controls elaborates on how this law, in conjunction with other laws such as Law No. 44 of 2008 on Pornography (the Anti-Pornography Law), the penal code's articles 207-208, 310-21, and 335 on defamation, and several Indonesian laws prohibiting blasphemy or "defamation of religions," including Law No. 1/PNPS/1965 (the Presidential Decision), is used for content regulation.

The EIT law also contains provisions on interception and wiretapping in article 31(4), which calls for the government to issue a regulation (Peraturan Pemerintah, PP) on the matter. Following a request for judicial review submitted by Anggara, Supriyadi Widodo Eddyono, and Wahyudi Djafar from the Institute of Policy Research and Advocacy (ELSAM), the Constitutional Court annulled article 31(4) because it contradicted articles 28G(1) and 28J(2) of the 1945 constitution. Furthermore, because wiretapping imposes a limit on individual privacy rights, which are a basic human right, the court ruled that it has to be regulated by legislation (Undang-undang) and not merely by government regulation.

DRAFT LAW ON TELEMATICS CONVERGENCE

To prepare for the convergence of traditional media and new media, the MCIT drafted the Telematics Convergence Law (Rancangan Undang-Undang Konvergensi Telematika), which

14 For more information on the Criminal Defamation Law, please see "Turning Critics into Criminals: The Human Rights Consequences of Criminal Defamation Law in Indonesia," Human Rights Watch, http://www.hrw.org/sites/default/files/reports/indonesia0510webwcover.pdf.

the government proposed as an overarching law to the Telecommunications Act, the EIT Law, and the Broadcasting Law governing telecommunications and ICT in Indonesia.

Telematics is defined broadly as any kind of application that uses the Internet to transmit (e.g., voice, images, data, content-based services, e-commerce, as well as other services provided through applications). The fact that the government drafted a law with such a broad definition of what it is supposed to regulate caused concerns that it will be used to control online content and information. After widespread criticism, the draft Telematics Convergence Law was shelved indefinitely by the MCIT. As an alternative, the People's Representative Council (Dewan Perwakilan Rakyat, DPR) initiated a draft Broadcasting Law and its deliberation process is underway. If the law passes, a Convergence Law will no longer be necessary.

DRAFT LAW ON INTERCEPTION MECHANISM

In Indonesia, there are at least twelve laws, two government regulations, and two ministerial regulations that outline the practice of wiretapping by state institutions in the name of law enforcement. In January 2013, Gatot S. Dewa Broto, the spokesperson for Indonesia's Ministry of Communications and Information Technology, stated that the government as a whole is preparing a draft law on interception mechanisms (Rancangan Undang-Undang Tata Cara Intersepsi). The section on Internet surveillance elaborates further on the legal and operational problems surrounding wiretapping in Indonesia.

DRAFT LAW ON INFORMATION TECHNOLOGY CRIMINAL OFFENCE

The People's Representative Council (DPR) drafted the Information Technology Criminal Offence Law (Rancangan Undang-Undang Tindak Pidana Teknologi Informatika, TIPITI) as a response to the proliferation of cybercrime in Indonesia. When it was first announced to the public, the bill was considered to be a major threat to freedom of expression because many people considered its provisions to be too broad, and to contain worse penalties than those in the controversial Electronic Information and Transactions Law (e.g., up to thirty years in prison and fines up to USD 1,060,000, according to the 2009 draft). Although the bill was considered to be a priority bill in the 2010 National Legislation Program, it was not until 2012 that it was finalized due to pressure from the MCIT. At the time of publication, the law is still waiting to be passed.

CYBER AND REGIONAL SECURITY INITIATIVES

Like almost all countries today, Indonesia recognizes that cyber security has become a major priority. Indonesia has become a full member of the Asia Pacific Computer Emergency Response Team (APCERT) and FIRST (Forum for Incident Response and Security Team) and a full member and founder of the OIC-CERT (Organization of the Islamic Conference-Computer Emergency Response Team). As of 2010, the draft law on cybercrime and

draft law on the ratification of the EU Convention on Cybercrime have been listed in the national legislation program as priorities to be discussed. Whatever the components of that cybersecurity strategy will be, it will invariably affect the character of information controls. Indonesia's cybersecurity strategy will reflect both contests among domestic interest groups and stakeholders, as well as the influence of regional and international norms and Indonesia's participation in regional and other security forums. In particular, the regional alliance—the Association of Southeast Asian Nations (ASEAN), of which Indonesia is a founding member—will be a major influence and source of norms and practices. In September 2013, ASEAN announced that a cybersecurity agreement was reached among member states in which Indonesia and other members will jointly develop a mechanism to combat cyber attacks, coordinate trainings, and share threat information—practices that have already begun among some of the region's CERTs. Along with our colleagues in the region, we will be monitoring these developments closely, especially in light of the impending arrival of the ASEAN Economic Community in 2015. We intend to issue reports on regional cybersecurity initiatives in Asia.

CONCLUSION

Indonesian information controls cannot be understood without considering the broader social, political, and legal context and the ICT environment within which they are embedded. The nature and character of information controls depend on the market structure of ISPs, telecommunication companies, informal relations, and practices among stakeholders, especially a diverse and politically active civil society, and the legal and policy structures that frame them all.

ANALYZING CONTENT CONTROLS IN INDONESIA

As we outlined in the introduction, information controls aim to manage the content accessible to a population, including information posted online. Content 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 – otherwise known as "Internet filtering." We employ a multidisciplinary mixed-methods approach to study content 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 country's legal and regulatory filtering framework. The combination of technical investigation with political, social, and legal contextual research is essential for understanding both how and why information controls are applied. We also aim to determine the specific techniques and, where possible, the products that are used to implement Internet content filtering.

Indonesia is a prime example of a country where mixed methods provide essential insight into the scope, scale, and character of content controls. As we described earlier, the country is characterized by a highly distributed and very competitive media environment in which Internet service providers (ISPs), civil society stakeholders, and government ministries engage in a sometimes contentious debate over what content should be filtered, by whom, under what processes, and according to which laws. The country has significant cultural and religious sensitivities around certain types of content. Although network measurement provides us with a baseline of data, our analysis of the scope, scale, and character of Indonesian content controls is greatly enriched by local knowledge of the Internet and cyberspace environment in the country, parts of which are explained in the section on infrastructure and governance.

Building on past network measurements, as well as legal and policy analyses undertaken by the OpenNet Initiative, we set out to better understand the current situation. Our analysis is set in the context not only of the 2013 IGF, but amid increasingly intense debates about free expression and access to information, and rapid technological change and development.

While the detailed results of our analysis and technical tests are outlined below, our main findings can be summarized like this:

- Implementation of Internet filtering in Indonesia is decentralized (in both policy and technical processes). Although the Indonesian government sets broad expectations and "rules" (sometimes informally communicated) about what content should be filtered by ISPs, and is moving toward standardizing telecommunication laws that would more systematically regulate content control practices, the actual control of content today is left primarily to ISPs' discretion.
- Reflecting the decentralized nature of the ISP environment, our research detected a range of Internet filtering devices and software, and a diversity of content control practices being used on different ISPs. Some use the government-promoted systems DNS Nawala and Trust+ Positif, while others use different systems. For example, we found one ISP using Netsweeper, a content-filtering service manufactured by a Canadian company based in Guelph, Ontario.
- We also detected the presence of devices manufactured by California-based Blue Coat Systems. We detected Packetshaper devices, which have the ability to monitor and control network traffic, on the two biggest Indonesian IPS, Telkom Indonesia and Indosat. We also found CacheFlow on Telkom Indonesia – an appliance whose primary function is to optimize bandwidth by caching but it can also be configured to block content.
- Although formally and officially, Indonesia requires pornography and gambling-related content to be blocked, we found that Indonesian ISPs apply content controls on content related not only to these areas of speech, but also to religious issues and religious advocacy groups, and content related to sexuality and gender (e.g., local LGBT community websites), among other content categories. We found that ISPs are inconsistent regarding the precise nature of content that they target for filtering.
- Citizens are prevented from accessing content that does not fall within objectionable content on ISPs which rely on evidently error-prone mechanisms to categorize website URLs. We provide evidence that websites of academic institutions and government agencies are categorized on a Trust+ Positif URL list as "porn," which results in these websites being blocked on ISPs relying on these URL lists.
- We ran network measurements on Internet connections provided at the 2013 IGF venue and found that the main network connection for workshop sessions was not filtered (as per the stipulations of the IGF host country agreement). However, backup connections (for public areas of the venue) provided by local Indonesian ISPs (Telkom and Indosat) did filter access to content. We compare these results with measurements from network vantage points outside of the IGF venue.

LEGAL AND REGULATORY FRAMEWORKS

Although Indonesia's constitution guarantees freedom of expression under article 28E(3), a number of laws limit freedom of expression online and restrict access to content considered dangerous or socially unacceptable. The penal code and a 1965 blasphemy law that 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. The section on infrastructure and governance explains the nature of these laws in greater detail.

The Electronic Information and Transaction Law limits freedom of expression and prohibits defamation. Free speech advocates requested a judicial review of the defamation article in the law, but the Constitutional Court denied the request in 2009. The Anti-Pornography Law was passed in October 2008 amid opposition from various groups who considered the law a threat to the cultural diversity and the rights of minority groups and women in Indonesia.

The Anti-Pornography Law, which was aggressively promoted and implemented by many ISPs and Internet cafés in 2010 in an effort to block millions of pornography sites during the holy month of Ramadan, was a major turning point for the country's filtering policies and practices. At the time, efforts to build more centralized systems, such as DNS Nawala and Trust+ Positif began to emerge with Indonesian policy-makers promoting their use among ISPs. Meanwhile, the government began installing Trust+ Positif on computers supplied to villages under its Desa Pintar (Smart Village) program. It was also during this period that the Indonesian government threatened to shut down BlackBerry in the country unless it began filtering pornographic content. BlackBerry announced in January 2011 that it would comply with the request and work with carriers to put a filtering solution in place.

Apart from specific invocations of the law, the Indonesian government also pressures ISPs to block websites it defines as extremist in nature. After religious violence erupted in the country in 2011, three hundred websites encouraging greater conflict were blocked as a consequence of this type of pressure. In July 2011, the ICT minister, Tifatul Sembiring, announced plans to filter websites offering illegal downloads of music and videos. He warned that users of these sites could face jail terms and heavy fines for illegal downloading. Individuals with intimate knowledge of these processes explained to us that requests to block content are occasionally passed on by government officials in phone calls or in person during meetings with ISPs and telecom employees. In other words, subtle pressures and moral suasion, rather than transparent and publicly accountable laws and regulations, are occasionally the means ministry officials employ to promote compliance.

As is the case in a number of other countries, Indonesian policy-makers have been using code words that create concerns of a growing interest in blocking access to or communication of content that is culturally, religiously, or politically offensive. For example, the INSAN Socialization Team of

the Ministry of Communications and Information Technology (MCIT) has been actively promoting a "healthy and safe" Internet. The objective of the program is to "socialize a healthy and safe use of Internet to various levels of society in order to avoid misuse and take benefits for society." Leading up to and during the 2013 IGF, Indonesian policy-makers emphasized the need to consider an "ethical" Internet – a euphemism around which some Indonesian civil society groups and IGF delegates, including the US State Department representative Christopher Painter, raised concerns.

PROSECUTION OF NETIZENS

Indonesian laws, rules, and informal directions around content controls are reinforced by occasional prosecution of individuals. The following are some of the more egregious cases.

