Excerpt from ronald j. deibert’s the geopolitics essay

Whereas once it was conventional wisdom to believe that the internet’s technological infrastructure was immune to control, today states and corporations are applying an ever-increasing level of skill and technological sophistication to precisely that mission. The result is that rather than being a single seamless environment, the internet a user connects to and experiences in Canada is far different than an internet a user experiences in Iran, China, or Belarus.

This chapter provides an overview of the geopolitics of internet control, and in particular state efforts to control information flows across borders, with comparative data from over 22 countries.

Earlier the same year, Tunisian authorities filtered the popular video-streaming service, DailyMotion. DailyMotion is known to carry a wide range of political videos, ncluding many satirical videos of the Tunisian government’s record on human rights. Many interred that Tunisia nad blocked the website because ot those videos, following its known track record of blocking access to opposition and human rights websites (Reporter Without Borders, 2007).

However, Tunisia uses (but does not openly admit to doing so) the U. S. commercial filtering product, Smartfilter, to block its citizens’ access to information (OpenNet Initiative, 2005a).

DailyMotion was, perhaps mistakenly, categorized within the Smartfilter database as “ pornographV’” a category apparently 323 RONALDJ. DEI BERT elected by Tunisia for blocking. After reports of the DailyMotion block surfaced, Smartfilter apparently corrected the categorization error, and

access to the DailyMotion website from within Tunisia was gradually restored.

The source for much of the evidence and illustrations used in this chapter comes from the research of the OpenNet Initiative (ONI)” collaboration among the Citizen Lab at the University of Toronto, the Berkman Centre for Internet and Society at Harvard Law School, the Cambridge Security Programme, U. K. , the Oxford Internet Institute, and partner non-governmental organizations (NGOs) worldwide.

The aim of the ONI is to document empirically patterns of internet censorship and surveillance worldwide using sophisticated means of technically interrogating the internet directly.

The ONI’S tests are carried out both remotely from North America and the U. K. , and in-field by dozens of local researchers.

Our reports over the last several years have documented a disturbing increase in the scale, scope, and sophistication of internet censorship practices worldwide. 2 This chapter summarizes some of the main findings of this research and draws connections to wider implications for global politics, security, nd human rights. The main questions addressed by this chapter are: how many states are filtering access to information on the internet?

What are the types of content that these states are targeting for filtering? What are the most effective methods used by states that filter? What is the range of transparency and accountability practices among states that filter? Are states open about their practices? And, what are some of the wider

implications of these practices? As will be described in this chapter, the picture of the internet that emerges from this research is of a hotly contested and deeply politicized realm. 324 Beneath the surface of internet communications What happens to a request when a user clicks on a link to a website or sends an e- mail?

For most surfers, the internet experience begins and ends with what happens on the computer screen in front of them. However, if surfers follow that e-mail or web request as it leaves a computer and passes down the fiber optic cable to the servers and routers of a local internet service provider (ISP), through the internet exchange points (IXPs), international gateways, and on to the undersea trunk cables of tier 1 telecommunication companies, they will find a complex and largely hidden nfrastructure of filters and chokepoints.

Most people assume that the internet’s vast intrastructure is an open, decentralized, network ot networks through which information flows freely along a shared routing protocol. While this description has some basis in the historical evolution of the internet, and captures parts of what makes it unique, it also obscures some of the details that structure internet communications beneath the surface. While it is true that there is no single node through which all traffic passes on the internet, and thus no form of centralized ontrol, there are thousands of nodes that parse out and filter information and act as gateways.

Each of these nodes and gateways” from routers to IXPs to autonomous systems” present opportunities for authorities to impose order on internet

traffic through some mechanism of filtering and surveillance. Some of this control takes place for technological reasons; some of it takes place for cultural, political, and economic reasons. Instead of a network of networks, therefore, it is perhaps more accurate to characterize the internet as a network of filters and chokepoints.

