2018

Planet Netsweeper

Jakub Dalek

Lex Gill

Bill Marczak

Sarah McKune

Naser Noor

See next page for additional authors

Authors

Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jonathon Penney, Adam Senft, and Ronald Deibert

PLANET NETSWEEPER

By Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert

APRIL 25, 2018
RESEARCH REPORT #108

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Suggested Citation

Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. "Planet Netsweeper," Citizen Lab Research Report No. 108, University of Toronto, April 2018.

Acknowledgements

Thanks to Elizabeth Gross, Gabrielle Lim, and Bahr Abdul Razzak for research assistance; Masashi Crete-Nishihata, Christopher Parsons, Jeffrey Knockel, and Geoffrey Alexander for peer review; Andrew Hilts and Miles Kenyon for website, layout, and communications support; and to the entire team at OONI and ICLab. Thanks to Censys and Shodan for providing access to their data. Financial support for Citizen Lab's research on information controls is provided by the John D. and Catherine T. MacArthur Foundation, the Ford Foundation, Open Society Foundations, Oak Foundation, and the Sigrid Rausing Trust.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Part One: Summary 7

Part Two: Background 9

How does Internet filtering work? What are middleboxes? 9
About Netsweeper, Inc. 11
How Netsweeper's Internet filtering systems work 11
Prior Citizen Lab research on Netsweeper 13
Communications with Netsweeper 14

Section 1- Methodology & Technical Findings 16

1.1 Research Questions 16
1.1.2 Countries of interest 16
1.2 Methodology 17
1.2.1 Developing a list of IP addresses of Netsweeper devices 18
1.2.2 Filtering our list of IP addresses 20
1.2.3 Identify content blocked by Netsweeper installations 23
1.3 General Technical Findings 26
1.3.1 Netsweeper installations 27
1.3.2 What is blocked? 30
1.3.3 Beacon Box tests 31
1.3.4 Host Header tests 32
1.3.5 Miscategorization 34
1.3.6 Blocking content by country 38

Section 2- Country Cases 39

2.1 Summary 39
The countries of interest 39
2.2 Afghanistan 41
2.2.1 Background 41
2.2.2 Information controls in Afghanistan 42
2.2.3 Data analysis 42
2.3 Bahrain 45
2.3.1 Background 45
2.3.2 Information controls in Bahrain 46
2.3.3 Data analysis 47

Contents

2.4 India 50
- 2.4.1 Background 50
- 2.4.2 Information controls in India 50
- 2.4.3 Data analysis 51

2.5 Kuwait 57
- 2.5.1 Background 57
- 2.5.2 Information controls in Kuwait 57
- 2.5.3 Data analysis 58

2.6 Pakistan 63
- 2.6.1 Background 63
- 2.6.2 Information controls in Pakistan 63
- 2.6.3 Data analysis 64

2.7 Qatar 67
- 2.7.1 Background 67
- 2.7.2 Information controls in Qatar 67
- 2.7.3 Data analysis 68

2.8 Somalia 70
- 2.8.1 Background
- 2.8.2 Information controls in Somalia 70
- 2.8.3 Data analysis 71

2.9 Sudan 73
- 2.9.1. Background 73
- 2.9.2. Information controls in Sudan 73
- 2.9.3. Data analysis 74

2.10 UAE 77
- 2.10.1 Background 77
- 2.10.2. Information controls in UAE 77
- 2.10.3 Data analysis 78

2.11 Yemen 84
- 2.11.1 Background 84
- 2.11.2 Information controls in Yemen 85
- 2.11.3. Data analysis 86

Section 3- Discussion & Conclusions 89

3.1 Summary 89

3.2 The international human rights framework applicable to filtering technologies 90

Contents

3.3 Corporate social responsibility issues for Internet filtering companies 92
3.3.1 Applying human rights and corporate social responsibility considerations in the case of Netsweeper 94
3.4 Netsweeper's relationship with the Canadian government 98
3.5 What are Canada's obligations? 99
3.5.1. Canada's responsibility for the human rights impact of domestic companies operating abroad 100
3.6 Recommendations for the Canadian government 102
3.6.1 Greater due diligence: financial incentives and transparency 102
3.6.2 Empower the new Canadian Ombudsperson for Responsible Enterprise 105
3.6.3 Make it easier for human rights victims to seek redress in Canada 106
3.6.4 Export transparency and controls 108
3.7 Conclusion 109

Key Findings

- Using a combination of publicly available IP scanning, network measurement data, and other technical tests, we identified Netsweeper installations designed to filter Internet content operational on networks in **30 countries**
- We then used other data points associated with these installations, including in-country measurements, to narrow our list to those installations that appear to be filtering content for national-level, consumer-facing ISPs in ten countries of interest: **Afghanistan, Bahrain, India, Kuwait, Pakistan, Qatar, Somalia, Sudan, UAE, and Yemen**
- We found that Netsweeper technology is being used to block access in these ten countries to a wide range of digital content protected by international legal frameworks, including **religious** content in Bahrain, **political** campaigns in the United Arab Emirates, and **media** websites in Yemen
- We identified a pattern of mischaracterization and/or over blocking involving the use of Netsweeper's systems that may have serious human rights implications, including blocking Google searches for keywords related to **LGBTQ identities** and blocking **non-pornographic** websites in various countries on the basis of an apparent miscategorization of these sites as 'Pornography'
- We raise issues with the nature of the categories delimited by Netsweeper for the purpose of filtering, including the existence of an **'Alternative Lifestyles'** category, which appears to have as one of its principal purposes the blocking of non-pornographic **LGBTQ** content, including that offered by civil rights and advocacy organizations, **HIV/AIDS prevention** organizations, and LGBTQ media and cultural groups. We also note that Netsweeper can be configured to block access to websites from **entire specified countries**
- The international deployment of this **Canadian-made** filtering technology raises a number of **human rights**, **corporate social responsibility**, and **public policy** concerns and questions. These questions include whether and to what degree Netsweeper undertakes due diligence with respect to sales of its technology to jurisdictions with problematic rights records, and whether the Canadian government should be assisting Netsweeper, financially or otherwise, when its systems are used in a manner that negatively impacts internationally-recognized human rights

Part One: Summary

Internet filtering technologies play a critical role in shaping access to information online. Whether we are connecting to the Internet from our homes, coffee shops, libraries, or places of work, software that inspects, manages, and/or blocks our communications has become commonplace. When used at the level of large, consumer-facing Internet Service Providers (ISPs), Internet filtering technologies can have significant human rights impacts. A growing number of governments employ Internet filtering systems at this scale in order to undertake national-level censorship of the Internet. Filtered content ranges from pornography, hate speech, and speech promoting or inciting violence, to political opposition websites, news websites, websites affiliated with various religions, and everything in-between.

The growing responsibilities among network operators to filter content, either within private enterprises or on public networks, have given rise to a large and lucrative market. One industry report estimated the value of the web content filtering market at $3.8 billion USD by 2022. While network operators can manually configure their infrastructure to block specific websites or applications, the task can be time-consuming, complicated, and ineffective. Internet filtering companies provide professional services to ISPs and other clients to take care of this responsibility. Typically, Internet filtering companies dynamically categorize Internet resources and then let their clients choose pre-selected content categories or services that they wish to block. Customers can also add custom lists of their own to content that is filtered or blocked. In the hands of authoritarian regimes, such professional services can limit the ability of citizens to communicate freely and help impose opaque and unaccountable controls on the public sphere.

This report presents our latest research into the Internet filtering company Netsweeper, Inc. Netsweeper is a privately-owned technology company based in Waterloo, Ontario, Canada. The company has branch offices in India, Netherlands, the United Arab Emirates, and the United Kingdom, and distributors in Australia, the Middle East, South America, and the United States. As part of our ongoing research into Internet censorship practices and the filtering technologies that support them, Citizen Lab has issued several prior reports on Netsweeper, in which we identified installations on public networks in Bahrain, Pakistan, Qatar, Somalia, United Arab Emirates, and Yemen. Citizen Lab has developed a distinct fingerprint for Netsweeper installations over the course of this research, allowing us to identify such installations with high confidence. Additionally, Netsweeper is of particular

research interest given that it is a Canadian company, encouraged by the Canadian government and society to "reflect Canadian values" in its operations.

For this report, we used network measurement methods to map the entire Internet for Netsweeper installations. We identified 30 countries in which Netsweeper installations were present, and, of those, we focused on ten countries that raise systemic human rights concerns: **Afghanistan, Bahrain, India, Kuwait, Pakistan, Qatar, Somalia, Sudan, UAE, and Yemen**. (Our full data set can be accessed here.)

Several objectives guided our research. First, we wanted to develop and refine network measurement methods that allow us to verify Internet filtering service installations, such as those sold by Netsweeper. Citizen Lab has used these methods for many years as part of our research into Internet censorship and surveillance, and there is a growing scholarly community employing these research methods. One contribution we make in this report is to show how data collected from outside (i.e., through remote scans and publicly available datasets) and inside a country (i.e., principally through tests that make use of the OONI probe system) can be combined to verify Netsweeper installations and their behaviors. Our search for Netsweeper installations included scanning every one of the billions of IP (Internet Protocol) addresses on the Internet to identify responses from those addresses that match a signature we developed for Netsweeper.

Second, we wanted to raise awareness about Internet censorship practices, and the technologies that support them, so that negative human rights impacts can be identified and mitigated. Generally speaking, corporate social responsibility (CSR) practices among companies in the digital security space are immature, and Netsweeper in particular has published or communicated very little to suggest the company has implemented CSR measures. Yet business enterprises like Netsweeper have responsibilities under international human rights law to respect human rights. Such responsibilities involve ensuring due diligence measures are used to identify, prevent, and mitigate any impacts their operations have on human rights; public transparency about those measures; and ensuring remedial action if negative impacts are identified. Netsweeper has provided little information about any such measures, systems, or policies. Meanwhile, our research has verified that Netsweeper installations are used in several countries to implement Internet censorship in ways that undermine internationally-recognized human rights.

The Government of Canada also has important obligations under international human rights law to protect human rights and require Canadian businesses to

engage in due diligence to avoid causing or contributing to negative human rights impacts. The Government also has a duty to provide effective remedies for human rights victims. Canada has taken a strong public stance in support of human rights in the digital environment, yet at the same time Canadian government entities have assisted Netsweeper in developing its international trade presence and export sales. Such assistance has occurred despite the human rights implications of Netsweeper's business activities abroad. We offer concrete recommendations to the Canadian Government on how to better meet its obligations around these issues.

The major sections of the report are as follows:

Section 1- Methodology & Technical Findings

Section 1- Methodology & Technical Findings details the research questions that informed our study, our network measurement methodology, and technical findings.

Section 2- Country Case Studies

Section 2- Country Case Studies focuses on ten countries with problematic human rights records and/or particular security or public accountability challenges in which we identified Netsweeper installations on large public-facing ISPs.