The most prominent case that invoked the Anti-Pornography Law involved pop singer Nazril Irham (also known as "Ariel"), whose homemade explicit videos were circulated on the Internet against his consent in June 2010. He was convicted and sentenced to three-and-a-half years in prison and a fine of USD 28,000, but he was released after serving only two-thirds of his prison sentence for good behaviour. Irham's conviction, followed by other sex scandals involving local celebrities and politicians, prompted renewed calls for content control by the ICT minister, Tifatul Sembiring, to block access to pornography websites during the Ramadan in 2010. His teams immediately set out to deploy firewalls for more than 2,000 Internet cafés around the country, which he explained as a "race against time" to protect children from harm. Indonesia's President Susilo Bambang Yudhoyono has also indicated his support for an Internet filter to block pornography.

One of the most prominent online defamation cases has been the prosecution of Prita Mulyasari, who was sued by the Omni International Hospital. Mulyasari, a Jakarta-based housewife and mother, communicated her disappointment with Omni Hospital's service by e-mail to her friends in September 2008, which was forwarded, circulated on electronic mailing lists, and posted online. Once the e-mail became public knowledge, Omni International Hospital responded by filing a criminal complaint and a civil lawsuit against Mulyasari. She was then arrested in May 2009, by the Banten Provincial Prosecutor's Office and charged under articles 310 and 311 of the penal code regarding defamation and article 27 of the EIT Law. The court had initially found Mulyasari liable in the civil case and ordered her to pay IDR 204 million (approximately USD 22,000) to Omni International. The charge sparked outrage among tens of thousands who joined a Facebook group in her support and held an online fundraising campaign called "Coins for Prita" to help her pay the fine. The campaign raised IDR 650 million or more than three times the amount of the fine. After appealing to the Supreme Court, she was later acquitted of all civil charges in September 2010. At the same time, criminal proceedings were underway, which eventually found her guilty. She was given a suspended sentence of six months' imprisonment contingent upon good behaviour. Upon appealing in 2012, the Supreme Court overturned the lower court's decision and quashed the criminal charges.

In June 2012, civil servant Alexander Aan was sentenced by a West Sumatra court to two-and-a-half years in prison and fined IDR 100 million (USD 11,100) (or face another two months in prison) for comments considered blasphemous made on his Facebook account and Facebook fan page, titled Ateis Minang (Minang Atheist). Aan's conviction was justified on the grounds that he had violated the blasphemy provisions of the penal code, as well as article 28 of the Electronic Information and Transaction Law by "spreading racial and religious hatred."

TECHNICAL IMPLEMENTATION OF CONTENT CONTROLS

Because the Internet environment in Indonesia is broadly distributed, 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. Some ISPs even still offer, on occasion, an entirely unfiltered Internet, although that is increasingly rare. We confirmed this variation in both manual and automated network measurements, made from inside and outside the country.

In spite of the decentralization, there are also growing tendencies of standardization, if not centralization. For example, a number of national-level systems have emerged that offer filtering services, promoted by the MCIT. 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 expectations. Additionally, ISPs have begun to purchase commercial filtering products developed outside of Indonesia, for example those made by Netsweeper and Blue Coat, whose services include categorizing and controlling access to content online, thus taking the burden of maintaining content controls away from ISP administrators. Should more ISPs use these types of services, the existing decentralized architecture of the ISP ecosystem could in practice tend toward a degree of standardized content targeted for filtering, though that is not yet the case today.

As part of its national program Healthy and Safe Internet, the INSAN Socialization Team of the MCIT is endorsing two DNS filtering projects that include configurations and URL lists to standardize content filtering on Indonesian ISPs, Trust+ Positif and DNS Nawala. Currently, the use of these programs is optional. Because ISPs use a variety of filtering systems and techniques, they are inconsistent regarding what content is blocked. During the IGF 2013 meeting, MCIT booths prominently displayed advertisements for and distributed materials about the Healthy and Safe Internet program that promotes Trust+ Positif and DNS Nawala (see Figure 5, next page).

FIGURE 5: Promotional materials for the "Healthy and Safe Internet" program disseminated by the MCIT at their IGF 2013 booth.

DNS-ENABLED FILTERING INITIATIVES

Private sector associations in Indonesia have made several attempts to standardize content to be filtered and techniques for DNS filtering. Beginning in 2008, the Association of Indonesia's Internet Cafés (AWARI) started an initiative to standardize filtering across Internet cafés and provide a means for users to report sites for blocking. Prior to 2008, filtering in Internet cafés was decentralized. Standardization of filtering was seen as positive development to ensure that Internet cafés operated on an equal footing.

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. Standardization of content filtering was seen as a requirement to ensure compliance with the INSAN program. When DNS Nawala was launched, PT Telkom, the largest ISP in

Indonesia, agreed to use the program. When PT Telkom announced it would use DNS Nawala, Eddy Kurina (vice president, public and marketing communication) stated that "for the growth and development and improvement of quality of young generation and as part of the Corporate Social Responsibility program, Telkom provides DNS Nawala able to select the internet contents [sic]." The program was set back when network disruptions followed an installation of DNS Nawala on a major Internet exchange point.

The Indonesian Internet Service Provider Association (Asosiasi Penyelenggara Jasa Internet Indonesia, APJII) has an agreement with DNS Nawala to provide the 250 members of the ISP association with use of the service. As part of this cooperation APJII provides DNS Nalawa with five servers and DNS Nawla in turn gives its block lists to APJII members.

The use of DNS Nawala is not compulsory for APJII members. However, in a statement APJII Chairman Sammy Pangerapan cautioned APJII members that they are responsible for content on their networks and the APJII encourages members to use the service.

TRUST+ POSITIF

Trust+ Positif is maintained and endorsed by the MCIT, and provides content-filtering capabilities distributed as configuration files and block lists for the popular open source Squid HTTP proxy and the SquidGuard add-on which is an open source implementation of URL access control lists for Squid. Trust+ Positif is another attempt to standardize content filtering in Indonesia and is described as providing access to a "safe and healthy internet by protecting Internet access based on series of lists containing healthy and reliable information." The system aims to protect society against values, ethics, and morals "that do not fit with the image of the Indonesian nation."

FIGURE 6: Ministry of Communication and Information Technology booth at IGF 2013 promoting Trust+ Positif.

Trust+ Positif feeds SquidGuard two URL databases:

» Domain List: This contains a list of top-level domains. If a domain is found on this list (e.g., facebook.com) then any subdomain or path (e.g., *.facebook.com or www.facebook.com/home.php) which includes the top-level domain will be included.

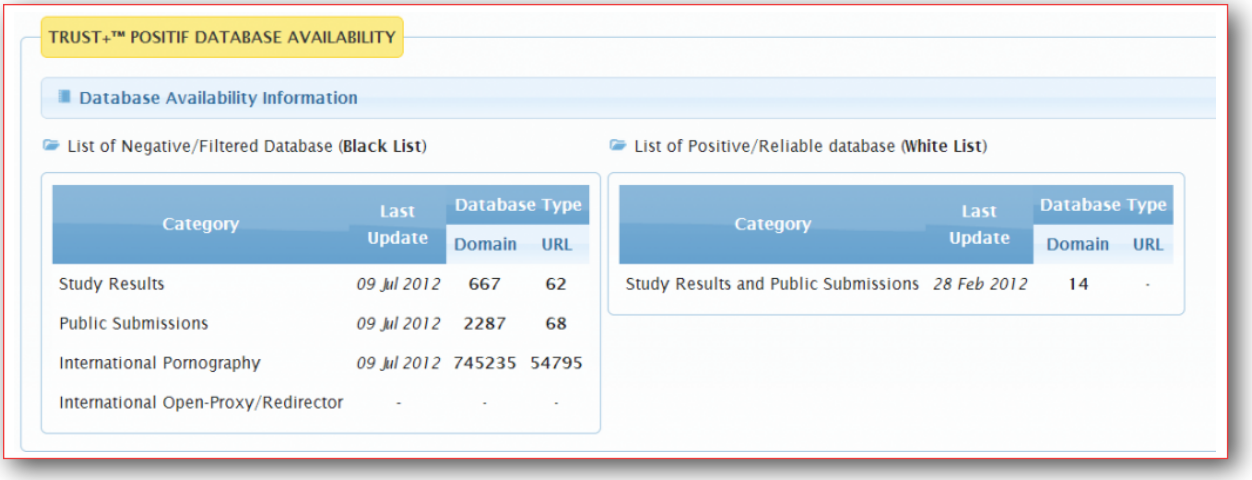
» URL List: This contains lists of single URLs (e.g., www.facebook.com/pages/Everybody-Draw-Mohammed-Day).

These lists group URLs and domains into a number of categories:

» White List (positive/reliable): This category includes domains and URLs that have been flagged as "positive or trusted" (e.g., government domains).

» Black List (negative/filtered): This category contains URLs and domains with content considered "negative" such as pornography. The black list is divided into three categories: "Study Results and Public Submissions," "International Pornography," and "International Open-Proxy."

The content of these lists and information about the number of domains and URLs included are made publicly accessible, as Figure 7 illustrates.



TRUST+™ POSITIF DATABASE AVAILABILITY

Database Availability Information

List of Negative/Filtered Database (**Black List**)

Category	Last Update	Database Type	
		Domain	URL
Study Results	*09 Jul 2012*	667	62
Public Submissions	*09 Jul 2012*	2287	68
International Pornography	*09 Jul 2012*	745235	54795
International Open-Proxy/Redirector	-	-	-

List of Positive/Reliable database (**White List**)

Category	Last Update	Database Type	
		Domain	URL
Study Results and Public Submissions	*28 Feb 2012*	14	-

FIGURE 7: Quantity of URLs and domains in Trust+ Positif databases.

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 was described as "under development"). However, how this submission process operates in practice is unclear and the MCIT ultimately decides what to block. No judicial order is required.

TRUST+ POSITIF URL MISCATEGORIZATION

The Trust+ Positif website provides users with the option to search for information about domain names or URLs that have been registered in the Trust+ Positif URL lists. This search helps users find out whether a domain name or URL has been listed in the Trust+ Positif database, and check for its categorization.

We entered URLs of websites containing sexual and pornographic content and the database returned their categorization as "porn" websites. For example, the URL www.playboy.com was returned as "porn," as Figure 8 shows (next page).

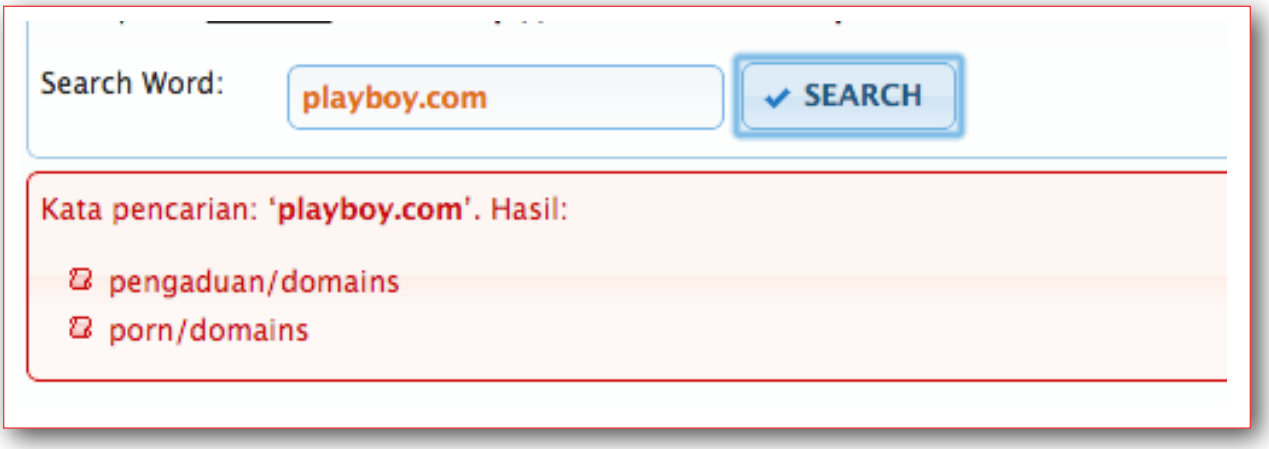


FIGURE 8: Trust+ Positif shows categorization of playboy.com as "porn."