The means by which content is blocked or filtered on the internet vary

CE NSORS widely in terms of complexity, effectiveness, and intent. Furthermore, not all of the means by which states attempt to control the internet are technological. In some cases, regulations are employed to supplement technical controls, which can create a climate of self-censorship among internet users. The following section defines some of the central terms associated with internet content filtering and surveillance before turning to specific examples of accountability and transparency issues.

Internet content filtering is a term that refers to the techniques by which control is imposed n access to information on the internet (Delbert and Villeneuve, 2004). Content filtering can be divided into two separate techniques: address blocking techniques and content analysis techniques.

Address blocking techniques refer to particular router confgurations used to deny access to particular internet protocol (‘ P) addresses and/or domain names, or specific services that run on particular port numbers.

For example, a state may run a blocking filter at the international gateway level that restricts access from within the country to websites that are deemed illegal, such as pornographic or human rights websites. Content

Analysis refers to techniques used to control access to information based on its content, such as the inclusion of specific keywords on a website or the address of a URL. Because parsing mechanisms employ keywords to block access, they are often the source of mistaken or unintended blockages.

Unintended blocking can occur as a result of IP based blocking as well, however, as it is not uncommon for many domain names to share the same IP address. Filtering that aims to block access to a specific website by blocking its IP address, in other words, can result in the collateral filtering of otentially thousands of unrelated sites sharing the same ‘ P. Depending on need implemented: ; and circumsta nce, different approaches to tiltering can Inclusion filtering: users are allowed to access a short list of approved sites, known as a “ white list,” only. All other content is blocked.

Exclusion filtering: restricts user access by blocking sites listed on a “ black list.

” All other content is allowed. Content analysis: restricts user access by dynamically analyzing the content of a site and blocking sites that contain forbidden keywords, graphics, or other specified criteria. The mechanisms used to do these types of filtering vary considerably. Routers act as junctions between networks, passing information packets back and forth, and thus routers are the main (though not only) nodes where such blocking takes place in the form of instructions written into the routing tables.

However, filtering software can be implemented into virtually any node throughout the internet’s system. As a consequence, the level at which filtering can be implemented varies widely too. Filtering can take place on an

individual’s personal computer, an office local area etwork (LAN), an internet caf©, an ISP, a wireless network, an SMS system, at the backbone or international gateway level, or some combination of all of these levels. Not surprisingly, nationallevel internet content filtering can vary dynamically, and across ISPs within a single country (Anderson and Murdoch, 2007).

Although filtering traditionally takes place by blocking requests for information from either reaching their destination or returning the requested information at information chokepoints, other nonflltering mechanisms can be employed that achieve the same ends.

After ll, filtering is simply denial of access to information. 325 Methods of investigating censorship Although filtering practices are widespread, knowledge of their use by states has tended to be limited. In part, this is a function of a lack of accountability and transparency among states that block access to information.

In part, however, it is also a function of the lack of empirical evidence about such practices.

Up until recently, the majority of reports on internet filtering tended to emerge from users, news reports, or advocacy organizations. Not surprisingly, they tended to be nsystematic and sometimes even unreliable. Moreover, because ot the complex and varied ways in which filtering can be implemented, as noted earlier, reports 326 -6 41 (h (e bk bk)) As is described below, new forms of blocking access to information are emerging based on the use of distributed denial of service attacks.

Such attacks bring web servers down by overwhelming them with requests for information, thus “ filtering” information at its source and denying access to all users equally. The same type of denial of service can (and occasionally does) take place by cutting off power to the uilding where web servers are located, or misconfguring routing tables to cause what appear to be network errors, but which in fact are deliberate attempts to shut off communications at the source.

As the Google Earth example demonstrates, filtering can also take place through reverse geolocation” that is, the server hosting websites can refuse to take requests from users based on the geographical origin of their computer’s IP address. The ONI has documented numerous instances of this type of reverse geolocation filtering, including by the website georgewbush. com during the 2004 U. S. Presidential Elections (ON’, 2004).

have often been made in error or have contained contradictory information.