Section 3- Discussion & Conclusions

Section 3- Discussion & Conclusions examines some of the legal, regulatory, corporate social responsibility, and other public policy issues raised by our report's principal findings. We focus on the responsibilities of Netsweeper and the obligations of the Canadian government to protect human rights and, then, suggest measures that stakeholders could take to mitigate negative human rights impact associated with Internet filtering technology.

Part Two: Background

How does Internet filtering work? What are middleboxes?

A network administrator tasked with restricting access to Internet resources has many different options available, each with their own strengths and weaknesses. One of the more simplistic ways to block access to a website is to change the site's domain name system (DNS) record to point to an IP address that will not return any content, or will return a "blockpage" (e.g., a page saying "this website is blocked"). Users can circumvent this blocking technique by changing the DNS settings on their device.

Another approach an administrator can use to filter access to Internet resources is to block the IP address of a website, such as by using a null route. This technique is imperfect because the site may share its IP address with many other (unrelated) websites. Thus, blocking an IP address can have the unintended consequence of blocking many other websites. Furthermore, a website blocked by this technique can circumvent the block by changing its IP address, or by using IP addresses from a service like Cloudflare, which is complicated for governments to block as content delivery services are widely used by corporations to deliver their content.

DNS blocking and IP address blocking can typically be conducted without adding additional hardware or software to a network, and both are relatively easy to circumvent. More sophisticated techniques are available if an administrator purchases and installs a middlebox on their network. A middlebox is a specialty network device, appliance, or software that inspects network traffic and performs some action upon traffic that matches certain characteristics, such as throttling, dropping, or redirecting data traffic being sent to, or received from, sources that are being filtered or censored.

A middlebox is normally installed in between ISP subscribers and the outside Internet. A middlebox may employ a deep packet inspection (DPI) technique to attempt to classify traffic belonging to certain encrypted apps or features (e.g., virtual private networks [VPNs] or voice-over-Internet-protocol [VoIP] applications) by examining various properties of packet flows. Thus, DPI techniques can be used to block services like WhatsApp voice calling while allowing unrestricted access to WhatsApp text messages. Many companies sell DPI-enabled middleboxes for a variety of "network management" purposes, including website caching, blocking viruses and spam, and enforcing usage quotas. A middlebox might also be purpose-built to filter web traffic to designated URLs, such as Netsweeper's product.

Circumventing middlebox-based blocking can sometimes be challenging. In theory, using a VPN or other circumvention applications can circumvent middlebox censorship, although DPI middleboxes can block many types of these applications. Citizen Lab has investigated the role played by DPI middlebox products from two companies– Blue Coat and Sandvine— in censorship and surveillance in its past reports.

About Netsweeper, Inc.

Netsweeper, Inc. develops an Internet content filtering product, also called Netsweeper, which is used by telecommunications companies, educational institutions, and governments. The company's promotional material describes the product as a means of protecting against malicious or inappropriate content, meeting compliance and regulatory requirements, and protecting sensitive information.

How Netsweeper's Internet filtering systems work

Netsweeper differentiates its product from other filtering tools on the market based on its "real-time web content categorization" technology. Given the highly dynamic nature of the Internet, manually maintaining lists of categorized web content is impractical. The company uses automated scanning and categorization techniques to maintain a large database of websites; each of these websites is assigned to a category based on its contents. A network administrator need only select a given content category– such as 'Gambling' or 'Hate Speech'– and all content categorized as such will be blocked. Creating this database of websites and the ongoing process of categorization is a substantial undertaking. The company claims it has categorized over 10 billion URLs and that it categorizes 22 million new URLs each day.

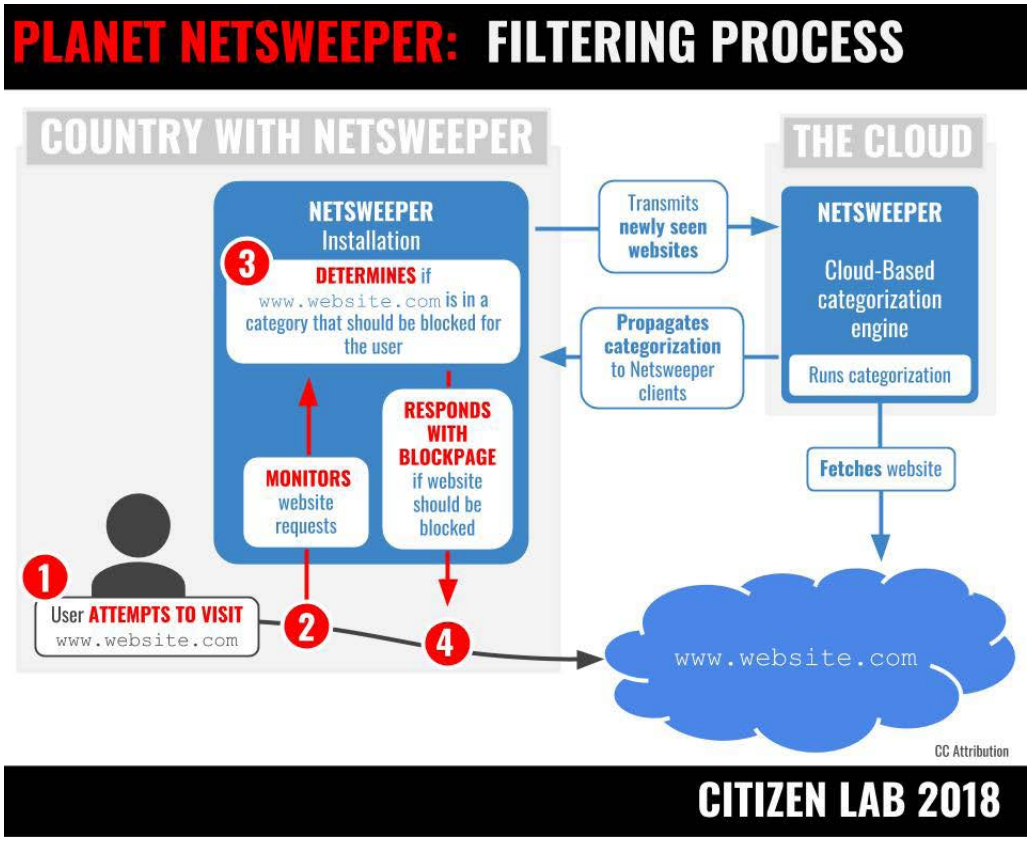

Figure 1. The Netsweeper Filtering Process

Netsweeper's content categories cover a wide range of web content, providing censors an easy and automated mechanism to bulk-filter entire content categories. ISPs and telecom operators can choose which of these categories they want to block but can also add their own categories and URLs manually. The comprehensiveness of the content categories suggests how pervasive Internet filtering can be. It also shows how a commercial company can aid national-level Internet censorship by providing technology and also by defining the parameters of permissible content retrieval– and thus access to information– through automated categorization.

Netsweeper's predefined content categories include:

Abortions	General News	No Text	Search Keywords
Adult Image	Hate Speech	Nudity	Self Help
Advertising	Host is an IP	Occult	Sex Education
Adware	Humour	Parked	Social Networking
Alcohol	Images	Pay to Surf	Sports
Alternative Lifestyles	Infected Hosts	Peer to Peer	Streaming Media
Arts and Culture	Intimate Apparel	Phishing	Substance Abuse
Classifieds	Intranet Servers	Phone Cards	Technology
Criminal Skills	Investing	Political	Tobacco
Culinary	Job Search	Pornography	Travel
Directory	Journals and Blogs	Portals	Under Construction
Education	Legal	Profanity	Viruses
Educational Games	Malformed URL	Real Estate	Weapons
Entertainment	Match Making	Redirector Page	Web Chat
Environment	Matrimonial	Religion	Web E-Mail
Extreme	Medication	Remote Access Tools	Web Proxy
Gambling	Network Timeout	Safe Search	Web Storage
Games	Network Unavailable	Sales	
General	New URL	Search Engines	

Part of our research in this report is intended to enumerate content category choices, censored content, and any other network behaviour on large consumer-facing ISPs in a particular country where we have identified Netsweeper installations. It is important to note that Internet content filtering is dynamic and variable and that it changes whenever a network administrator decides to update its local installation. Our tests do not provide exhaustive lists of censored content but, instead, provide representative samples that are a snapshot in time coinciding with our testing periods.

Our data collection and testing can reveal whether particular content categories are chosen, as well as whether URLs are added to a custom list and whether those choices are undertaken transparently or not (i.e., undertaken with some clear notification to users). In some instances, when a request is made for censored content, a blockpage is returned to the user that explains the reason why the content is blocked. In other cases, however, the user experiences a "time-out," which may give the mistaken impression that something is wrong with the connection or that the content is no longer available. Internet censorship is most insidious when it involves the latter approach, because users cannot ascertain why information is inaccessible.

Prior Citizen Lab research on Netsweeper

Citizen Lab began research into the use of Netsweeper technology in 2011. That year, as a part of the OpenNet Initiative project, we published a report that documented the use of Netsweeper technology to filter content on consumer-facing ISPs: "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011." This report documented the use of Netsweeper installations to censor content on three regional ISPs: Qtel (Qatar), du (UAE), and YemenNet (Yemen). The Yemen case was particularly notable because prior to using Netsweeper services, the ISP, YemenNet, used the WebSense filtering software. WebSense discontinued service to YemenNet for violating policies against government-mandated censorship following the publication of our report.

In June 2013, Citizen Lab published "O Pakistan, We Stand on Guard for Thee." That report described the use of Netsweeper technology to filter websites relating to human rights, sensitive religious topics, and independent media on Pakistan's largest ISP, PTCL.

In February 2014, we published "Internet Filtering in a Failed State: The Case of Netsweeper in Somalia," which documented the presence of Netsweeper technology on the networks of three Somalia-based ISPs. The use of filtering technology in Somalia– a country with a history of contested authority, under the influence of a radical insurgency, and considered one of the world's 'failed states'– raised significant human rights concerns.

In October 2015, we published "Information Controls During Military Operations," which analysed information controls during the Yemen armed conflict. This report found that Netsweeper installations were being used on the networks of state-run YemenNet, the country's largest ISP, to filter critical political content, independent

media websites, and all URLs belonging to the Israel (.il) top-level domain. This censorship occurred at a time when YemenNet was under the control of the Houthis, an armed rebel group who had taken over the Yemeni capital in September 2014.

In September 2016, we published the report "Tender Confirmed, Rights at Risk: Verifying Netsweeper in Bahrain," which documented the use of Netsweeper technology on nine Bahrain-based ISPs. The Netsweeper installations appeared to have been activated several months after the release of a public tender by Bahrain's Telecommunications Regulatory Authority that indicated Netsweeper had won a bid to provide a "national website filtering solution." Testing on the ISP Batelco showed that the Netsweeper installation was being used to filter content relating to human rights, political opposition websites, Shia websites, local and regional news sources, and content critical of religion. The report noted that the use of Netsweeper technology to filter protected speech in Bahrain was particularly problematic given the country's ongoing political crisis and record of human rights abuses against oppositional political figures and human rights activists.