However, when we tried URLs of nonpornographic websites that have been found blocked on some Indonesian ISPs, the database returned no data. For example, a search for the website www.faithfreedom.org, which has alternative views on the faith of Islam, returned the message "Tidak ada data" (no data), as can be seen in Figure 9.

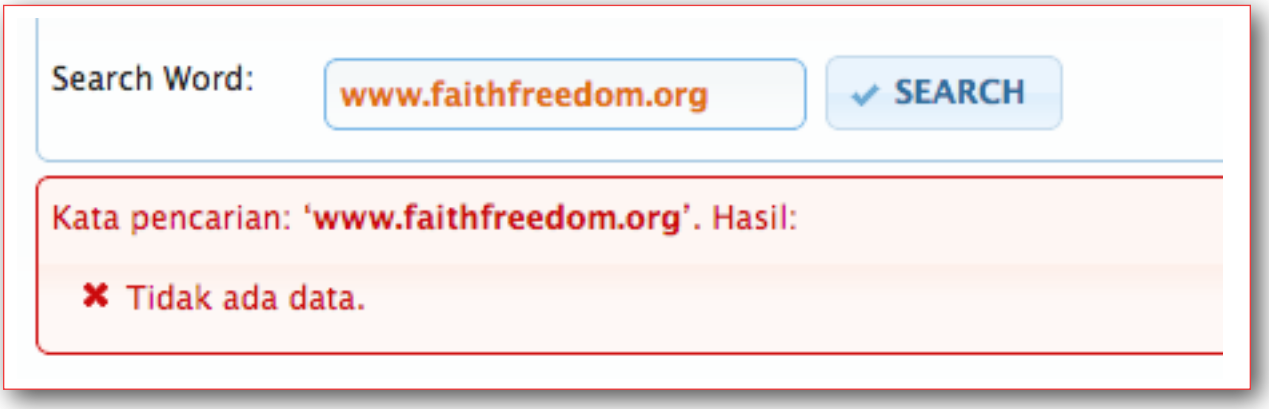


FIGURE 9: Trust+ Positif reports no data available for the blocked URL faithfreedom.org.

We analyzed how the Trust+ Positif URL dataset categorizes a sample of URLs and found that there are numerous URL miscategorizations that result in erroneous blocking. We downloaded the block list that categorizes which domains are pornographic—it is publicly available on the Trust+ Positif website. We then searched through the list to find examples of potential miscategorizing. Once completed, we verified that these URLs and domains are currently in the Trust+ Positif URL lists by submitting them to their online URL-checking tool.

Examples of such miscategorization are provided in Table 1.

URL	CONTENT	CATEGORIZATION IN TRUST+ POSITIF DATABASE
glbtss.colostate.edu	GLBT Resource Center, Colorado State University	Porn
www.muslimsconnect.com	Dating site	Porn
gibraltar.gov.uk	UK government website about Gibraltar	Porn
newspiritchurch.org	New Spirit Community Church	Porn
www.libertyeducationforum.org	Liberty Education Forum – think tank from Washington, DC	Porn
www.civilmarriagecivilright.com	LBGT social issues and personal site	Porn
www.equalityforum.com	LGBT social issues site	Porn
wcl.american.edu/journal/lawrev/49/vol49-5rothenberg.pdf	Academic paper about peeping Toms	Porn (urls)
lib.rochester.edu	Library at the University of Rochester	Porn
www.slowtrains.com	Literary journal	Porn
www.eastcoastcomputers.com	IT firm from Florida	Porn
www.lavalife.com	Dating site	Porn

TABLE 1: Examples of URLs miscategorized in the Trust+ Positif database as "porn."

Alexa ranks the Trust+ Positif website served to users who browse blocked content on certain ISPs (www.internet-positif.org) among the top hundred pages accessed in Indonesia (number 72 on 24 October 2013) which suggests that a significant number of access attempts are served the block page.

COMPARISON OF DNS NAWALA AND TRUST+ POSITIF BLOCK LISTS

We compared both DNS Nawala and Trust+ Positif lists of domains that they categorize as pornographic content. The DNS Nawala block list was retrieved at a time in which a misconfiguration of the DNS Nawala website in 2010 allowed for the download of the block list. The Trust+ Positif blocklist was retrieved directly from a public link on their website. We found that the majority of domains listed are common between the two sets of lists. The Trust+ Positif list does not include any additional domains that are included in the DNS Nawala list, while the DNS Nawala list has 205 additional domains that are not in the Trust+ Positif list.

CANADIAN AND US COMMERCIAL URL FILTERING PRODUCTS DETECTED IN INDONESIA

NETSWEEPER

Netsweeper is a technology company based in Guelph, Ontario, that provides software products used to filter web content. In previous research, we found that Netsweeper software was deployed to censor political and human-rights-related content at the national level in Pakistan, Qatar, Kuwait, UAE, and Yemen. We searched for signatures of the Netsweeper products in the search engine Shodan, using methods described here, and we found an installation of Netsweeper on the Indonesian ISP PT Excelcomindo Pratama.

The Netsweeper control panel appears at http://202.152.254.227:8080/webadmin/start, while the block page is accessible at http://202.152.254.227:8080/webadmin/deny/index.php.

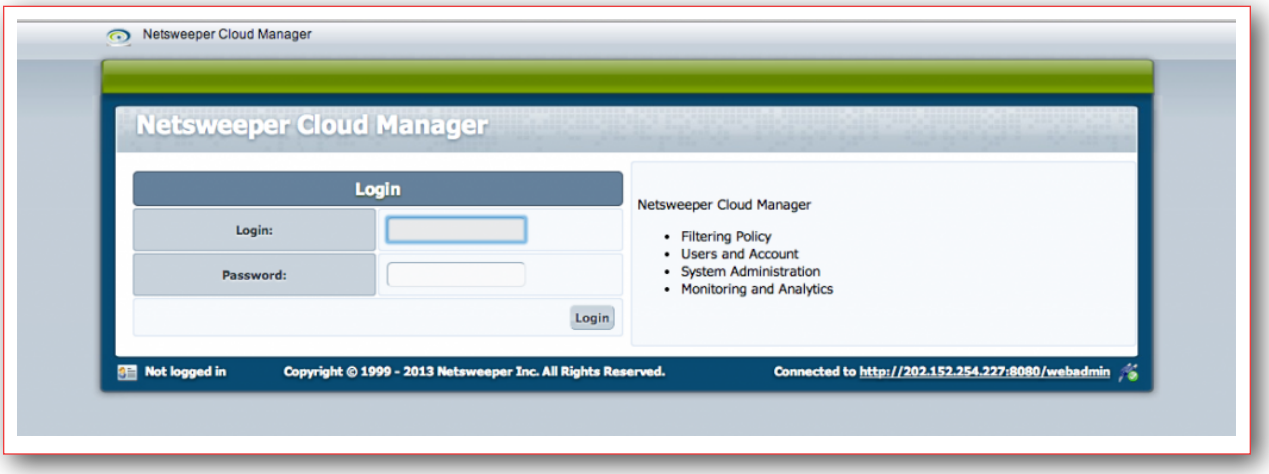


FIGURE 10: Netsweeper control panel installed on ISP PT Excelcomindo Pratama.

BLUE COAT

Blue Coat Systems is a California-based provider of network security and optimization appliances. Some of these products can enable network filtering and surveillance. These products include: ProxySG which works with WebFilter, to categorize web pages for filtering; PacketShaper, a cloud-based networking management device that can establish visibility of over six hundred web applications and control undesirable traffic; and CacheFlow, a web-caching appliance that optimizes bandwidth. ProxySG provides "SSL Inspection" services to solve "issues with intercepting SSL for your end-users." PacketShaper has the ability to monitor and control network traffic: it is integrated with WebPulse, Blue Coat Systems'

real-time network intelligence service that can filter application traffic by content category. CacheFlow can be configured to block content.

While these tools can be used to maintain and secure networks, they can also be used to implement politically motivated restrictions on access to information, and monitor and record private communications. Depending on their end use, these tools can be used to serve legitimate and positive purposes, or purposes resulting in adverse impacts on human rights. This capacity is often referred to as "dual-use," a term adapted from language used to describe technologies with both civilian and military applications.

As part of prior Citizen Lab research that included a combination of wide-area scanning techniques, Shodan queries, and other experimental methods, we found Blue Coat devices on public networks in eighty-three countries (twenty countries with both ProxySG and PacketShaper, fifty-six countries with PacketShaper only, and seven countries with ProxySG only). Among those findings was the presence of PacketShaper on the networks of both Indosat (http://202.155.63.62/login.htm) and Telkom Indonesia (http://203.130.193.156/login.htm) networks. We also found installations of CacheFlow on Telkom (http://180.252.181.1).

NETWORK MEASUREMENTS

We used a variety of techniques for measuring censorship on networks in Indonesia, including client-based tests performed within Indonesia and remote tests through publicly available web proxies and virtual private networks (VPNs).

Client-based Tests

Data was collected by performing synchronized HTTP requests in both a field location (i.e., a location where web censorship is suspected) and 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. The field locations included a number of Indonesian ISPs.

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

A number of data points are collected for each URL access attempt: HTTP headers and status code, IP address, page body, and in some cases 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.

In addition to tests using our measurement software, tests were also run with two other network measurement tools: Netalyzr and OONI-Probe. Netalyzr is a network diagnostic tool developed at the University of California, Berkeley. We ran it to gather additional data about the properties of tested networks. Collin Anderson, an independent researcher who attended the 2013 IGF, also ran tests with OONI-probe (a client-based Internet censorship measurement tool developed by the Tor project) and contributed his results to this section.

Remote Tests

We ran tests of website accessibility using publicly available Indonesian web proxies and VPNs. The purpose of these tests was to help develop our URL-testing lists for client-based measurements.

2008-2010 NETWORK MEASUREMENT RESULTS

Between 2008 and 2010 we ran client-based network measurements on twenty different ISPs in Indonesia. The results of this testing show significant decentralization in how Indonesian ISPs technically implement filtering; they also show inconsistency between ISPs in terms of what content is blocked.

On Indosat (AS 4795) and XL Axiata (AS 24203) we observed block pages delivered via DNS redirection to IP addresses hosted by each ISP, and we noted that Indosat's use of block pages began in late 2010. Similarly, we observed XL Axiata implementing a combination of DNS redirection and block pages in 2010, but we lacked longitudinal data about this ISP.

In contrast to Indosat and XL Axiata that display block pages, BIZ Net (AS 17451) implemented DNS redirects that went to non-routable IPs that therefore look like transient failures from the user's perspective. In 2008, redirects went to IP 0.0.0.1, but in 2009 and onwards we saw this shift to the link-local IP 169.254.1.1 address. Finally, in sixteen different tests over three years, First Media (AS 23700) showed no evidence at all of DNS redirection.