The aim of the ONI has been to overcome these shortcomings by developing a systematic way to investigate empirically internet filtering practices from within state borders over an extended period of time. The project employs a unique methodology that combines infield investigations by partners and associates who travel to or live in the countries concerned, and a suite of technical interrogation tools that probe the internet directly for forensic evidence of content filtering and filtering technologies.

These tools work from the “ inside out” of the internet, probing parts of the information infrastructure not generally apparent to the average user. The methods range from automating connecting requests to servers hosting

websites simultaneously from within the country under investigation and a control location in a non-filtered location, to using tracing and other network mapping tools to interrogate the location of and technologies used to do the filtering. Tests for accessibility to internet content were based on categorized lists of websites.

These ategories were meant to cover as comprehensively as possible the likely targets for filtering by states while allowing for as precise as possible identification of content categories singled out for filtering. While most states that filter target pornographic content, as will be shown later a wide range of non-pornographic, political content” such as opposition parties or minority rights, for example” is now being targeted as well by several states.

This method allows for a comprehensive picture of internet content filtering in a particular country by probing all aspects of the national nformation infrastructure (internet caf©s, ISPs, wireless networks, backbone gateways) and over an extended period of time testing accessibility in both English and local languages to lists of thousands of websites in each of these categories. 5 Since 2002, the project has produced detailed reports on 1 1 countries” Belarus, Yemen, Tunisia, Burma, Singapore, Iran, China, Bahrain, United Arab Emirates, Vietnam, and Saudi Arabia.

More recently, in 2006 the ONI conducted extensive tests over several months in more than forty countries worldwide.

The following sections highlight some of the ain trends and findings emerging from this research. The globalization of online censorship In 2002, only a handful of countries were known to engage in internet content

filtering, most prominently China, Iran, and Saudi Arabia. By 2007, 26 of 40 examined countries were found to engage in internet filtering practices to some degree.

China is still the world’s most notorious and sophisticated censoring regime (ON’, 2004, 2005a, b, c, d; Dowell, 2006; L’, 2003; L’, 2004). Its filtering system comprises multiple levels of legal regulation and technical control, the latter implemented primarily at he backbone level using specially confgured Cisco routers. The system involves numerous state agencies and thousands of public and private personnel, and a dense web of everthickening legal restrictions.

The range of information that China seeks to limit and control from within its borders is broad.

China targets content for filtering across every major category tested, including human rights, opposition and independence and secessionist movements, minority faiths, pro-democracy groups, search engines, free e-mail and webhosting services, anonymizers and circumventors, pornography and sexually explicit material, and others. However, China is not alone. Although many countries Justify their censorship practices as a way to block access to pornography or other culturally sensitive material, our research has documented a large and growing swathe of content beyond pornography that is targeted for filtering.

At least 14 countries blocked access to content that spans the major categories of political, social, and conflict/ security content, including Burma, China, Ethiopia, Iran, Oman, Syria, Thailand, Tunisia, United Arab Emirates

(IJAE), Uzbekistan, Vietnam, Pakistan, Saudi Arabia, Sudan, and Yemen (See Figure 23. 1). Some of the countries in which we found evidence of content filtering in each of these major categories began by blocking only a few select sites in one category, usually pornography. After a period of time, however, the scope of content targeted for filtering began to increase to other content areas.

In Thailand, for example, what started out as an effort to block pornography has been gradually broadened to include politically sensitive websites as well, particularly since the September 2006 military coup. In addition to pornographic content, Thailand blocks access to the popular video streaming service, YouTube.

om, ostensibly in response to a single video posted on the service satirizing the deposed King. Pakistan began filtering websites that contain imagery offensive to Islam, and now targets all sites related to the Balochistan independence movement as well .