Communications with Netsweeper

As a standard part of our research process for most of these reports, we sent Netsweeper a letter that described our findings, presented a series of questions regarding the use of Netsweeper technology in these countries, and committed to publishing their response in full alongside our research report. Netsweeper did not respond to any of our letters. However, in January 2016 the company filed a defamation suit against Citizen Lab director, Professor Ronald Deibert, and the University of Toronto with the Ontario Superior Court of Justice, seeking $3,500,000 in general and aggravated damages following the publication of our 2015 report on the use of their technology in Yemen. Netsweeper discontinued its claim, in its entirety, in April 2016.

Prior to the publication of this report, Citizen Lab sent a letter to Netsweeper on 10 April 2018. The letter notified the company of our intention to publish a report and described our key findings. It also offered to "publish any response you would like to provide to this letter in its entirety alongside that report." On 12 April 2018, Netsweeper CEO Perry Roach replied by email acknowledging receipt and indicating a response would be forthcoming.

On 23 April 2018, Netsweeper responded through counsel with a document titled, "Media Release: Netsweeper responds to media enquiries regarding international

operations," sent to Citizen Lab and individual journalists. While Netsweeper stated that it "welcomes the opportunity to clarify the conduct of its operations," the media release did not address any of the questions Citizen Lab posed to Netsweeper. Rather, it asserted that Citizen Lab's questions did not sufficiently meet Netsweeper standards to merit answers:

> **"Netsweeper has always and remains fully compliant with Canadian law and in those countries where it has ongoing concerns. We appreciate receiving analysis and questions that meet professional tests of sound technological understanding and balanced interpretation."**
>
> **"It is our view the information and questions provided to Netsweeper fail adequately to meet those tests."**

At the same time, however, the media release appeared to acknowledge that Netsweeper does face corporate social responsibility dilemmas inherent to the provision of Internet filtering products:

> **"Netsweeper cannot prevent an end-user from manually overriding its software. This a dilemma shared by every major developer of IT solutions including globally renowned corporations that make the internet work. Our firm's technology and its applications are fully disclosed in the public realm. Even the most elementary review of our posted material shows that Netsweeper's design does not include any organic functionality to limit the online content Mr. Diebert [sic] highlights."**

Netsweeper's acknowledgement that IT companies face a dilemma is a step in the right direction and advances the conversation on corporate social responsibility. However, the company provided no further detail within the media release to explore the exact nature of this dilemma. For example, it did not address issues concerning the conduct of human rights due diligence to limit sales that would present significant human rights risks in the first place; the establishment of rights-oriented policies or procedures (which other companies within this market have adopted — see Section 3.3); or the existence of the 'Alternative Lifestyles' and 'Countries' filtering categories, which do appear to represent "organic functionality to limit the online content" as highlighted by Citizen Lab. Puzzlingly, this statement also seems to suggest that the company views the censorship effects noted by Citizen Lab as resulting from misuse of its technology, given the characterization of the end-user deployment as "manually overriding its software," rather than operating the technology as designed.

Section 1- Methodology & Technical Findings

This section details the research questions that informed our study. We also outline in detail the methods that we adopted to identify Netsweeper installations worldwide, and those that we employed to reduce the findings to countries of interest. We also present high-level technical findings and observations.

1.1 Research Questions

Our research for this report was guided by the following questions:

1) Can we identify all Netsweeper installations on the Internet? What technical methods and tools can we use to do that?
2) What tools and methods can we use to confirm which of these Netsweeper installations are on the networks of consumer-facing ISPs?
3) Are any of the installations that are identified on consumer-facing ISPs located in jurisdictions in which their use represents a human rights concern?
4) What can we say about how censorship is applied by the installations found in jurisdictions associated with human rights concerns? What types of content are censored? How is it censored? How transparent is such censorship to users? What is the legal and regulatory framework governing censorship in these jurisdictions?
5) Can we confirm if the installations found in jurisdictions that are associated with human rights concerns are actively serviced by Netsweeper, Inc.?

1.1.2 Countries of interest

Netsweeper has customers around the world. While our prior research has focused on the use of Netsweeper technology in countries of the Global South, the company also has customers in the Global North, including Canada, where it is headquartered, and in the United Kingdom, where it opened an office in 2017. Many of the purchasers of Netsweeper products are institutional customers, particularly in the education sector, where the company advertises compliance with both U.S. (CIPA) and U.K. (OFSTED) guidelines regulating children's access to online content. Other customers in these countries include private companies seeking to control employee access to the Internet.

Our primary research interest pertains to the filtering of content on consumer-facing ISPs. In most cases, filtering on consumer ISPs does not have an opt-out option, which leaves users with no alternative for accessing blocked content (unless they are able to switch to a non-filtering provider). This same dynamic is not at play in the case of employees or students who experience website or Internet blocking in an institutional or a corporate setting. As a result, we have chosen to exclude institutional and private-sector Netsweeper installations from deeper analysis.

We further focus on countries that routinely violate human rights in areas of free expression, as we think that these countries are more likely to abuse filtering technologies to restrict access to political or human rights content. We selected countries ranked as "Authoritarian" by the 2017 Economist Democracy Index and added other countries that are not ranked as "Authoritarian," including India, Pakistan, and Somalia, because of the unique history and characteristics of Internet filtering in the countries. India has a long and complex history with Internet filtering that has been the subject of many contentious public debates. Historically, Pakistan has censored the Internet extensively, including blocking all of YouTube in 2008. Somalia is a failed state torn by insurgencies and persistent violence.

1.2 Methodology

Our technical methodology is divided into three phases. In the first phase, we *collected* a list of IP addresses that might be associated with Netsweeper installations. In the second phase, we *filtered* our list to include only bona fide Netsweeper installations deployed on consumer ISPs in countries of interest. In the third phase, we *examined* what content these Netsweeper installations were blocking and whether they may have been communicating with Netsweeper, Inc.

Purpose	Methods	Data Source
Develop a list of IP addresses of Netsweeper installations	Searching existing Internet scanning data sources	Censys, Shodan
Develop a list of IP addresses of Netsweeper installations	Searching existing Internet censorship data sources	OONI, ICLab, Packet captures, Ad hoc testing
Filter our list of IP addresses to bona fide Netsweeper installations on consumer-facing ISPs	Remotely scanning the IP addresses	Specialized scanning

Purpose	Methods	Data Source
Identify content blocked by these Netsweeper installations	Searching existing Internet censorship data sources	OONI, ICLab, Packet captures, Ad hoc testing
Identify content blocked by these Netsweeper installations	Remotely scanning IP addresses in countries of interest using HTTP Host headers aimed at triggering censorship	Host Header test
Identify whether the Netsweeper installation may be communicating with Netsweeper, Inc.	Running our Beacon Box test	Beacon Box test

Table 1.1. Our methodology

1.2.1 Developing a list of IP addresses of Netsweeper devices

We developed our list of IP addresses by examining existing Internet scanning data from two sources and existing censorship measurement data from two sources.

Existing Internet scanning data

Shodan and Censys are two platforms that probe most Internet-connected devices at regular intervals and make the results publicly accessible. In previous work, we developed various signatures for how Netsweeper devices respond to the probes that Shodan and Censys send. We queried these services daily for results matching our fingerprints. **Figure 1.1** shows the specific queries we sent to Shodan and Censys.

```
# WebAdmin
censys: 80.http.get.title: “Netsweeper Business”

censys: 80.http.get.title: “Netsweeper SMB”

censys: 80.http.get.title: “Netsweeper School”

censys: 80.http.get.title: “Netsweeper Cloud Manager”

censys: 80.http.get.title: “Netsweeper Manager”

censys: 80.http.get.title: “Netsweeper Webadmin”

### Common include in HTML source for WebAdmin

censys: “/webadmin/common/templates/”

## 403 Forbidden Redirects to /webadmin/

censys: “You don’t have permission to access /webadmin/ on this server” AND 443.https.tls.
certificate.parsed.names: “localhost.localdomain”
```

```
## 302 webadmin headers for Shodan

shodan: “/webadmin/redirect/index.php”

## Config Manager runs on alternate port in old versions

shodan: “Netsweeper Configuration Manager”

# Deny Page

censys: “/webadmin/deny/index.php”

censys: “The site you have attempted to visit is restricted.”

shodan: “/webadmin/deny/index.php”

# SNMP Sigs

shodan: “.el5.netsw”

shodan: “.el6.netsw”
```

Figure 1.1. Signatures used to identify Netsweeper installations in Censys and Shodan search

The IP addresses we collected provide a broad picture of publicly visible Netsweeper installations, including both public ISP installations, and institutional and private sector installations.

Existing Internet censorship data

The Open Observatory of Network Interference (OONI) and Information Controls Lab (ICLab) collect data on Internet filtering and network interference from vantage points all around the world by convincing volunteers in various countries to run specialized measurement tools. The tools include web connectivity tests that attempt to access lists of potentially censored content, collect the resulting responses, and then analyze them for evidence of censorship. OONI and ICLab data are both publicly searchable.

We searched OONI and ICLab data using signatures (**Figure 1.2**) that we developed in our prior work to identify additional Netsweeper installations.

```
OONI
1. Download all web_connectivity JSON result files for a given day
2. Look for the regex: ‘<iframe src=.*?\?dpid=\d&.*?></iframe>’ in each JSON
3. If a JSON file matches, then parse the JSON and get all URLs in which the body response
   contains the regex from Step 2
4. Further see if we can parse Netsweeper URL query parameters by checking if either of
   the following regexes match:
```

a. '\?dpid=(.+)&dpruleid=(.+)&cat=(.+)&ttl=(.+)&groupname=(.+)&policyname=(.+)&username=(.+)&userip=(.+)&connectionip=(.+)&nsphostname=(.+)&protocol=(.+)&dplanguage=(.+)&url=(.+)"\swid'

b. '\?dpid=(.+)&dpruleid=(.+)&cat=(.+)&dplanguage=(.+)&url=(.+)"\swid'

5. If the blockpage is a domain, resolve that domain to an IP address

ICLab

1. Download all "http_" results provided for 2017-06 to 2017-08
2. Look for either of the following strings:
   a. "\?dpid="
   b. "/webadmin/deny"
3. If the blockpage is a domain, resolve that domain to an IP address

Figure 1.2. Signatures used to identify Netsweeper installations in OONI/ICLab data.

We included the blockpage IP addresses in our list of IP addresses of possible Netsweeper installations. We also used OONI and ICLab data (**Section 1.2.3**) to identify blocked websites.