The specific content blocked is also inconsistent across ISPs. Pornographic content and gambling websites were regularly blocked by Indonesian ISPs in our sample. However, testing conducted from 2009 to 2010 showed that on some ISPs (e.g., Indosat, XL Axiata) blocked websites included content related to free expression (e.g., www.freespeech.org, an online video network, and www.freespeechcoalition.com, a free speech group), as well as anonymizers and

censorship circumvention software. Content related to local LGBT community groups and information portals was also found blocked.

A summary of historical data that ONI has collected from Indonesia from 2008 to 2010 appears in Figure 11. It shows the ration of blocking behaviours observed on different ISPs in the region. The possible behaviours indicated are:

- No DNS response: when there is no DNS response given in Indonesia, while there is a response in Toronto.
- DNS redirection: when a DNS query redirects to a different IP in Indonesia compared to a DNS query from Toronto.
- No HTTP response: when an HTTP response is seen in Toronto but not in Indonesia.
- LCRST (low confidence reset): when the page is retrieved successfully in Toronto (Response code < 400) while a reset packet is observed in Indonesia with no content returning.
- RST (reset): when LCRST occurs more than three times in a week for the URL in Indonesia.
- Block page: when a known block page is returned in Indonesia.

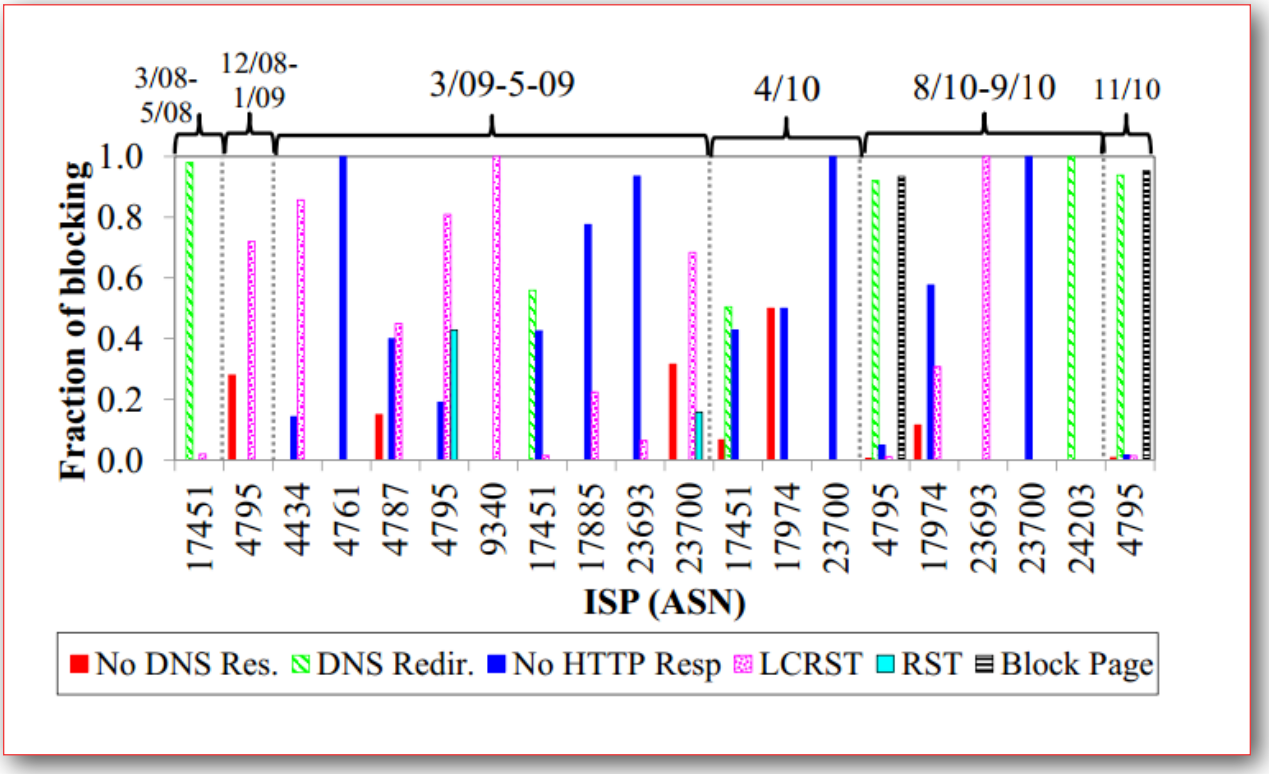


FIGURE 11: Summary of blocking in Indonesia (ISPs with at least ten blocked URLs per year in at least two years). For further technical details regarding how these categories are determined, please refer to table 3, page 5 in http://www.cs.stonybrook.edu/~phillipa/papers/ONIAnaly.html.

2013 NETWORK MEASUREMENT RESULTS

Remote Measurement Results

DNS Nawala: Testing was conducted using DNS Nawala's publicly accessible DNS servers (180.131.144.144 and 180.131.145.145) using the same list of URLs used for in-country testing. 215 URLs from this list of 1,387 URLs resolved to the IP address 180.131.146.7, which is the block page for the DNS Nawala service shown in Figure 12. The full list of URLs tested and found blocked using the DNS Nawala service can be found here.

The block page reads (translation from Indonesian):

> The website you are trying to open cannot be accessed on this network. www.playboy.com is categorized as one of the following:
>
> - Porn
> - Gambling
> - Phising [sic] /malware
>
> SARA [SARA stands for "Suku, Agama, Ras, Antar-golongan," which refers to content related to ethnicity, religion, race, and intergroup relations].
>
> If you feel the website that you want to access is erroneously categorized, please contact us via email info@nawala.org.

FIGURE 12: DNS Nawala block page.

Client-based Measurement Results

Client-based network measurements were run on four ISPs, including three connections provided to delegates at the IGF 2013 venue and one ISP outside of the IGF venue to provide a basis for comparison between content controls at the IGF and those elsewhere in the country.

ISP: Tri
AS: THREE-AS-ID Hutchison CP Telecommunications, PT
Netalyzr Results

Testing was conducted on 22 and 23 October 2013 on the ISP Tri using a 3G mobile connection tethered to a laptop running our client-based measurement software. Test results showed 142 URLs blocked out of the sample of 1,387 URLs we tested. Blocked content spanned twenty-two content categories, including LGBT content, critical religious content, independent media, circumvention tools, sex education sites, gambling, and pornography. A full list of blocked content can be found here.

Blocked content resolved to a private routable IP address of 10.70.25.111 and displayed a nontransparent block page stating "It works!" The HTML source is identical to the default web page of a fresh installation of the Apache Web server, as Figure 13 illustrates.

FIGURE 13: Block page and HTML source found on ISP Tri.

IGF Venue Network Measurement Results

The Bali Nusa Dua Convention Center (the venue for the 2013 IGF) provided four wireless connections to participants (SSIDs: IGF 2013, IGF-a, IGF2013.wifi.id, IGF2013@Indosat) (See Figure 14).

FIGURE 14: Sign describing wireless Internet access points at the IGF 2013 venue.

The host country agreement signed between the government of Indonesia and the United Nations mandates that an open Internet connection is provided. The primary wireless network, identified by the SSID IGF2013, intended to offer this unfettered access. A network administrator from the organizing committee informed us that "the main wi-fi access managed by [the IGF host] committee is using SSID IGF2013, and we didn't filter any sites." A 5 Ghz version of this primary network, with the SSID IGF2013-a, was also made available. Both of these connections rely on bandwidth from Telkomsei and are routed out of the country through that ISP. However, these connections have their own network operations centre (NOC).

Two other networks were available at the event and are under the filtering regimes of their respective ISPs: IGF2013@wifi.id is provided by Telkomsei and IGF2013@Indosat is provided by Indosat. These ISPs are the two largest providers in Indonesia and regularly provide connectivity to the Bali Nusa Dua Convention Center where the 2013 IGF and other major events such as the recent 2013 APEC conference summit were held.

SSID: IGF2013 - IPV6 (2.4 GHgz)
AS: IGF2013-ID Internet Governance Forum 2013
Netalzyer Results

Testing on the SSID IGF2013 (AS: IGF2013-ID Internet Governance Forum 2013) showed no evidence of filtering out of the 1,387 URLs tested. Organizers described this network as offering unfettered access as per the UN host agreement, and our technical testing verified this claim.

SSID: IGF2013@wifi.id
AS: TELKOMNET-AS2-AP PT Telekomunikasi Indonesia
Netalyzer Results

Testing on the SSID IGF2013@wifi.id (AS TELKOMNET-AS2-AP PT) found 197 URLs blocked out of the sample of 1,387 URLs tested through DNS tampering. A variety of content was blocked, including LGBT content, independent media sites, critical religious content, and circumvention and anonymizer tools. A full list of blocked URLs can be found here.

All blocked content resolved to the IP address 118.98.97.100. Users were redirected to a block page hosted at www.internet-positif.org, like this response to an HTTP GET request:

> HTTP/1.1 307
> Server: nginx
> Date: Mon, 21 Oct 2013 10:22:31 GMT
> Content-Type: text/html
> Transfer-Encoding: chunked
> Connection: close
> Cache-Control: no-cache
> Location: href="http://internet-positif.org/site.block?

Upon redirection, the block page shown in Figure 15 was served to users.

FIGURE 15: Trust+ Positif block page observed on the SSID: IGF2013@wifi.id.

The text on the block page reads:

> This forbidden site cannot be accessed because it is indicated that it may contain one of the following: Pornography, Gambling, Phising [sic], SARA [SARA stands for "Suku, Agama, Ras, Antar-golongan," which refers to content related to ethnicity, religion, race, and intergroup relations], or PROXY. If you feel that this site is not included in any of the aforementioned categories, please contact advankonten [at] depkominfo [dot] go [dot] id.

The Trust+ Positif block page serves a number of advertisements hosted on third-party sites. Figure 16 shows the HTTP gets to different domains required when you visit the block page once.

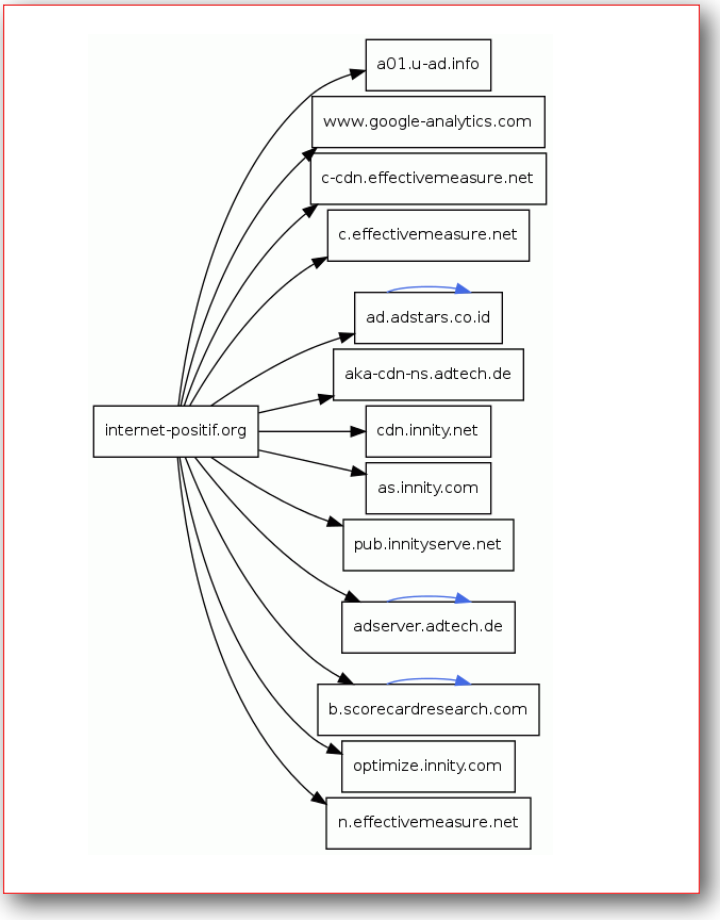


FIGURE 16: HTTP transactions from a visit to http://internet-positif.org. Image taken from http://urlquery.net/report.php?id=7114070.