The Thai and Pakistan cases are illustrative of what may be a more general trend: that is, once the tools of censorship are put in place, the temptation for authorities to employ them secretly for a wide range of ulterior purposes may be large” particularly in circumstances where there is little civilian oversight or accountability” a phenomenon we refer to as nternet censorship “ mission creep. ” A number of other countries were found to be engaged in less pervasive forms of internet filtering, typically concentrated 327 Figure 23.

1 Content filtering by major category.

Source: Far’s and Villeneuve, 2006. 328 around a single content area or contentious internet service. For example, in addition to blocking some gambling and pornographic sites, ISPs in South Korea block access to all websites related to North Korea. India blocks access to websites related to extremist and militant groups, particularly those associated with Hindu and Islamic xtremism. A number of Middle Eastern and Gulf Countries, including Syria, Jordan, IJAE, Bahrain, and Saudi Arabia, block access to the entire Israeli (.

11) domain (see also Warf and Vincent, 2007).

Though having strict controls over traditional media and heavy penalties for libel, Singapore blocks access only to a small handful of pornographic websites (see also Rodan, 1998). Following the Thai and Pakistani examples above, we might hypothesize that over time these states will likely use their filtering systems to block a growing body of content. Increasing censorship sophistication Not surprisingly, the methods used to do internet content filtering have become more sophisticated, as states and the firms that sell censorship and surveillance technologies continually refine them. There are several examples of increasing sophistication.

First, authorities are becoming increasingly adept at targeting newly developed modes of communication, such as blogs, SMS, chat, and instant messaging protocols, and voice over internet protocol (VOIP) services.

In the past, such newly devised methods of information sharing could be used as a means to circumvent internet censorship. However, today authorities are becoming more adept at targeting new media and developing

methods particular to such services. Second, although content filtering is prone to overblocking and error, there are examples where authorities have been able to use such technologies with precision.

A good example is China’s targeting of the specific string of codes embedded in the URL of the Google cache function.

The latter is a service provided by Google whereby users can connect to archived information from websites stored on Google’s servers, rather than on the servers of the original website. The service was designed to provide a way to access information through redundancy, but it is also a very simple and effective way to get around content filtering. Since users connect to Google servers rather than to the blacklisted servers, they bypass the content filters.

Upon learning of this technique, China implemented a blocked string on their backbone/gateway routers that prevented any use of the Google cache function from within China. A third example of increasing sophistication of content filtering is the targeting of local languages and websites of opposition movements and dissidents particular to a pecific national context.

Tests from within China comparing the top 100 Google search results for keywords in English and Chinese show a very significant disproportionate amount of keywords are filtered when they are searched for in Chinese as opposed to English (ON’, 2005b).

For example, a search for the terms “ Chinese Labor Party’ in Chinese yields a 93 percent inaccessible rate when compared to the same search

performed in English, which yields only a 20 percent inaccessible rate. Iran, in 2005, showed a similar relationship among English and local language filtering (ON’, 2005c). In the case of Iran, many of the blocked websites in various categories had a higher percentage of inaccessibility in Farsi as opposed to English.

Overall, 80 percent of the Farsi-language websites tested were inaccessible whereas 45 percent of English-language sites were inaccessible. Such localization filtering” where “ international” sources of information are left accessible while local variants are blocked” may at first seem counterintuitive.

However, there are two potential explanations. First, localization filtering targets those groups that matter most to regime stability and power, such as local opposition movements and dissident roups presenting contentious information in languages spoken by citizens within the country.

Second, the disproportionately open access to Englishlanguage international sites can give the impression that access to global information is wide open, particularly to foreign Journalists who do not speak local languages. Authorities can point to contentious human rights and news sites and say that they allow access to information while blocking relatively more obscure sites from a global perspective that matter most in local politics. The tests conducted across 40 countries in 2006 rovided further confirmation that state content filtering tends to concentrate on local content and websites.