1.2.2 Filtering our list of IP addresses

We next sought to narrow our list of IP addresses (Section 1.2.1) to bona fide Netsweeper installations filtering content on consumer-facing ISPs. We first ran probes against each IP address to see whether the IP was associated with a bona fide Netsweeper installation. Second, we probed each IP to see whether the installation was on a consumer-facing ISP.

Is the IP address a bona fide Netsweeper installation?

We ran a variety of tests to answer this question, described in **Table 1.2**.

Question to be answered	Data source	Value suggestive of Netsweeper installation	Test code
Do the headers for a request for the IP address show a direction to http://<IP address>/webadmin?	Headers from HTTP HEAD request to http://<IP address>	Redirection to http://<IP address>/webadmin	b1

Question to be answered	Data source	Value suggestive of Netsweeper installation	Test code
Is the redirect from a previous data point followed by a redirect to http://<IP address>/webadmin/redirect?	Headers from redirection to http://<IP address>/webadmin	Redirection to http://<IP address>/webadmin/redirect	b2
Does an attempt to access http://<IP address>/webadmin return a valid page?	HTTP GET request to http://<IP address>/webadmin	Valid page	b3
Does an attempt to access http://<IP address>/webadmin/alert return a valid page?	HTTP GET request to http://<IP address>/webadmin/alert	Valid page	b4
Does an attempt to access http://<IP address>/webadmin/deny return a valid page?	HTTP GET request to http://<IP address>/webadmin/deny	Valid page	b5
Does an attempt to access http://<IP address>:8081/auth/Login.action return a valid page?	HTTP GET request of http://<IP address>:8081/auth/Login.action	Page containing copyright notice: “2009 Netsweeper Inc.”	b6
Does the sysdesc SNMP value of the IP address contain the string “.netsw”?	Public GET of SNMPv2 value: “SysDescr”	E.g. “Linux NS-WebAdmin 2.6.32-358.2.1.el6.x86_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86_64”	b_snmp
Does a reverse DNS resolution of the IP address suggest that the IP address belongs to a Netsweeper installation?	Reverse DNS lookup on the IP	A domain name which is indicative of a Netsweeper installation (e.g. nsfilter2.spg.more.net)	rdns
Does the page returned from /deny define CSS templates which suggests a Netsweeper installation?	HTTP GET request from http://<IP address>/webadmin/deny	“Shared” “Webadmin2012” “Webadmin2016”	css
Does the /deny page include a “mailto” link which suggests it is a Netsweeper installation?	HTTP GET request of http://<IP address>/webadmin/deny	HTML page body contains “mailto:” link suggestive of Netsweeper	denypage_mailto

Question to be answered	Data source	Value suggestive of Netsweeper installation	Test code
Does the page returned from /deny contain an HTML title which suggests a Netsweeper installation?	HTTP GET request from http://<IP address>/webadmin/deny	"Access Denied"	denypage_title

Table 1.2. Summary of data points collected to validate potential Netsweeper installations. The "Test code" values are referenced in the data analysis of our country case studies in Section 2.

Discussion of tests

In general, we considered an IP address to belong to a bona fide Netsweeper installation if the following Boolean expression was matched:

```
b_snmp || (b1 && b2) || b6 || (b1 && b3 && b4 && b5)
```

The *b_snmp* test, which checks whether the SNMP `sys_descr` value contains the string "`.netsw`", is a very good indication that Netsweeper software is installed, as this string is unlikely to appear in servers not running software developed by Netsweeper. Similarly, the b6 test tells us whether or not a visit to the path: "/auth/Login.action" on port 8081 returns a page with a copyright notice of "2009 Netsweeper Inc."

We do not weight some of the other tests as highly, as they could be matched by non-Netsweeper products. For instance, test *b1* only measures whether a direct visit to the IP address redirects to the path: `/webadmin`. It seems conceivable that non-Netsweeper products could match this test, as "webadmin" is a common word. The tests *b3* to *b5* all return true if any page is returned in response to their respective queries. A web server that is configured to respond with HTTP 200 to any request would likely return "True" to all these tests. However, it is less likely that a non-Netsweeper server would be in our initial list of IP addresses, because of how we generated that list (**Section 1.2.1**).

The *rdns, css, denypage_title,* and *denypage_mailto* tests do not have Boolean return values. Therefore, the strength of these tests depends on how clear the value returned is in regards to potentially identifying the function of the server. For example, if the deny page title was "Netsweeper – Blocked," it would be a strong indicator of a Netsweeper installation; if the title was "Not Found," that would be a weak indicator.

Is the installation on a consumer-facing ISP?

We ran a variety of tests to answer this question, described in **Table 1.3**.

Question to be answered	Data source	Value suggestive of consumer-facing ISP
Does the page returned from /deny contain links to domains which suggest who is responsible for administering the installation?	HTTP GET request from http://<IP address>/webadmin/deny	"nsblock.<ISP NAME>.com"
Does a reverse DNS resolution of the IP address suggest who is responsible for administering the installation?	Reverse DNS lookup on the IP	A domain name which is indicative of the administrator of the installation (e.g: restrict.kw.zain.com)
Does the sysdesc SNMP value of the IP address suggest who is responsible for administering the installation?	Public GET of SNMPv2 value: "SysDescr"	E.g. "Linux NS-WebAdmin 2.6.32-358.2.1.el6.x86_64 #1 SMP Wed Mar 13 00:26:49 UTC 2013 x86_64"
Does the /deny page include a "mailto" link which suggesting who is responsible for administering the installation?	HTTP GET request of http://<IP address>/webadmin/deny	HTML page body contains "mailto:" link indicative of the installation's administrator
Do the OONI or ICLab measurements for this installation show a blockpage that includes logos or text indicating an ISP or government authority?	OONI and ICLab	Blockpage contains logos or text indicating an ISP or government authority
Do the OONI or ICLab measurements for this installation show censorship from multiple vantage points?	OONI and ICLab	Multiple different vantage points experiencing censorship by a single Netsweeper installation
Do our results from **Section 1.2.1** show multiple adjacent IP addresses on the same network?	Censys, Shodan, OONI, and ICLab	Multiple adjacent IP addresses on the same network

Table 1.3. Summary of data points collected to validate whether Netsweeper installations are on consumer-facing ISPs

1.2.3 Identify content blocked by Netsweeper installations

We further examined bona fide Netsweeper installations on consumer-facing ISPs in countries of interest in order to determine what websites they were blocking and whether or not they might be communicating with Netsweeper, Inc.

Ad-hoc manual testing

In some cases, we collected limited data from users who had access to a vantage point on a network in a country of interest. In such cases, users who had access to

a network of interest accessed a set of websites within a web browser and noted the responses. Identifying if a site is inaccessible as a result of deliberate filtering is context-specific and is discussed in further detail in specific country case studies. This type of testing has limitations: it relies on manual data entry and interpretation of results observed. This testing leads to a higher likelihood of error than automated testing.

OONI and ICLab data

We examined our results from OONI and ICLab (**Section 1.2.1**) to determine which websites were being blocked. OONI and ICLab use the same testing lists, which include a global list tested in every country, and a per-country *local* list. The lists are manually created by volunteers and there is variation in the size of the lists and the scope of content they cover. As a result, they may only find a subset of censorship that is present at the time of testing. These lists do not provide an exhaustive inventory of Internet filtering.

Host Header test

We also used a measurement technique that does not require a vantage point on the censored network. This test involves sending requests to IP addresses on a censored network and observing if any of these packets receive an injected blockpage.

To begin, we conducted a zmap scan of the Internet, sending all IPv4 addresses a request containing a Host field that might be blocked by Netsweeper. We picked low-risk URLs, such as invalid URLs that did not point to any web content, or the Netsweeper "deny page test" (e.g., denypagetests.netsweeper.com/category/catno/32) for these global scans in order to avoid a situation where a target IP address might be implicated in circumventing censorship. We examined responses to our scan with an IPID value of 242, which our previous research had shown as being a characteristic of Netsweeper injections. We selected a subset of those IPs for further in-depth testing. In order to ensure ethical testing, we selected only IPs tagged as an "infrastructure router" on Censys or IPs that were clearly operated by ISPs themselves and not ISP customers. We then tested these IPs by sending requests for URLs in our local testing list and double-checked our results.

Beacon Box test

We next sought to determine if Netsweeper installations were communicating with infrastructure controlled by Netsweeper, Inc. This test uses properties of the Netsweeper content categorization system to demonstrate communication

between the installation and databases used for categorization maintained by Netsweeper, Inc. A positive result on this test can suggest that the company has an ongoing relationship with an installation in a country and thus may have the ability to know how services are used (or misused) in a particular jurisdiction.

Netsweeper's Internet filtering system is made up of two components. The first is software that intercepts requests for websites and determines if they are to be denied or permitted and the second is a database of website categorizations. The software component looks up how a requested website is categorized through the database component. If a requested website belongs to a content category that has been selected for filtering, the website is blocked.

Given the highly dynamic nature of web content, assigning categories to that content is a significant undertaking; as a consequence, categorization of web content is a key method that filtering vendors use to differentiate their services. According to Netsweeper's "Live Stats" website, they typically categorize on the order of tens of millions of websites per day. Each Netsweeper customer has a local copy of that database. If a website is requested that has not been categorized in that local database (e.g., a newly-registered domain) the local installation will contact Netsweeper's cloud-based categorization engine, which will fetch the website, categorize it, and make that categorization available to customer installations to be included in their local databases, within a few seconds.