Tests of website accessibility on this network were also undertaken by independent researcher Collin Anderson, who collaborated with us on the research for this section. Anderson performed a DNS consistency test with OONI-probe against the Alexa top 1 million URL list. Based on those results, Anderson extracted the domains that pointed to the filtering server. He then scripted a retrieval of the OpenDNS assessments on every filtered domain and extracted community categorizations for each. The results of these tests can be found here and the distribution of blocked URLs in each primary category can be seen in Figure 17.

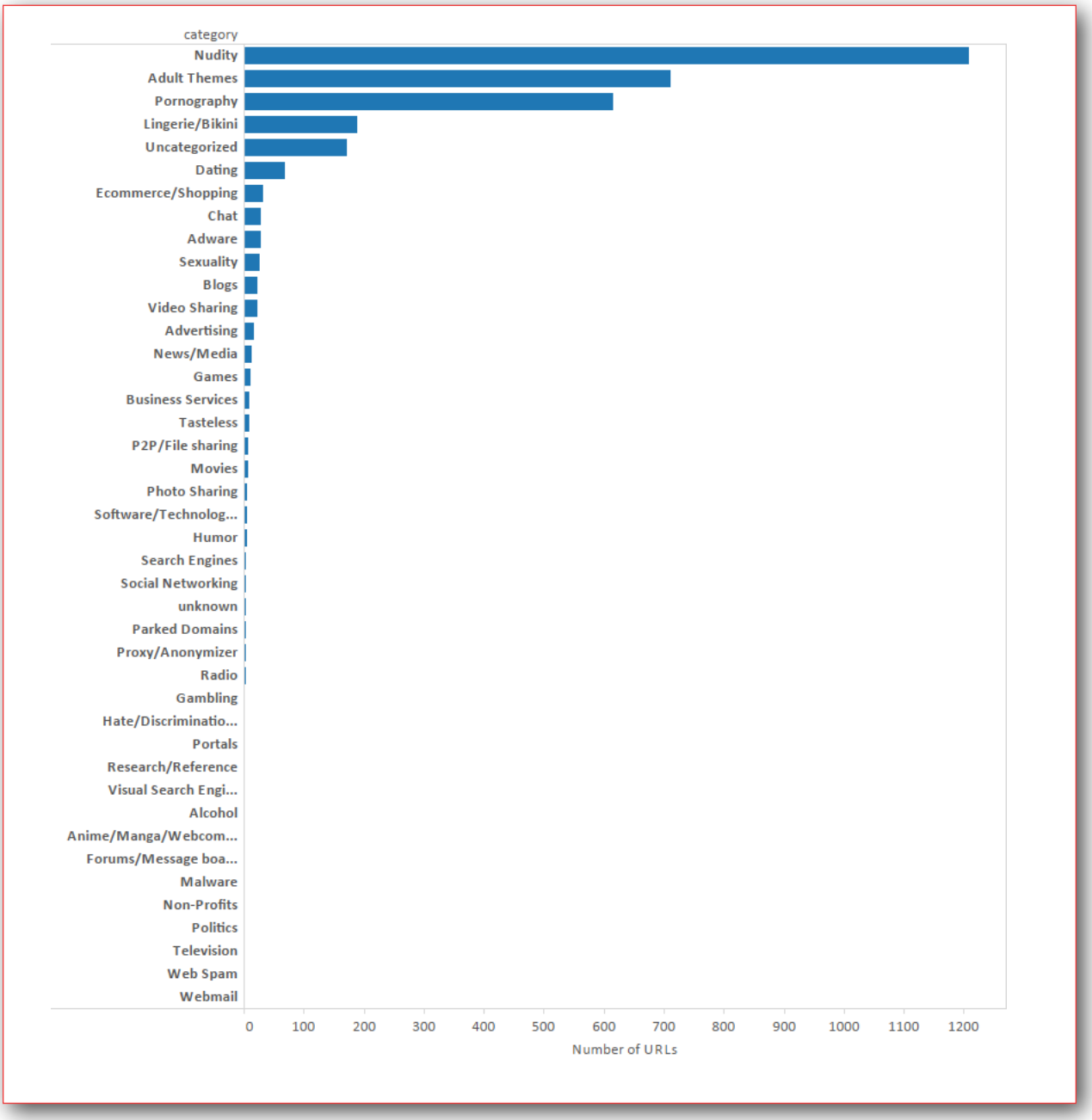


FIGURE 17: Alexa 200,000 top URLs blocked on SSID IGF2013@wifi.id per primary OpenDNS categorization.

During the IGF, the website for Freegate (www.internetfreedom.org), a circumvention tool, was found to be filtered on this network. On 21 October at 4:00 pm, a conference attendee notified network administrators about this blocked website, and by 11:00 pm the site was made accessible. The prompt response by network administrators and the ISP is an example of remediation for

potentially erroneous blocking, but also demonstrates an informal ad-hoc process.

ISP: IGF2013@Indosat
AS: INDOSATM2-ID
Netalyzer Results

Testing conducted on SSID: IGF2103@indosat (AS: INDOSATM2-ID) found 164 URLs blocked out of the sample of 1,387 URLs tested. These websites include LGBT content, independent media sites, critical religious content, gambling websites, and pornography. Websites found blocked included Free Speech TV (www.freespeech.org), Equal Marriage for Same-Sex Couples (www.samesexmarriage.ca), and the Indonesian religious site Faith Freedom (indonesia.faithfreedom.org/doc). The full list of URLs blocked on this ISP can be found here.

This ISP filters by DNS tampering, with all filtered domains resolving to the IP 124.81.92.132. After being redirected to this IP, users are served the block page seen in Figure 18.

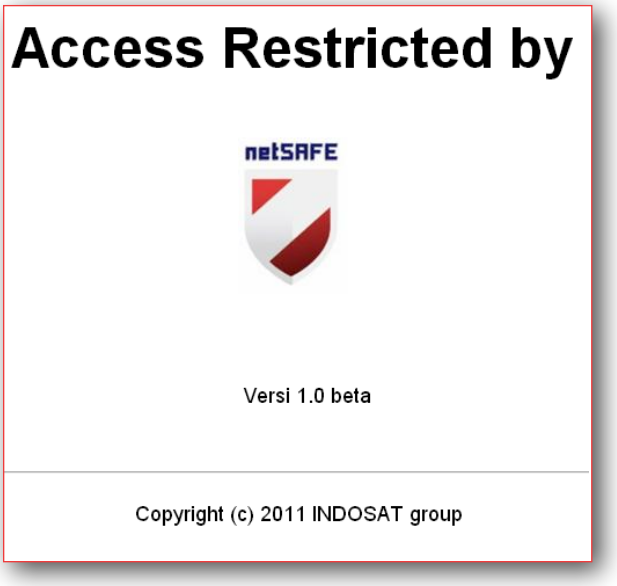


FIGURE 18: Block page observed on SSID IGF2013@Indosat.

This block page has the following HTML source:

```
<html>
<body>
<center>
<p>
<hr>
<font face="arial" size="15" color="black">
<b>Access Restricted by</b>
<p>
<img src="logo_netsafe.JPG" alt="netSAFE"></img>
<p> 
<font size="4">
Versi 1.0 beta
<hr>
<p> 
Copyright (c) 2011 INDOSAT group
</body>
</html>
```

Cross-ISP Comparison

Indonesia's highly decentralized filtering environment means that what content is filtered and how filtering is implemented can vary greatly between ISPs. Our results do show such a variation in filtering, although there is a general overlap in the types of content filtered. Our test results show that pornography, a putative focus of the filtering regime, is highly filtered on all ISPs, as is nonpornographic LGBT content. One notable area of difference is anonymizers and circumvention tools, which are heavily filtered on Telkmonet's IGF network while generally available on the other two networks.

A breakdown of the variation in filtered content between ISPs can be seen in Figure 19 (next page).

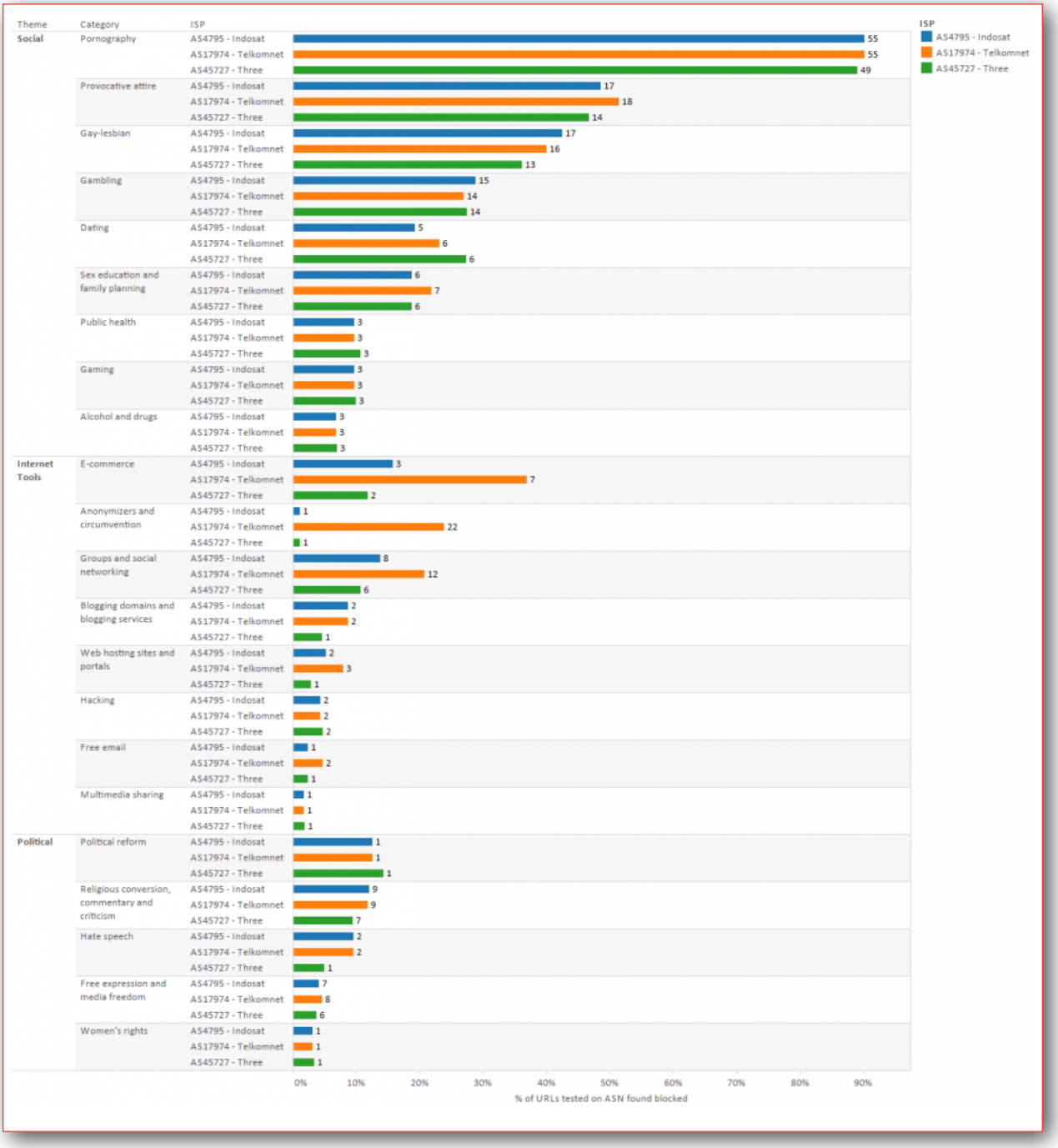


FIGURE 19: Proportion of tested URLs found blocked on each ISP, sorted by URL content category.