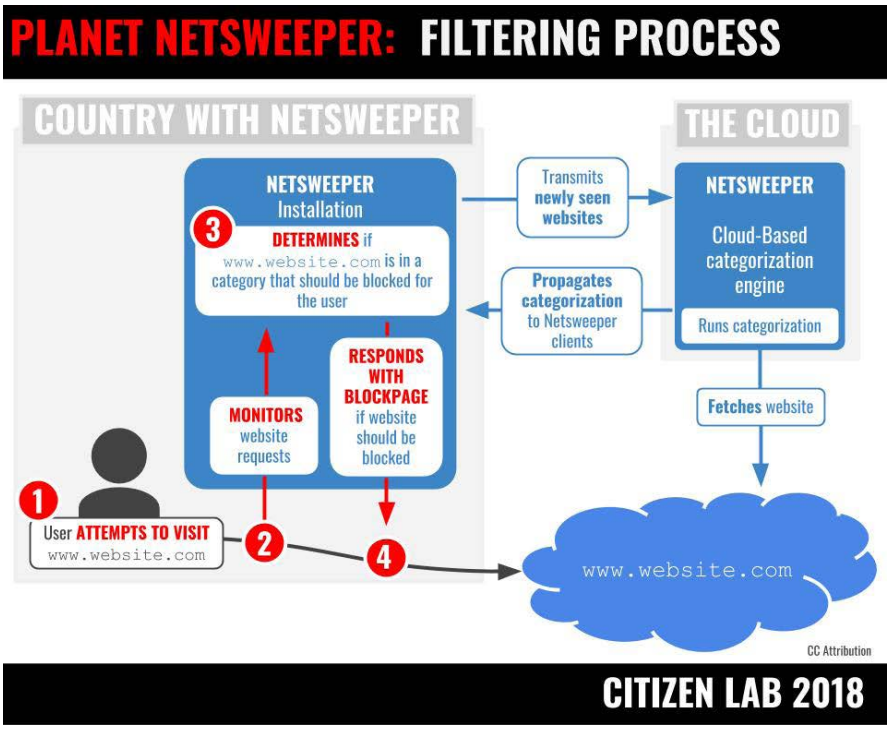

Figure 1.3. The Netsweeper Filtering Process

We registered a set of new domains on which we hosted innocuous text content. We divided the domains into two groups: (1) a control group that we never accessed from anywhere and (2) a test group that we accessed in a country of interest. We expect that server logs from the control group would be empty and server logs from the test group would show two entries:

1) An HTTP GET request for our website from the vantage point
2) A second HTTP GET request from a different IP address within a few seconds

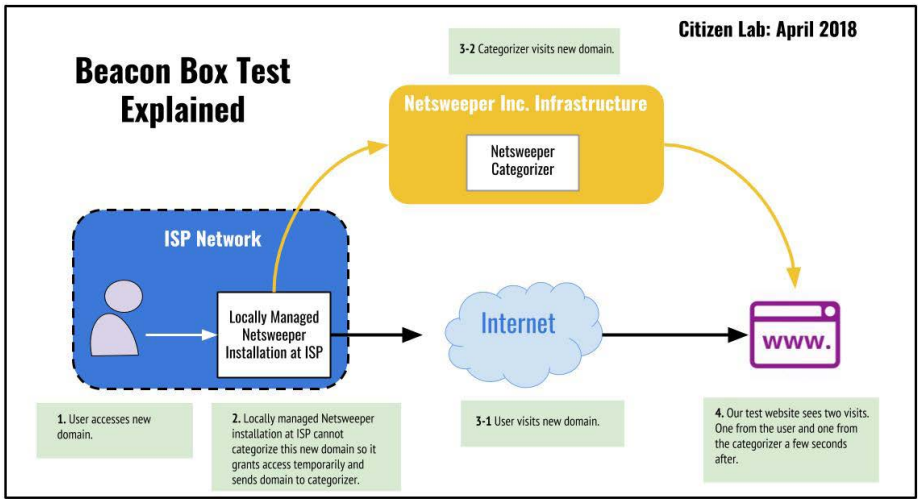

Figure 1.4. An explanation of the flow of information in the Beacon Box test.

In prior research in Yemen, our control group behaved as expected and the test group all showed a request within one second from an IP address belonging to a customer of cloud provider Rackspace. In prior research in Bahrain, our control group behaved as expected and the test group all showed requests within one second from IP addresses belonging to a customer of cloud provider DigitalOcean. A 2015 forum post by a user of Australian ISP Telstra describes a similar follow-up visit from a Rackspace-hosted IP address, a practice which Telstra confirmed to be Netsweeper, Inc.'s categorization process.

1.3 General Technical Findings

In this section, we summarize the general findings of our data collection. For our case studies of bona fide Netsweeper installations on consumer-facing ISPs in specific countries of interest, see **Section 2**.

1.3.1 Netsweeper installations

Our data collection period ran for seven months from August 31, 2017 to April 9, 2018. We identified the possible installations listed in **Table 1.4** after collecting Internet scanning data and on-network measurements that matched our signature (**Section 1.2.1**). This list includes installations being used in institutional settings as well as those operated at private businesses. There may also be matches to our Netsweeper signature present in this table that are false positives.

Country	Number of IP addresses	Number of Autonomous Systems (AS)
Canada	80	8
United States	70	29
Great Britain	69	17
India	42	13
Pakistan	20	2
Bahrain	12	9
Afghanistan	10	2
Qatar	8	1
Ireland	8	3
Australia	8	5
Yemen	6	1
Somalia	6	3
Saudi Arabia	5	2
Kuwait	5	2
Sudan	4	2
New Zealand	4	3
Indonesia	4	3
Cyprus	3	1
United Arab Emirates	3	1
South Africa	2	2
Singapore[1]	1	1
Palestinian Territory	1	1
Netherlands	1	1
Greece	1	1
Dominica	1	1
Germany	1	1
Colombia	1	1
Brunei Darussalam	1	1

1 The reverse DNS entry for the installation found in Singapore is **apacdemo.netsweeper.com**; we believe that this installation is for sales demonstration purposes and is used by Netsweeper for marketing in the Asia-Pacific region.

Country	Number of IP addresses	Number of Autonomous Systems (AS)
Argentina	1	1
Albania	1	1
TOTAL		
30 Countries	**379 IP addresses**	**111 ASNs**

Table 1.4. List of all possible Netsweeper IP addresses found

Note that a single installation maybe double-counted in **Table 1.4** if it was associated with more than one IP address during our data collection period. Geolocation information is based on the latest MaxMind GeoIP2 Country database at the time of collection. We manually corrected some incorrect geolocations that we noticed, such as the ASN "VIVA Bahrain," which geolocated to Saudi Arabia, despite being a Bahraini ISP.

We narrowed our findings from the master list of all Netsweeper installations to focus on installations being used to censor content on consumer-facing ISPs in countries of interest. Our countries of interest are any country ranked "Authoritarian" in the 2017 Economist Democracy Index, along with India, Pakistan, and Somalia. We added these latter three countries because of the unique history, political and security situation, and characteristics of Internet filtering in the countries (**Section 1.1.2**). **Table 1.5** below identifies Netsweeper installations in countries of interest.

Country	Economist 2017 Democracy Index Ranking	IP addresses of Netsweeper installations	Autonomous System Names	Names of ISPs
Afghanistan	Authoritarian	10	Afghantelecom Government Communication Network	Afghan Telecom
			Etisalat Afghan	Etisalat Afghanistan
Bahrain	Authoritarian	16	Batelco	Batelco
			Etisalcom Bahrain Company W.L.L.	Etisalcom
			Kalaam Telecom Bahrain B.S.C.	Kalaam Telecom
			Mena Broadband Services WLL	Mena Broadband Services
			Northstar Technology Company W.L.L.	Northstar Technology Company
			Nuetel Communications S.P.C	Nuetel
			Rapid Telecommunications W.L.L.	Rapid Telecom
			ViaCloud WLL	Viacloud
			VIVA Bahrain BSC Closed	VIVA
			Zain Bahrain B.s.c.	Zain Bahrain
India	Flawed Democracy	42	BHARTI Airtel Ltd.	Bharti Airtel
			Bharti Airtel Ltd. AS for GPRS Service	Bharti Airtel
			Hathway IP Over Cable Internet	Hathway
			Hughes Escorts Communications Limited Is A Satellite Based Broadband Isp & Asp	Hughes Communications
			National Internet Backbone	BSNL Broadband
			Net4India Ltd	Net4
			Pacific Internet India Pvt. Ltd.	PacNet
			Primesoftex Ltd	Prime Softex
			Reliance Communications Ltd.DAKC MUMBAI	Reliance Communications
			Reliance Jio Infocomm Ltd	Jio
			TATA Communications formerly VSNL is Leading ISP	TATA Communications
			TATA SKY BROADBAND PRIVATE LIMITED	TATA Sky
			Telstra Global	Telstra

Country	Economist 2017 Democracy Index Ranking	IP addresses of Netsweeper installations	Autonomous System Names	Names of ISPs
Kuwait	Authoritarian	5	Fast Telecommunications Company W.L.L.	Fastelco
			Mobile Telecommunications Company	Zain
Pakistan	Hybrid Regime	20	Pakistan Telecommunication Company Limited	PTCL
			Paknet Limited Merged into PTCL	Paknet
Qatar	Authoritarian	8	Ooredoo Q.S.C.	Ooredoo
Saudi Arabia	Authoritarian	1	Etihad Atheeb Telecom Company	Go
Sudan	Authoritarian	4	KANARTEL	Canar/Canartel
			Sudatel	Sudatel
Somalia	N/A	7	Golis-Telecom-AS	Golis Telecom
			HORMUUD	Hormuud Telecom
			O3b Limited	O3b
UAE	Authoritarian	3	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	du
Yemen	Authoritarian	6	Public Telecommunication Corporation	Yemennet

Table 1.5. Summary of Netsweeper installations identified in countries of interest

We discuss these installations in more detail in **Section 2**.

1.3.2 What is blocked?

We collected data concerning the blocking of URLs (**Section 1.2.3**) and summarize our findings in **Table 1.6**.

Number of times in our testing where a blockpage was returned	20,607
Number of URLs blocked per country (sum over all countries where blocking observed)	2,464
Number of countries where a blockpage was ever returned, including both countries of interest and non-interest	17
Number of content categories ever seen in a blockpage query string	18

Table 1.6. Overview of observed blocking behaviour.

Netsweeper assigns all URLs to a set of content categories. System administrators select from the set of available content categories to decide which content to

block. System administrators can also add URLs to categories such as the “Custom” category.

Category	Number of URLs on testing lists that we saw blocked at least once, in at least one country, in each category[2]
Custom	1,493
Pornography	490
[Blank][3]	141
Web Proxy	136
Gambling	76
Substance Abuse	45
Alternative Lifestyles	28
Alcohol	19
Hate Speech	13
Nudity	6
Multiple Categories	7
Criminal Skills	3
Viruses	2
Sex Education	1
Phishing	1
Matrimonial	1
Match Making	1
Abortions	1
TOTAL	**2,464**

Table 1.7. Content categories found in blockpages

The disproportionate number of URLs blocked in the “Custom” category is due to data collected from India. All URLs found blocked in India were assigned to this content category and data from this country contributed significantly to the large number of blocked URLs.

1.3.3 Beacon Box tests

We conducted seven Beacon Box tests on seven ISPs. Each test was performed with newly registered domain names. These tests showed communication between installations at three ISP networks and infrastructure that we believe is controlled by Netsweeper, Inc. **Table 1.8** summarizes the results of these tests.

2 It is possible that some URLs might be added to these categories by individual operators and do not represent categorizations performed by Netsweeper, Inc

3 Some measurements did not include a content category; these instances are labelled as “[Blank]”.

Country	ISP	Time of initial visit	Follow-up visit	User-agent of follow-up visitor
Kuwait	Zain	14:25:22.783	14:25:23.116 From 162.243.69.215 (DigitalOcean)	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
India	Airtel	09:38:17.188	09:38:19.380 From 159.203.196.79 (DigitalOcean)	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
Yemen	Yemennet	07:22:50.293	07:22:50.485 From 159.203.42.143 (DigitalOcean)	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0

Table 1.8. Summary of our positive Beacon Box tests

In these three cases, the initial visit to our newly-created domain was followed within less than 2 seconds by a visit from a DigitalOcean-hosted IP address. In all three cases, the user-agent string was identical, perhaps indicating the same software was running on all three DigitalOcean IP addresses. These results were as expected, given our previous testing in 2016 in Bahrain and 2015 in Yemen.

We also ran Beacon Box tests that produced negative results (i.e., the test did not result in any follow-up visits). The negative results were from Airtel and Air Jaldi in India, PTCL in Pakistan, and Ooredoo in Qatar. It is not clear why these tests did not lead to follow-up visits from the Netsweeper categorizer.

We conclude that the Netsweeper installations on the ISPs in **Table 1.8** are likely actively communicating with and receiving URL categorization services from infrastructure controlled or maintained by Netsweeper, Inc. Also of note with respect to these communications, there are potential privacy concerns regarding transmission of user web request data to a foreign jurisdiction.

1.3.4 Host Header tests

Our host header tests found Netsweeper-injected responses on 14 ISPs in six countries.

Country	ISP
Afghanistan	Asix
	Etisalat Afghan

Country	ISP
Bahrain	Bahrain Internet Exchange
	Batelco
	Infonas WLL
	Kalaam Telecom Bahrain B.S.C.
	Mena Broadband Services WLL
	Nuetel Communications S.P.C
	Rapid Telecommunications W.L.L.
India	CityCom Networks Pvt Ltd
	Hathaway IP Over Cable Internet
	Telstra Global
Japan	Telstra Global
United States	Windstream Communications Inc
Yemen	Public Telecommunication Corporation

Table 1.9. Positive results of our Host Header test

Bahrain Case Study

We identified an infrastructure IP address in Bahrain and sent a series of Host Header probes to the IP address containing each URL in the Bahrain local testing list. We received blockpages for 57 of these URLs. The blockpages were consistent with the blockpage seen by Bahraini Internet users and were returned in packets with an IPID value of 242. The results of this testing are discussed further in the Bahrain country case study in Section 2.

```
IP (tos 0x0, ttl 48, id 242, offset 0, flags [none], proto TCP (6), length 403)
[REDACTED].80 > [REDACTED].35409: Flags [FP.], cksum 0xa858 (correct),
seq 2756251069:2756251432, ack 739199291, win 4096, length 363: HTTP, length: 36
3
HTTP/1.0 200 OK

Pragma: no-cache
Cache-Control: no-cache
Content-Length: 255
Content-Type: text/html
<meta name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.
0"/><style>body{margin:0px;padding:0px;}iframe{width:100%;height:100%}</style><iframe
src="http://www.anonymous.com.bh/" width="100%" height="100%" frameborder=0></
iframe>[!http]
```

Figure 1.5. A sample packet containing a blockpage returned during our Host Header testing.

1.3.5 Miscategorization

Although Netsweeper and other filtering companies promote the breadth of their website categorization databases and the effectiveness of their automated categorization methods, it is inevitable that content will be miscategorized. Automated categorization systems can misinterpret the presence of certain keywords, such as by confusing sexual health material for adult content or mistaking drug rehabilitation services for those promoting drug use. Prior research on the filtering product SmartFilter showed how errant categorizations can have large impacts on the accessibility of content and can leave both content creators and users with few opportunities for recourse.

Our data collection identified a number of apparent content miscategorizations. In some cases, we can identify the *same miscategorization across several Netsweeper installations*, which indicates that Netsweeper's categorization system may be responsible. In other cases, it is unclear whether Netsweeper or the operator of a single Netsweeper installation may be responsible for a miscategorization. Even temporary or unintended miscategorizations can prevent people from accessing information, often with minimal avenues for recourse.

Google searches for "gay" and "lesbian" classified as pornography

We found that Google searches for the keywords "gay" (i.e., http://www.google.com/search?q=gay) and "lesbian" (i.e., http://www.google.com/search?q=lesbian) were blocked in the UAE, Bahrain, and Yemen. In the UAE and Bahrain, these searches were blocked because that URL was included in the "Pornography" category. Testing data from Yemen did not indicate the category to which the blocked URL belonged, but it may be because of the same miscategorization.

However, it is unlikely that a user would actually see a blockpage for a specific Google search, because if they visit the homepage of www.google.com prior to conducting their search, they will be automatically redirected to HTTPS, which obscures the user's search terms from Netsweeper.

Other miscategorizations as pornography

One of the dangers of automated categorization systems is that content might be miscategorized based on the presence of certain keywords or terms. For example, the website of the Centre for Health and Gender Equity (http://www.genderhealth.org/), which contains content discussing sexual and reproductive health, was found categorized as "pornography."

In our testing data, the website of the World Health Organization (WHO) was also found to be blocked in the "pornography" category in the UAE and Kuwait. In addition to the WHO homepage (http://www.who.int), several other WHO URLs that were tested were also blocked, including the WHO's pages on sexual and reproductive health (http://www.who.int/reproductivehealth/), HIV/AIDS (http://www.who.int/topics/hiv_aids/), and a website on avian influenza (http://www.who.int/influenza/human_animal_interface). These websites also did not appear to be blocked in every test in UAE and Kuwait; some tests showed that these websites were accessible.

A number of sites that do not appear to host any sexual content were also blocked as a result of being categorized as pornography in at least one instance. Importantly, we do not know whether these miscategoriations were a result of Netsweeper's categorization process or erroneous manual intervention by the operators of a single Netsweeper installation.

Site Description	URL
The Christian Science Monitor	http://www.csmonitor.com
World Union for Progress Judaism	https://wupj.org
Center for Health and Gender Equity	http://www.genderhealth.org/
Change Illinois, a political advocacy group in Illinois	http://www.changeil.org
White Honor, a white supremacist website	http://whitehonor.com/
BackTrack Linux	http://www.backtrack-linux.org
Middle East Transparent, a news website	https://middleeasttransparent.com/fr/

Table 1.10. Non-pornographic sites observed categorized as Pornography, either due to Netsweeper or due to erroneous manual intervention by the operators of a single Netsweeper installation

Previous research published by the ONI showed how Netsweeper's categorization of social media platform Tumblr as pornography– potentially due to the presence of pornographic content on some Tumblr sites– led to the entire platform being blocked in Kuwait, Qatar, UAE, and Yemen. A "one-size-fits-all" approach is likely to cause significant collateral impact given the diverse types of content hosted on social media and media sharing platforms.

Multiple miscategorizations of gay.com

The URL http://www.gay.com was blocked in Yemen, Afghanistan, and the UAE where it was variously categorized as "Pornography," "Match Making," "Alternative

Lifestyles," and "Web Proxy." The site was previously an LGBTQ social networking and personals site but, since 2016, has been the homepage of the Los Angeles LGBT Center. It is possible that the categorization of the website is out of date in some cases.

Alternative lifestyles category

Figure 1.6. Filtered LGBTQ content in the UAE.

One category provided by Netsweeper, called "Alternative Lifestyles," warrants special discussion. The category is defined by Netsweeper as follows:

> **"This includes sites that reference topics on habits or behaviors related to social relations, dress, expressions, or recreation that are important enough to significantly influence the lives of a sector of the population. It can include the full range of non-traditional sexual practices, interests and orientations. Some sites may contain graphic images or sexual material with no pornographic intent."**

The category itself raises a number of concerns. First, the framing of LGBTQ identities as "non-traditional" illustrates the inherently discriminatory nature of this content

category. By creating this category, Netsweeper is enabling censorship authorities to implement the wholesale blocking of LGBTQ content, including websites of civil rights and advocacy organizations, HIV/AIDS prevention organizations, and LGBTQ media and cultural groups. This category appears to serve no other purpose beyond facilitating the blocking of non-pornographic LGBTQ content.

The problematic use of this Netsweeper content category was flagged in 2011 by the ACLU in their complaint to the Missouri Research & Education Network (MOREnet). MOREnet had used the Alternative Lifestyles category to block LGBTQ content in more than 100 school districts across the state. Following the ACLU's outreach, MOREnet disabled the blocking of the Alternative Lifestyles category. Network filtering company Lightspeed Systems removed their own similar "education. lifestyle" content category, which contained non-pornographic LGBTQ content, following similar complaints from the ACLU.

We found 28 sites blocked in the Alternative Lifestyles content category (all in the UAE), including:

Site Description	URL
Gay & Lesbian Alliance Against Defamation	http://www.glaad.org
Human Rights Campaign	http://www.hrc.org
The International Lesbian, Gay, Bisexual, Trans and Intersex Association	http://ilga.org/
Gay Men's Health Centre	http://www.gmhc.org
The International Foundation for Gender Education	http://www.ifge.org
Queerty, an LGBTQ online magazine	http://www.queerty.com
Transsexual road map	http://www.tsroadmap.com/
Gay Calgary	http://www.gaycalgary.com
GlobalGayz, an LGBTQ travel and culture site	http://www.globalgayz.com
Caritas International, a Catholic relief, social services and development organization	http://www.caritas.org

Table 1.11. Sites observed categorized as Alternative Lifestyles

Other, unexplained miscategorizations

Some sites were likely miscategorized as "Web Proxy" in at least one instance. Such sites include:

Site Description	URL
Date.com	http://www.date.com/
B'nai B'rith International	http://bnaibrith.org
World Jewish Congress	http://www.worldjewishcongress.org
Vanguard Blog from the LA LGBT Center	http://www.gay.com/
Feminist Majority Foundation	http://www.feminist.org
Jewish Defense League	http://www.jdl.org/
TMZ, a celebrity news site	http://www.tmz.com
Former Catholic	http://www.formercatholic.com
The Bahai Faith	http://www.bahai-faith.org/

Table 1.12. Non-proxy sites observed categorized as Web Proxy

We also found 11 Blogspot-hosted URLs that were blocked in Kuwait as a result of being assigned to the "Viruses" category. It is not clear why this was the case.

1.3.6 Blocking content by country

Netsweeper has a feature that allows for the blocking of websites from specific countries. The company's documentation lists "Countries" as one of the main category groups, alongside web content, web apps, and protocols. It is not clear what justifiable use case would require the blocking of all content from a specific country or set of countries. Our past research has shown that all content from the Israel top-level domain (.il) was found to be blocked in Yemen, although we cannot be sure that such blocking was implemented using this feature.

Section 2- Country Cases

In this section, we spotlight several countries where we have evidence of public ISPs blocking websites using Netsweeper's products. Each country has significant human rights, public policy, insecurity, or corruption challenges, and/or a history of using Internet censorship to prevent access to content that is protected under international human rights frameworks. We also provide a snapshot of the data we collected concerning Netsweeper installations in the country as of April 2018, as well as a selection of content that we determined was being filtered.