Figure 20 shows the variation and overlap in blocked content between the three ISPs.

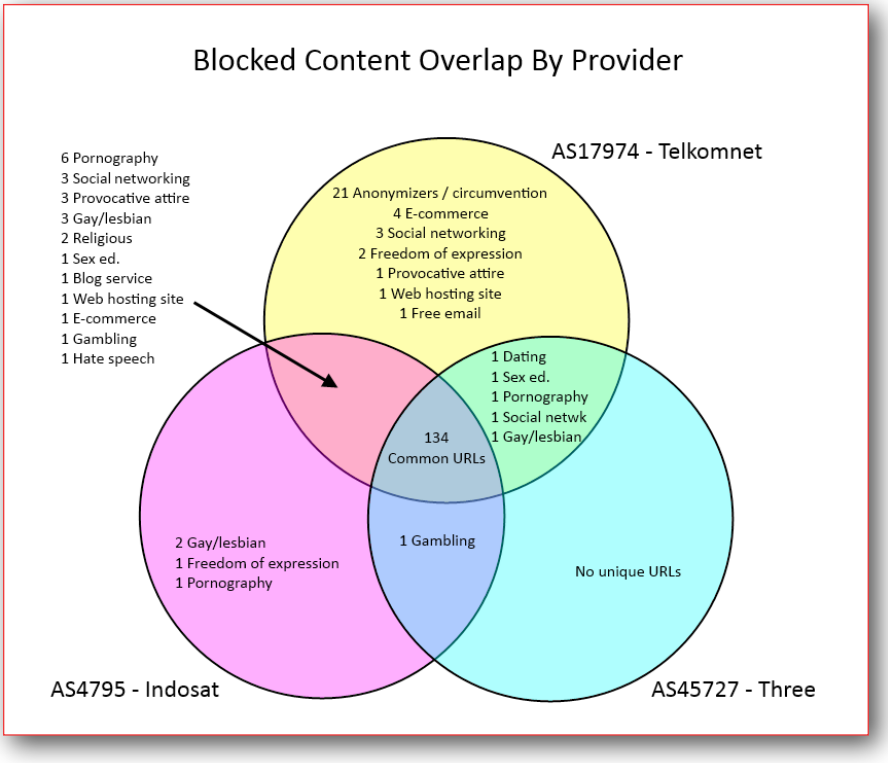


FIGURE 20: Venn diagram of number of URLs blocked between three ISPs, grouped by content category.

SUMMARY AND NEXT STEPS

The research and analysis presented here shows that an understanding of content controls requires a combination of methods and insights from both technical and qualitative approaches, and in particular perspectives from those who understand the social, political, cultural, and economic context of Indonesia. It is clear from the data we collected and the analysis we undertook that Indonesian content controls are exercised in a way that is inconsistent, lacks transparency, and includes numerous instances of over-blocking, or blocking of content far beyond what is publicly justified and discussed. Some of this over-blocking is the consequence of categorization errors; other examples appear to be the result of over-zealous compliance by ISPs, and still others the result of factors such as pressure and influence from government and non-ruling political parties. As Indonesian development in ICTs continues to progress rapidly, the lack of transparency, accountability, and clear process for content control will likely exacerbate tension among stakeholders operating in an uncertain environment.

DATA

Completed lists of URLs used for testing, and URLs found blocked through both remote and client-based tests can be found here:

GOOGLE DOC VERSION

https://docs.google.com/spreadsheet/pub?key=0Ah0XQ-1lDRPYdG9haWFseE9zZ3JsNzRKREJmZTQ4TUE&output=html

CSVS

- IGF2013@wifi.id URLs found blocked through in-country testing
- IGF2013@wifi.id URLs found blocked through OONI-probe testing
- IndonesiaIGF2013-IGF2013@Indosat-incountry.csv
- IndonesiaIGF2013-Nawala-dns.csv
- IndonesiaIGF2013-Tri-incountry.csv
- IndonesiaIGF2013-Global List.csv
- IndonesiaIGF2013-Indonesia local list.csv

EXPLORING COMMUNICATIONS SURVEILLANCE IN INDONESIA

Surveillance is one of the most effective, if less obvious, forms of information control. Governments and private companies engage in surveillance for a wide range of reasons, many of them beneficial for society. However, surveillance can also be used to target dissidents and undermine privacy. If surveillance is undertaken without proper accountability, it can lead to the abuse of power. Surveillance of the Internet and other communications is now a huge growth industry, with many companies supplying governments with passive and targeted surveillance products and services.

Citizen Lab research has documented the use of surveillance technologies, products, and services in Indonesia, including those designed for or capable of targeted (FinFisher) and passive (Blue Coat) surveillance. Additionally, smartphone maker BlackBerry (previously known as Research in Motion) has come under pressure from Indonesian authorities to locate back-end infrastructure within the country as a means of facilitating surveillance of users. BlackBerry, as well as other electronic service providers, has continued to be pressed by the Indonesian government to locate their data centres in Indonesia, in line with the government regulation 82 of 2012 on the Operation of Electronic Systems and Transactions.

This section summarizes Citizen Lab's prior research on surveillance in Indonesia, including documented evidence of FinFisher command-and-control servers and Blue Coat Systems devices on IPs owned by Indonesian ISPs. It also identifies recent trends in Indonesian surveillance practices, laws, and regulations that provide potential avenues for further research.

PRIOR RESEARCH: CENSORSHIP AND SURVEILLANCE IN INDONESIA

FINFISHER

Citizen Lab research has documented the use of surveillance technologies, products, and services in Indonesia. Since 2012, Citizen Lab researchers have revealed the presence of FinFisher command-and-control (C2) servers in thirty-six countries across the globe, including Indonesia. These findings have led to activists and advocacy groups in several countries launching legal complaints in national and international settings, including in

Pakistan, Mexico, the United Kingdom, and the OECD. We have translated a "fact sheet" about our findings from English to Malay and Indonesian.

FinFisher is a commercial surveillance toolkit that provides an attacker with remote control and access over a target's computer system. According to leaked promotional materials, FinSpy, a component of the FinFisher suite, is capable of exfiltrating data; intercepting e-mail, instant messaging, and VoIP communications; and spying on users through webcams and microphones. Captured information is then transmitted to a designated FinSpy C2 server. FinFisher is developed by Munich-based Gamma International GmbH. The UK-based Gamma Group advertises FinFisher as a suite of "governmental IT intrusion and remote monitoring solutions" and claims to sell exclusively to law enforcement and intelligence agencies.

In August 2012, Citizen Lab published *The Smartphone Who Loved Me: Finfisher Goes Mobile?*, in which researchers identified potential FinSpy C2 servers in ten countries by scanning IP addresses and fingerprinting for FinSpy's characteristic C2 protocol. Among the observed servers was an IP (112.78.143.26) owned by Biznet, an Indonesian ISP. Martin Muench, the managing director of Gamma Group, publicly denied that the scanned servers were connected to any component of the FinFisher suite.

In the March 2013 follow-up report *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab identified thirty-six FinSpy servers (thirty new, six previously identified) in nineteen different countries, many of which have a history of human rights violations. The report documented four additional C2 servers in Indonesia on three IPs belonging to ISPs Biznet (112.78.143.34), PT Matrixnet Global (103.38.xxx.xxx), and PT Telkom (118.97.xxx.xxx). During the course of this research, we found mobile-related evidence with a specific connection to Indonesia that is significant and deserves further scrutiny. The FinFisher product for mobile phones can send stolen data back using SMS messages. We found one sample of a mobile phone version of FinFisher that contained a phone number in Indonesia, which the spyware used to send stolen data back over SMS.

Our researchers did not know who was targeted with this particular sample, but infer that the people who were targeted were likely in Indonesia because the SMS number was there. Usually there is a charge for sending international text messages, which is levied by the telecom company that a user subscribes to. If charges for sending international text messages begin to appear on a phone bill, and the target knows they did not send those messages, they may become suspicious. Our researchers inferred from this reasoning that the use of an Indonesian phone number indicates that there are people in Indonesia who are targeted with FinFisher. The phone number we identified in the FinFisher sample was:

+6281310xxxxx4 – Indonesia

Although these findings have raised alarms among activists and media, it is important to be clear about several contextual points. The presence of FinFisher C2 server in a particular country is not necessarily proof that the government is responsible for purchasing or operating the FinFisher suite. Someone could be operating the C2 server from another jurisdiction, and using the location to mask attribution. Moreover, there are legitimate ends to which law enforcement and other government agencies might employ the FinFisher toolkit, such as legally "wiretapping" suspected criminals (i.e., with a judicial warrant). However, products used by law enforcement and government agencies for "lawful interception" become problematic in countries with weak rule of law and where dissident activities are viewed as criminal, or where military and intelligence agencies have a track record of targeting local populations or civil society. For example, the Citizen Lab has found evidence of FinFisher being used to target Bahraini activists as well as evidence of FinFisher campaigns with political content relevant to Ethiopia and Malaysia.

In response to Citizen Lab's findings, a spokesperson for Indonesia's Ministry of Communications and Information Technology (MCIT) stated that the ministry would evaluate the information and take "decisive action" if Biznet, PT Telkom, and other ISPs were operating surveillance software. The ministry further stated that any such act would constitute a violation of article 40 of Indonesia's Telecommunications Act, which explicitly prohibits unlawful eavesdropping on information transmitted over telecommunications networks. The implication that the ISPs themselves were responsible for the purchase of FinFisher software contradicts Gamma Group's claim to sell only to governmental entities.

BLUE COAT

Blue Coat Systems is a California-based provider of network security and optimization appliances with functionality permitting network filtering and surveillance. These include: ProxySG devices that work with WebFilter, which categorizes web pages to permit filtering of unwanted content; PacketShaper, a cloud-based networking management device that can establish visibility of over six hundred web applications and control undesirable traffic; and CacheFlow, a web-caching appliance that functions to optimize bandwidth. ProxySG provides "SSL Inspection" services to solve "issues with intercepting SSL for your end-users." PacketShaper has the ability to monitor and control network traffic: it is integrated with WebPulse, Blue Coat Systems' real-time network intelligence service that can filter application traffic by content category. CacheFlow can be configured to block content. While these Blue Coat products can be used to maintain and secure networks, they can also be used to implement politically motivated restrictions on access to information, and monitor and record private communications.