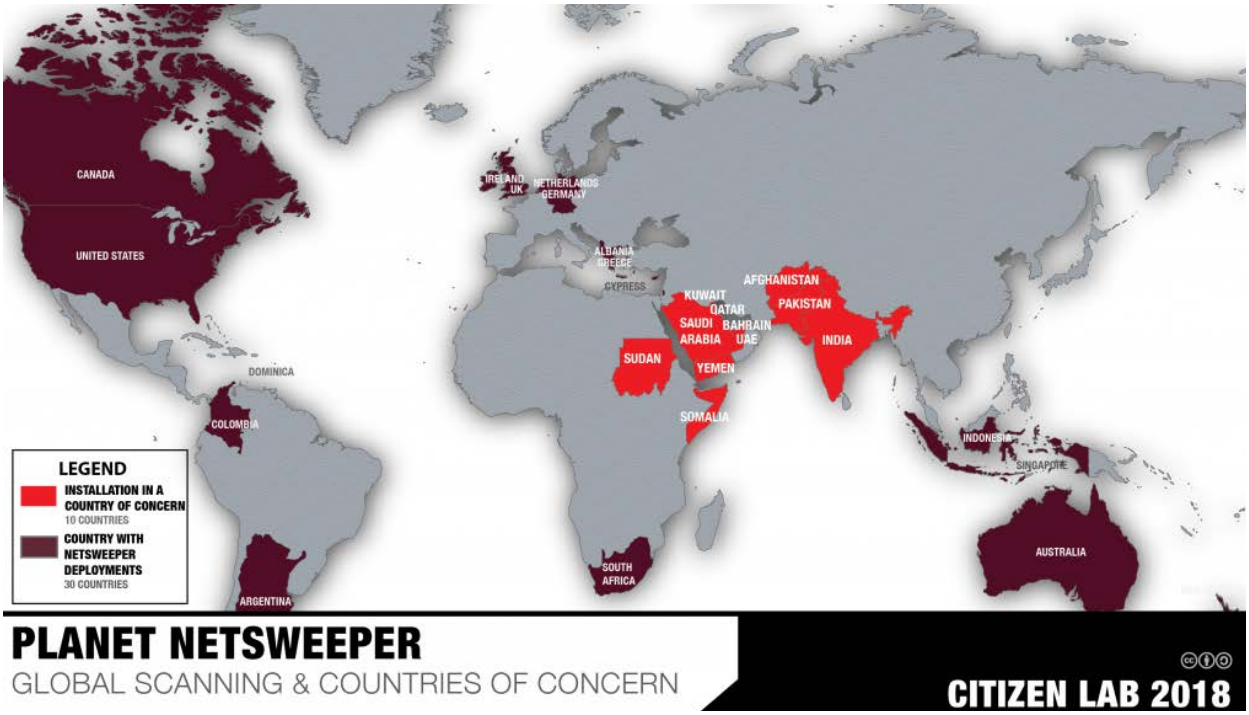

Figure 2.1. Netsweeper installations and countries of concern.

2.1 Summary

From our initial mapping efforts identifying Netsweeper installations in 30 countries (Section 1), we narrowed our focus to 10 countries characterized by significant human rights, public policy, insecurity, or corruption challenges, and/or a history of using Internet censorship to prevent access to content that is protected under international human rights frameworks. The broader political, security, and human rights context characterizing these countries is important to acknowledge in the context of Internet content filtering. These countries' Internet censorship practices are a reflection of this broader context. In **Section 3**, we discuss how this context should be factored into decisions concerning the provision of Internet content filtering services, by both Netsweeper and the Government of Canada.

In what follows, we provide a snapshot of the broader human rights and information controls context for each country, summarize the results of our tests, and highlight some significant findings concerning Internet censorship in each country. Our results include both websites actually blocked, as well as websites that are not *actually blocked*, but which operators *intend to block*. For instance, our results showed that pages on twitter.com corresponding with certain Twitter accounts were blocked in several countries. However, users can actually access these pages because the full URL is very unlikely to be transmitted without HTTPS in practice, and the entire twitter.com site is not blocked.[4](The full data set is available here).

The countries of interest

Afghanistan does not guarantee human rights, lacks democratic governance, and suffers from a perilous security situation. Unique among our dataset, certain blockpages returned in Afghanistan included reference to the 'Matrimonial,' 'Match Making,' and 'Criminal Skills' content categories, with LGBT content improperly categorized as 'Match Making.'

Bahrain has drawn condemnation from human rights group for its ongoing human rights abuses and crackdowns on dissidents, which have included dissolving oppositional groups. The monarchy blocks access to political criticism and religious faith content.

In **India**, minority and other vulnerable groups suffer from human rights violations, including certain castes, religious minorities, Indigenous peoples, women, and LGBT groups. Indian censors have blocked hundreds of websites in various content categories, including websites covering the plight of refugees and religious minorities.

Kuwait bans religious and political criticism, especially if levelled at the head of state. Among the blocked websites in Kuwait were news websites, human rights groups, and secular discussion forums.

In **Pakistan**, security forces abduct and arrest citizens over their criticism of state authorities and religious expression is tightly controlled. In parallel, the censors have blocked content on political and religious grounds.

Qatar bans political parties, restricts workers' associations, and does not grant women full rights. The country applies similar restrictions online and has blocked religious criticism and social content related to LGBT.

4 Because twitter.com is on the browser HSTS preload list.

Sudan violates civil and political rights and restricts religious freedoms. The country's security agency has detained student activists, human rights defenders, journalists, and opposition members. Moreover, Sudanese authorities restrict journalists from covering any issue the government deems to create a security threat and have confiscated copies of newspapers to prevent their distribution. Blocked content categories included 'Occult,' 'Sex Education,' and 'Web Proxy.'

Somalia, Africa's most-failed state, suffers from a human rights crisis. The government passed a repressive, vaguely worded law that prohibits media workers from publishing what it deems as false news. Citizen Lab has previously documented the use of Netsweeper in Somalia for Internet filtering. In 2016, ISPs blocked 29 websites with critical political content. Current testing confirmed the blocking of file-sharing, gambling, and circumvention tool websites.

The **UAE** restricts the rights to freedom of expression and association and detains and prosecutes government critics, opponents, and foreign nationals over their objectionable activities, online and off. Hence, the government censors block various websites run by political critics and human rights advocates, as well as religious and social content they deem objectionable.

Yemen is in the midst of a devastating civil war in which a rebel group is in charge of the sole national ISP. Yemen blocks access to many independent and opposition websites. Yemen's key leaders are sanctioned by the United Nations Security Council for threatening peace and security.

2.2 Afghanistan

Worldwide Governance Indicators for Afghanistan		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.09	21.18
Political stability and absence of violence/ terrorism	-2.75	0.95
Government effectiveness	-1.22	9.62
Regulatory quality	-1.33	7.21
Rule of law	-1.62	3.85
Control of corruption	-1.56	3.37

Table 2.1. World Bank Worldwide Governance Indicators for Afghanistan (2016 data). Source: World Bank Worldwide Governance Indicators, 2017.

2.2.1 Background

Afghanistan's 2004 constitution enshrines democratic processes and human rights protections alongside the country's Islamic identity. However, successive disputed elections and weak state authority have prevented constitutional guarantees from being fulfilled in practice. International human rights groups have expressed concern about the government's ability to guarantee human rights and maintain democratic governance due to the perilous security situation in the country. Weak political institutions have allowed for endemic corruption and ad hoc changes to the constitutional order, such as the power sharing deal following the most recent election, which created the new position of Chief Executive.

While the Afghanistan constitution includes broad and explicit protections for free expression, these rights are constrained in practice by a countervailing provision that enshrines deference to Islam in the legal order. The 2005 media law banned content deemed to be anti-religious, slanderous, contrary to the constitution, or which identified the victims of violence.

2.2.2 Information controls in Afghanistan

Free expression rights were constrained in 2010, when the government implemented nationwide Internet filtering. Authorities ordered the blocking of pornography, sites related to alcohol and gambling, dating sites, and social media. Later that year, the country blocked a news website. In 2017, the government's attention turned to messaging apps, which have become increasingly popular across the country. The government ordered the blocking of Telegram and WhatsApp in November 2017.

2.2.3 Data analysis

2.2.3.1 Evidence of Netsweeper presence

We found 10 IP addresses in Afghanistan that were part of Netsweeper installations (shown in **Table 2.2**). Behavioral testing results are shown in **Table 2.3**.

AS name	AS Number	IP Address	Date first seen	Date last seen
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.88.62	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.88.58	2017-08-31	2018-04-04

AS name	AS Number	IP Address	Date first seen	Date last seen
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.80.162	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.78.110	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.76.2	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.69.170	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.65.58	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.64.6	2017-08-31	2018-04-04
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	55330	180.94.64.2	2017-08-31	2018-04-04
Etisalat Afghan	131284	180.222.138.78	2017-08-31	2018-04-04

Table 2.2. Netsweeper installations identified in Afghanistan

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr hostname	deny page title
180.94.64.2	AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK									Linux Kabul-NS-PS01	Access Denied
180.94.64.6										Linux Kabul-NS-PS02	Access Denied
180.94.65.58										Linux Mazar-NS-PS01	Access Denied
180.94.69.170										Linux Herat-NS-PS01	Access Denied
180.94.76.2										Linux Kandahar-NS-PS01	Access Denied
180.94.78.110										Linux NS-Deny-Page	Untitled document
180.94.80.162										Linux Jalalabad-NS-PS01	Access Denied
180.94.88.58										Linux NS-WebAdmin	Access Denied
180.94.88.62										Linux NS-Reporter	Access Denied
180.222.138.78	Etisalat Afghan										Etisalat Afghanistan Web Filteration Voilation Alert

Table 2.3. Behavioural validation tests for installations found in Afghanistan

The behavioural results (**Table 2.3**) are color coded. Green indicates a positive response (matching Netsweeper), red indicates a negative response.

All 10 installations matched our Boolean expression for Netsweeper installations (**Section 1.1.2)**. The available SNMP sysdescr values include Netsweeper-related terms, such as "NS," "WebAdmin," "Reporter," and "PS," and list the locations where these devices are likely located (e.g., Kandahar, Kabul, etc.). The Netsweeper installation on the Etisalat Afghanistan network's deny page title explicitly lists that it is a "Etisalat Afghanistan Web Filteration Voilation Alert" [sic].

Network measurements from both Afghantelecom and Etisalat Afghanistan appeared in OONI test results and showed that attempts to access blocked content received an injected blockpage. For example, OONI records the following response to an attempt to access the LGBT news site Gay Today (http://gaytoday.com/) on Afghantelecom on September 9, 2017:

```
<iframe src="http://180.94.78.110/webadmin/deny?dpid=1&dpruleid=78&cat=23&ttl=-200&gr
oupname=default&policyname=Default&username=[REDACTED]&userip=[REDACTED]&connec
tionip=127.0.0.1&nsphostname=Jalalabad-NS-PS01&protocol=policyprocessor&dplanguage=-
&url=http%3a%2f%2fgaytoday%2ecom%2f" width="100%" height="100%" frameborder=0></
iframe>
```

A similarly formatted iframe was returned from a test on Etisalat Afghanistan.