The Citizen Lab has conducted research on Blue Coat Systems products using a combination of wide-area scanning techniques, Shodan queries, and other experimental methods. Citizen Lab researchers have found Blue Coat devices on the public networks of eighty-three countries (twenty countries with both ProxySG and PacketShaper, fifty-six countries with PacketShaper

only, and seven countries with ProxySG only).

In a January 2013 report titled *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Citizen Lab discovered PacketShaper installations in Indonesia on the networks of both Indosat (http://202.155.63.62/) and PT Telkom (http://203.130.193.156/login.htm). The Citizen Lab also found installations of CacheFlow on PT Telkom (http://180.252.181.1). Citizen Lab researchers connected to the Blue Coat devices to confirm that they were active.

The presence of Blue Coat devices in a country does not necessarily imply that they are being deployed for surveillance. However, their presence raises substantial concerns, particularly in light of Citizen Lab finding FinFisher on three Indonesian ISPs as well as governmental pressure exerted on BlackBerry to locate its back-end servers within the country as a means of facilitating surveillance of users. Additional concerns revolve around the lack of rigorous independent oversight for Indonesia's State Intelligence Agency (Badan Intelijen Negara, BIN). In light of these findings and this context, further investigation is required.

Blue Coat Systems offers product certification courses through a number of "Authorized Training Centers," such as Red Education. Headquartered in North Sydney, Australia, Red Education offers courses on information technology and computer networking, and has training centres across the globe including in Jakarta. The company offers training courses in PacketShaper and ProxySG administration, as well as certification exams for Blue Coat proxy administrators and professionals.

TRENDS IN SURVEILLANCE AND FURTHER ISSUES FOR RESEARCH

BLACKBERRY

Indonesia is a significant market for Canadian telecommunications company and smartphone manufacturer BlackBerry Ltd. As of 2013, analysts estimated that approximately 15 million BlackBerry users are in Indonesia, accounting for almost 20 percent of all BlackBerry consumers worldwide.

In a multistakeholder meeting in January 2011, BlackBerry agreed to comply with four demands the Indonesian government stipulated, including the creation of domestic after-sales service centres, the establishment of network aggregators or servers on Indonesian soil, the implementation of government censorship requirements for Internet content, and an agreement to discuss the possibility of granting Indonesian law enforcement "lawful interception access" to key BlackBerry services. BlackBerry implemented the government's filtering requirements, established forty service centers, and claimed to have

fulfilled the "lawful interception" condition (i.e., will provide access to its network if a violation occurs) through coordination with Indonesia's Corruption Eradication Commission, but the company did not disclose further details about its implementation.

Despite BlackBerry's claims, the Indonesian Telecommunications Regulatory Body (Badan Regulasi Telekomunikasi Indonesia, BRTI) filed a complaint against the company for locating a key data centre in Singapore rather than Indonesia as requested. The BRTI threatened to shut down BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS), claiming that the use of servers in Canada to process BBM and BIS data threatened the security of Indonesian users. The Indonesian government has also argued that local servers are necessary for monitoring criminals and terrorists using the BlackBerry platform for communications.

Indonesia's requirement to locate servers within its borders reflects a trend BlackBerry encountered when it began operating in countries with significant controls over information. Concerns over monitoring citizens' communications have prompted the governments of Saudi Arabia and the United Arab Emirates to make similar demands of the company. Saudi Arabia and the United Arab Emirates also threatened to ban BlackBerry data and messaging services due to alleged security concerns. As with Saudi Arabia and the United Arab Emirates, Indonesia is facing the challenge of controlling information on devices whose traffic is processed outside of its jurisdiction. During an open discussion held by the Indonesian E-commerce Association (IdEA) in May 2013 in Jakarta, MCIT's Director General of Informatics Application, Ashwin Sasongko, said, "If the data centers are located overseas and there are issues, (Indonesian) law enforcement will face problems in getting to the data. Law enforcers cannot gain physical access because it is in another country." As of 2013, BlackBerry has not yet built a server inside Indonesia.

GAMMA TSE

Indonesia's military establishment has bolstered its surveillance capabilities through international partnerships and commercial purchases. From 2006 to 2008, the US government provided a USD 57 million outlay to Indonesia for the establishment of an Integrated Maritime Surveillance System (IMSS), designed to combat terrorism, smuggling, and piracy in Indonesian waters. The system includes surveillance cameras, surface radar, global position systems, and other combinations of sensors, devices, and technical platforms to monitor maritime traffic.

The Indonesian military recently purchased "unspecified 'wiretapping' equipment" from Gamma TSE. The undisclosed equipment will be used by the Indonesian military's Strategic Intelligence Agency. Privacy International described this deal as "deeply troubling" given the Gamma Group's previous commercial deals with authoritarian regimes and the Indonesian military's history of human rights violations. Members of Indonesia's House of Representatives also expressed concern that surveillance equipment could be abused in the run-up to the 2014

general election. The House Commission on Defense and Information warned the military not to use any purchased equipment for politically motivated surveillance.

LEGAL ENVIRONMENT AND SURVEILLANCE

As we mentioned in the section on infrastructure and governance, there are many laws that regulate interception and wiretapping in Indonesia. Figure 21 shows that at least twelve laws, two government regulations, and two ministerial regulations outline the practice of wiretapping by state institutions in the name of law enforcement. This is because communication interceptions today are usually carried out by law enforcement agencies to expose crimes, particularly organized and transnational crimes. In many of these cases, wiretapping was helpful, even necessary. However, they are also prone to misuse and may lead to violations of privacy without comprehensive legislation regulating their use.

In January 2013, Gatot S. Dewa Broto, the spokesperson for the MCIT, stated that the government as a whole is preparing a draft law on interception mechanisms (Rancangan Undang-Undang Tata Cara Intersepsi).

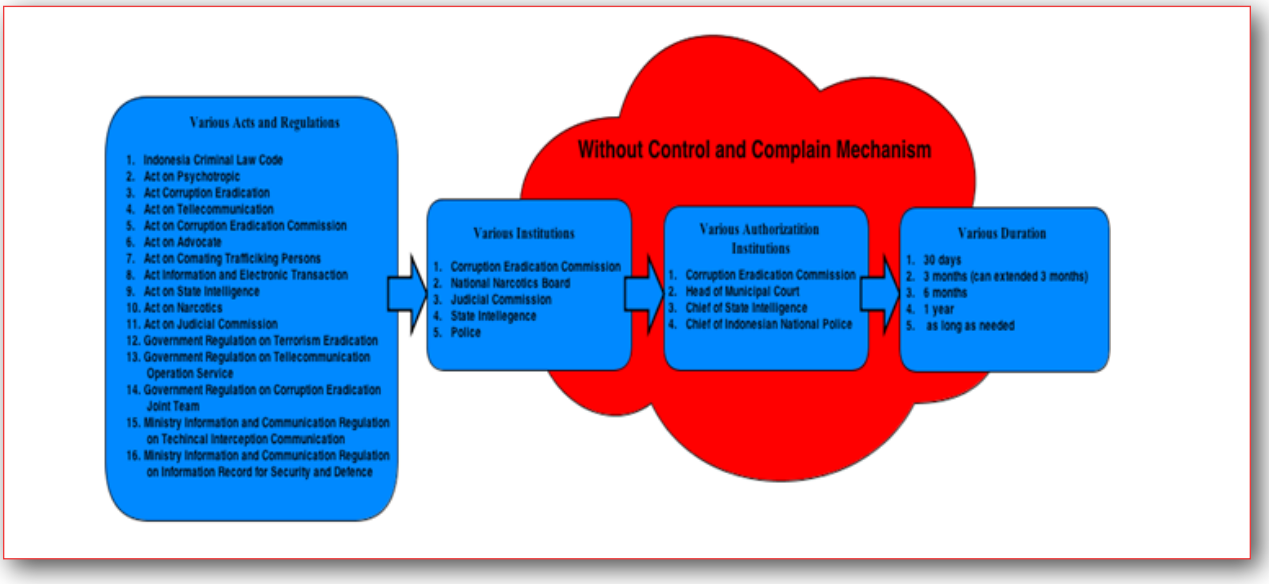


FIGURE 21: Various acts and regulations governing interception and wiretapping.[15]

However, prior to the attention the Constitutional Court generated by annulling article 31(4) in the Electronic Information and Transactions Act, the debate about interception was stirred by the enactment of Act No. 17 Year 2011 on State Intelligence, which was widely criticized for

15 Sinta Dewi Rosadi, Privacy International Draft Report, 2013.

granting broader authority, and not enough accountability, to the State Intelligence Agency to intercept communications. The Alliance of Independent Journalists, four nongovernmental organizations, and thirteen individuals subsequently filed a judicial review of the act at the Constitutional Court in Jakarta in January 2012. They were concerned with its vague and broadly defined articles, for instance, on the issue of "intelligence secrets," and the opportunity that it provides authorities to classify public information as state intelligence. These provisions imperil journalists because using or citing documents that had been classified could be deemed a crime. Certain articles also evoked fears of surveillance by "Big Brother," such as article 29 which gives the State Intelligence Agency power over foreigners or foreign institutions planning to take Indonesian citizenship, or visit, work, study, or open a representative office in the country. In October 2012, the Constitutional Court turned down the judicial review, arguing that the act "appropriately regulated intelligence practices in Indonesia."

The State Intelligence Law is one of at least nine laws that allows the authorities to conduct surveillance or wiretapping, and although a court order is required in most cases, there are concerns that permission will be granted too easily due to limits on judicial independence. Furthermore, surveillance techniques are most often deployed in Indonesia for combatting terrorism, but there is inadequate oversight or checks and balances in place to prevent abuse by those who are conducting the monitoring. The only other law that explicitly states the need for judicial oversight is the Law on Narcotics, but the requisite procedures for that oversight remain unclear.

AREAS FOR FURTHER RESEARCH

Surveillance is an unavoidable characteristic of cyberspace. The use of sophisticated data mining and analytical tools that collect, mine, and isolate network traffic has spread quickly. Likewise, the market for enhanced surveillance products and services has become a major and growing commercial segment.

Our research on Indonesia is not uncharacteristic of what we have seen in other countries today: the government faces urgent public policy issues around cybercrime, national security issues involving insurgencies, regional tensions, and omnipresent concerns about acts of terror. Not surprisingly, we would expect the government to develop or acquire advanced signals intelligence, computer network exploitation, and surveillance capabilities. At the same time, because of many technological systems' "dual-use" nature, we should not be surprised to find evidence of such technologies making their way into ISPs and telecommunication companies, and even the private businesses who use them for increasingly complex challenges of network management.
Key to this discussion will be the question of oversight, accountability, and transparency around surveillance – particularly surveillance involving government intelligence and law enforcement agencies. As findings emerge of products that can be used or repurposed to put civil society and others at risk, it is imperative that research is directed toward clarifying their end uses. Further research is clearly required to this end in Indonesia.

AN ANALYSIS OF THE 2013 IGF AND THE FUTURE OF INTERNET GOVERNANCE IN INDONESIA

The Internet Governance Forum (IGF) brings various stakeholder groups together to discuss public policy issues related to the Internet. The 2013 IGF took place in Bali, Indonesia under the overarching theme of "Building Bridges: Enhancing Multistakeholder Cooperation for Growth and Sustainable Development." For the country's vibrant civil society, the IGF presented a range of stakeholders with an opportunity to raise awareness, mobilize support, and shape the agenda. Now that the forum has concluded, however, challenges remain in building a progressive Internet governance agenda that realizes the right to freedom of expression and information.

A growing number of Indonesia's 240 million people use the Internet daily, whether to get around, to communicate with friends, or to get involved in social campaigns. Indonesia is quickly becoming the "social media capital of the world." The capital city of Jakarta is the most active Twitter city in the world and the country as a whole is the fourth most active on Facebook. The government, recognizing the importance of high-speed Internet to economic and social development, has committed to developing the country's information and communications technology (ICT) infrastructure by launching the "Indonesia Connected" program to boost connectivity in border and remote areas. Along with this development, however, came an increase in the government's concern over online content. While multistakeholder groups have participated in the often-contentious debate over what online content should be filtered, by whom, under what processes, and according to which laws, their impact on policy-making is uncertain.

As the section on infrastructure and governance discusses, Indonesia is currently drafting or revising a number of ICT-related laws that contain serious human rights implications. It is important, therefore, that elements maintaining respect for human rights are incorporated in the scope of these legislations. The Snowden revelations and a number of high-profile corruption cases in Indonesia have renewed calls for stricter regulations regarding wiretapping. The draft Information Technology Criminal Offence Law (Rancangan Undang-Undang Tindak Pidana Teknologi Informatika, TIPITI) has raised concerns for being too broad and containing harsher penalties than the controversial Electronic Information and Transactions Law (Undang-Undang

Informasi dan Transaksi Elektronik, EIT). After much criticism, the government is currently revising the EIT law, particularly article 45 which specifies the penalty for defamation as up to six years' imprisonment and fines of up to IDR 1 billion (approximately USD 106,000). The penalty has reportedly changed from six years to three, but the revision stopped short of decriminalizing defamation.

The Internet market in Indonesia is highly distributed and, as a consequence, the scope and depth of filtered content vary across over two hundred different ISPs. Recently, however, the Indonesian government has aimed toward more centralized systems. The independent Nawala Foundation provides a DNS server that enables service providers to block websites for pornography and gambling, among other categories. Its use is not compulsory for members of the Indonesian ISP Association (APJII), but it is encouraged. In addition, the Ministry of Communications and Information Technology (MCIT) maintains and endorses Trust+ Positif, a set of configuration files and block lists for the popular open source Squid HTTP proxy and the SquidGuard add-on, which is an open source implementation of URL access control lists for Squid. Trust+ Positif block lists include over 745,000 domain names and 55,000 URLs categorized as pornographic content. Because implementation has been inconsistent across service providers, the MCIT is preparing a draft Ministerial Decree on Controlling of Internet Websites with Negative Content (RPM Pengendalian Situs Internet Bermuatan Negatif) to establish a uniform mechanism and conditions for blocking and filtering.

The implementation of content controls in Indonesia has been criticized for a number of reasons. Representatives from the APJII have warned that the costs associated with implementing content-filter systems are burdensome for smaller ISPs and could potentially slow down Internet traffic. Also, our research has found that there have been instances of "mission creep" where websites containing religious issues and religious advocacy groups, and content related to sexuality and gender (e.g., local LGBT community websites), among other content categories, are also blocked. Civil society has criticized the government's opaqueness and unresponsiveness to their concerns, especially with regard to the Trust+ Positif system (e.g., which legislation governs the blocking mechanism of illegal content and the use of tools such as Trust+ Positif? If a website containing no illegal web content is blocked, what is the remedy mechanism? Who will pay for the costs incurred for monitoring and screening websites?). These concerns are made all the more serious when citizens are "very much invited" to participate in content control by forwarding URLs to an e-mail address or filling out a submission form (at the time of publication, this form was "under development").

CIVIL SOCIETY'S ROLE IN THE 2013 IGF

Civil society organizations play a key role in increasing awareness of citizens' rights online. ICT Watch, a member of the Cyber Stewards Network, as well as a number of other organizations such as Institute of Policy Research and Advocacy (ELSAM), Relawan TIK Indonesia (ICT Volunteers Indonesia), Center for Innovation Policy and Governance, and Hivos, launched the Indonesian CSO Network for Internet Governance (ID-CONFIG) in December 2012, which is a coalition of local civil society organizations (CSOs) that regularly dialogues on Internet governance issues. Under the banner of ID-CONFIG, civil society organizations participated actively in the 2013 IGF process. The steering and organizing committees, for instance, included ID-CONFIG, the government, and the private sector.

During the event's planning stages, the organizing committee faced delays in finalizing the host country agreement, as well as budgetary shortfalls (partially stemming from political turmoil following corruption allegations facing the Ministry of Communications and Information Technology), which threatened to see the event cancelled. The issue of funding for the 2013 meeting also sparked a more fundamental debate over how to fund the Internet Governance Forum generally. Following reports on social and news media that the Bali IGF would be cancelled due to a lack of funds, and a series of discussions on several mailing lists inquiring if this was really the case, the chair of the IGF Multistakeholder Advisory Group (MAG) and former IGF Executive Secretary, Markus Kummer, maintained that "the UN has not received any official confirmation that Indonesia is withdrawing its offer to host the 2013 IGF" and that "cancelling the whole event is no option." The group was eventually able to raise the funds, with domestic and international actors making financial contributions to cover the funding gap.

These different stakeholders coming together during the early stages of the event shaped how the 2013 IGF was constituted. The IGF has traditionally been a government-driven event because a substantial amount of funding is required to cover a host country's responsibilities, such as paying for the meeting venue and participant transportation, as well as the travel, per diem, and at-home replacement costs of UN staff, among other expenses. But the lack of government support provided the space for business and civil society communities to step up their roles in the forum's organization, and their influence could be seen throughout. For instance, in addition to fundraising for the event together, they suggested two overarching themes, "Internet Governance Towards Information Society Through Multistakeholder Participation" and "Internet Governance to Achieve Sustainable Development Through People's Participation." The theme that was adopted, "Building Bridges: Enhancing Multistakeholder Cooperation for Growth and Sustainable Development," contained the key words "multistakeholder" and "sustainable development," which were considered by these stakeholder groups as crucial components of Internet governance.

Civil society formed an integral part of the 2013 IGF Secretariat, responsible for running the

event, which meant that they were in charge of creating and maintaining the website and determining the distribution of resources among participants (e.g., nine booths were allocated to civil society versus seventeen in total for government and private sector representatives). The secretariat worked with the Penabulu Foundation, a Hivos partner organization, who introduced measures to ensure financial transparency and accountability, such as standard operating procedures for auditing and reporting. During the event, a number of workshops such as "Civil Society and Internet Governance Multi-Stakeholder Engagement Practices from Southeast Asia and Beyond" and "Social Media for Social Movement: How Civil Society Can Optimize the Internet to Conduct Online Public Advocacy of Human Rights" were organized by civil society groups. The IGF pre-event, traditionally organized as a ministerial meeting, was broadened in scope and was referred to this year as the High-Level Leaders Meeting (HLLM). Over seventy civil society participants were invited to the HLLM, three of whom were speakers—including Citizen Lab's Director Ron Deibert—compared to only two speakers each from government and the private sector. Indonesia's Minister of Communications and Information Technology's statement at the HLLM was drafted with input from civil society. Following the event's conclusion, the 2013 IGF narrative report was drafted by civil society, including the Citizen Lab.

Citizen Lab staff and associates have participated in every IGF since the first meeting was held in Athens in 2006, as well as the WSIS meetings that preceded it in 2003 and 2005. At the 2005 WSIS meeting in Tunis, Citizen Lab researcher Nart Villeneuve's presentation on Internet filtering was disrupted by Tunisian authorities and nearly cancelled. Moreover, our participation in the 2009 IGF in Egypt included having the book launch for the OpenNet Initiative's *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* interrupted by United Nations' officials, following complaints by Chinese government representatives concerning our reference to Tibet and the Great Firewall of China in our published material. In contrast, the Citizen Lab was able to participate freely and openly at the 2013 IGF, including hosting a press conference on the preliminary findings of this report, which discussed at length Indonesia's content filtering and surveillance regimes.

LOOKING FORWARD

The IGF provided a springboard for Indonesian civil society organizations, working together with other stakeholder groups, to rally behind pressing Internet governance issues such as censorship and surveillance. The influence that civil society had on the 2013 IGF has been lauded as a model for how multistakeholder participation can operate at these events. We hope that the momentum of pushing for greater protection of the basic principles of human rights in Internet governance in Indonesia can be maintained, and that the multistakeholder process can be sustained well past the event.

The government is working toward building ICT infrastructure and services to connect the archipelagic country from Sabang to Merauke. Indonesia's youthful population ensures that technologies like the Internet are being adopted quickly. By the end of 2013, Indonesia's Internet penetration rate is expected to reach 33 percent, or roughly 80 million users. The business community's role is crucial in ensuring that the growth in accessibility and Internet usage is achieved. For this development to happen, the country's legal and regulatory framework must be consistent, greatly simplified, and harmonized to make it less burdensome and more transparent for business. These goals can be achieved by encouraging greater government accountability and transparency.

Indonesia, as a founding member of the Open Government Partnership (OGP), has committed to a model of government that is "sustainably more transparent, more accountable, and more responsive to their own citizens." The OGP pledge can be extended to the Internet governance sphere by the government's collaboration with fellow stakeholders, such as businesses and civil society, when designing Internet-related policies, as well as creating mechanisms to facilitate and deepen this cooperation. For instance, while the government has held focus group discussions of early drafts of legislations, civil society has called for these discussions to be more transparent (e.g., recorded and made public), and for the government to ensure that relevant feedback is incorporated into the final drafts.

One of the more urgent concerns the Indonesian government faces is cybercrime, and the population is becoming even more aware of its impact. A recent Akamai report indicated that the number of cybercrime incidents in the country is growing significantly. It is unsurprising, therefore, that Indonesia is involved in a number of regional initiatives to combat cybercrime. In 2011, the Association of Southeast Asian Nations (ASEAN) met in Bali to discuss transnational crime, recognizing that the organization should jointly combat cybercrime. The ASEAN Senior Officials Meeting on Transnational Crime met in Vietnam in 2013 to reconfirm its commitment to fighting crime in the region, and concluded with an endorsement for a working group on cybercrime. The Asia-Pacific Economic Cooperation (APEC), of which Indonesia is a member, is working to ensure cooperation on combatting cybercrime through the Security and Prosperity Steering Group's "Cybercrime Experts Group", which is designed to

"promote and improve cooperation among member economies in the fight against cybercrime." Cybercrime issues are also expected to be discussed at the ninth World Trade Organization (WTO) Ministerial Conference to be held in Indonesia in December 2013. Commentators are urging the WTO to help global victims of cybercrime and economic cyber espionage through clear "guidelines and penalties." Unless a balance is maintained between national security concerns and lawful procedures and oversight mechanisms, these initiatives run the risk of adversely affecting civil liberties and human rights.

As development continues apace, civil society has an important role to play in engaging the general public, government, and private sector to ensure that Indonesia's Internet governance regime respects and protects basic principles of human rights. Achieving this balance requires constant monitoring and continuously reexamining policies and practices, and a proactive engagement with like-minded domestic and international stakeholders. With the impending establishment of the ASEAN Economic Community in 2015, it is expected that there will be more consolidated collaboration in the area of cybercrime and cyber security. Together with our colleagues in the region, we will be monitoring developments in the country's Internet governance agenda closely and we support one that promotes democracy, human rights, transparency, and accountability.

Download the PDF version at citizenlab.org

UNIVERSITY OF TORONTO
MUNK SCHOOL OF GLOBAL AFFAIRS
Canada Centre for Global Security Studies