2.2.3.2 Examples of blocked content

According to OONI data, blockpages were returned mentioning the following categories on Afghantelecom and Etisalat Afghanistan:

- Pornography
- Web Proxy (Etisalat Afghan only)
- Match Making (Etisalat Afghan only)
- Matrimonial (Etisalat Afghan only)
- Alcohol (Afghantelecom only)
- Criminal Skills (Afghantelecom only)
- Gambling (Afghantelecom only)

The Afghanistan case is the only instance in our dataset where we saw blockpages returned mentioning the 'Matrimonial,' 'Match Making,' and 'Criminal Skills' content categories.

We identified 19 blocked URLs. The list below indicates the URLs as well as the categories returned in the blockpages:

- 4Chan (http://www.4chan.org/) (Pornography)
- http://spys.ru/ (Web Proxy)
- http://translation.langenberg.com/ (Web Proxy)
- http://www.gay.com/ (Match Making)
- http://www.matrimony.org/ (Matrimonial)
- http://www.peacefire.org/circumventor/simple-circumventor-instructions.html (Web Proxy)
- http://www.youporn.com/ (Pornography)
- http://astalavista.box.sk/ (Criminal Skills)
- http://attrition.org/ (Criminal Skills)
- http://gaytoday.com/ (Pornography)
- http://www.4chan.org/ (Pornography)
- http://www.89.com/ (Pornography)
- http://www.drunkard.com/ (Alcohol)
- http://www.monacogoldcasino.com/ (Gambling)
- http://www.playboy.com/ (Pornography)
- http://www.royalvegas.com/ (Gambling)
- http://www.twistedInternet.com/ (Criminal Skills)
- http://www.usacasino.com/ (Gambling)
- http://www.wetplace.com/ (Pornography)

As we described in **Section 1.3.5**, http://www.gay.com/ is improperly categorized as 'Match Making'; the website is actually the homepage of the Vanguard Blog that is run by the Los Angeles LGBT Center.

During Host Header testing, we saw blockpages returned from IP addresses in two Afghani ASNs: Etisalat Afghan and Asix.

2.3 Bahrain

Worldwide Governance Indicators for Bahrain		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.45	8.37
Political stability and absence of violence/ terrorism	-0.86	18.10
Government effectiveness	0.32	65.87

Worldwide Governance Indicators for Bahrain		
Regulatory quality	0.61	72.12
Rule of law	0.46	66.35
Control of corruption	-0.06	56.25

Table 2.4. World Bank Worldwide Governance Indicators for Bahrain (2016 data) Source: World Bank Worldwide Governance Indicators, 2017

2.3.1 Background

International human rights groups have expressed grave concern over a crackdown on dissent in the country. Bahrain's largest political opposition group has been dissolved and its only independent newspaper shut down. Numerous opposition leaders have been jailed, including for critical speech on social media. In a 2017 report, Amnesty International called on "states supplying equipment to Bahrain that could be used for internal repression" to take immediate action.

2.3.2 Information controls in Bahrain

The Bahraini authorities use a variety of legal, physical, and digital tactics to prevent their citizens from accessing information deemed objectionable. The Bahraini authorities have repeatedly summoned outspoken critics of the monarchy for questioning, legal proceedings, or even to commit them to intermittent jail sentences in an apparent attempt to harass these critics into silence.

ISPs restrict Internet connectivity by throttling Internet speeds around the time of political protests. For example, the authorities have imposed Internet curfews in the town of Diraz by shutting down mobile data services and disrupting fixed-lined connections. Bahrain has also used spyware tools, including FinFisher, to spy on dissidents, political opposition, lawyers, and journalists.

Prior Citizen Lab research has documented the use of Netsweeper in Bahrain. A 2016 report documented the presence of Netsweeper installations on the networks of nine ISPs in Bahrain. We conducted the research after a January 2016 tender was published that indicated that Netsweeper was the sole bidder for a "National Website Filtering Solution." The research utilized network measurement tests that were run on the Batelco ISP and identified that websites pertaining to local opposition political groups, human rights organizations, religious content, and critical independent media were filtered. Tests from two other Bahrain-based ISPs showed evidence that the Netsweeper installations in Bahrain were communicating with Netsweeper's infrastructure, which we interpreted as suggesting that the installations were officially supported by the company.

2.3.3 Data analysis

2.3.3.1 Evidence of Netsweeper presence

We found 16 IP addresses in Bahrain that were part of Netsweeper installations (shown in **Table 2.5**). Behavioral validation results are shown in **Table 2.6**.

AS Name	AS Number	IP Address	Date first seen	Date last seen
Batelco	5416	193.188.112.86	2017-08-31	2018-04-04
Etisalcom Bahrain Company W.L.L.	35457	80.95.222.115	2017-08-31	2018-04-04
Etisalcom Bahrain Company W.L.L.	35457	80.95.222.114	2017-08-31	2018-04-04
Kalaam Telecom Bahrain B.S.C.	39273	87.236.52.38	2017-08-31	2018-04-04
Mena Broadband Services WLL	39015	188.116.227.226	2017-08-31	2018-04-04
Northstar Technology Company W.L.L.	35546	80.241.146.26	2017-08-31	2018-04-04
Nuetel Communications S.P.C	35568	87.236.136.187	2017-08-31	2018-04-04
Nuetel Communications S.P.C	35568	87.236.136.186	2017-11-21	2018-04-04
Rapid Telecommunications W.L.L.	62123	185.34.229.237	2017-08-31	2018-04-04
Rapid Telecommunications W.L.L.	62123	185.34.229.236	2017-08-31	2018-04-04
ViaCloud WLL	35729	87.252.99.246	2017-08-31	2018-04-04
VIVA Bahrain BSC Closed	51375	84.235.107.72	2017-08-31	2018-04-04
VIVA Bahrain BSC Closed	51375	84.235.107.71	2017-08-31	2018-04-04
VIVA Bahrain BSC Closed	51375	84.235.107.206	2017-08-31	2018-04-04
VIVA Bahrain BSC Closed	51375	84.235.107.203	2017-08-31	2018-04-04
Zain Bahrain B.s.c.	31452	109.161.148.250	2017-08-31	2018-04-04

Table 2.5. Netsweeper installations identified in Bahrain

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr hostname
109.161.148.250	Zain Bahrain B.s.c.									zain-tmp-ps02
185.34.229.236	Rapid Telecommunications W.L.L.									rapid-ps01
185.34.229.237										rapid-ps02
188.116.227.226	Mena Broadband Services WLL									
193.188.112.86	Batelco									
80.241.146.26	Northstar Technology Company W.L.L.									Northstar-PS01
80.95.222.114	Etisalcom Bahrain Company W.L.L.									etisalcom_ps01
80.95.222.115										etisalcom_ps02
84.235.107.203	VIVA Bahrain BSC Closed									viva-tubli-ps01
84.235.107.206										viva-tubli-ps02
84.235.107.71										viva-hora-ps01
84.235.107.72										viva-hora-ps02
87.236.136.186	Nuetel Communications S.P.C									nue-tel-server-ps01
87.236.136.187										nue-tel-server-ps02
87.236.52.38	Kalaam Telecom Bahrain B.S.C.									kalaam-ps02
87.252.99.246	ViaCloud WLL									localhost.localdomain

Table 2.6. Behavioural validation tests in Bahrain

All but one of the IP addresses matched our Boolean expression for Netsweeper installations (**Section 1.1.2**). Of the 16 IP addresses, 14 returned SNMP sysdesc values that followed a relatively consistent naming scheme (e.g. viva-tubli-ps01, Northstar-PS01, etc.).

The blockpages in Bahrain all involve an iframe pointing to "http://www.anonymous.com.bh," which we saw in prior research, e.g.:

```
<iframe src="http://www.anonymous.com.bh/?dpid=9&dpruleid=1&cat=23&ttl=-200&groupname=Batelco&policyname=Batelco_Policy&username=[REDACTED]&userip=[REDACTED]&connectionip=127.0.0.1&nsphostname=batelco-ns-ps01&protocol=policyprocessor&dplanguage=-&url=http%3a%2f%2fwww%2egoogle%2ecom%2fsearch%3fq%3dgay" width="100%" height="100%" frameborder=0></iframe>
```

This generates a blockpage similar to the one seen in **Figure 2.2**. As of April 8, 2018, we are not able to access this page from outside of Bahrain.

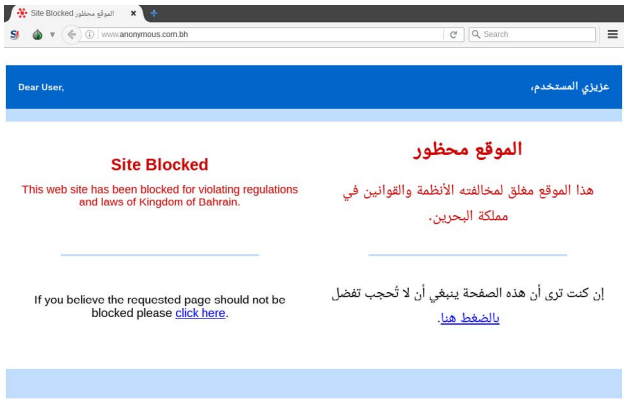

Figure 2.2. Blockpage received in Bahrain from http://www.anonymous.com.bh/.

During Host Header testing, we saw blockpages returned from IP addresses in seven Bahraini ASNs: Bahrain Internet Exchange, Batelco, Infonas WLL, Kalaam Telecom, Mena Broadman, Nuetel Communications, and Rapid Telecommunications.

2.3.3.2 Examples of blocked content

According to OONI data, blockpages were returned mentioning the following categories on Afghantelecom and Etisalat Afghanistan:

- Custom
- Gambling
- Pornography
- Web Proxy

We identified 145 blocked URLs in Bahrain. Some of these URLs are listed in **Table 2.7**.

Website Description	URLs
Websites affiliated with local political groups including opposition movements	http://www.vob.org/
	http://www.14febrayer.com/
Websites of local and regional human rights and advocacy organizations	http://www.bahrainrights.org/
	http://anhri.net/
Bahraini publications that post content critical of the government of Bahrain	http://bahrainmirror.com/
	http://bhmirror.no-ip.org/index.php
	http://lualuatv.com/
	http://www.periscope.tv/LuaLuaTV/
	http://twitter.com/lualuatv
	http://instagram.com/LuaLuaTV
	http://alduraz.net/
Pan-Arab and international media	http://aljazeera.net
	http://www.alquds.co.uk/
	http://www.arabtimes.com
Websites on the Shia sect	http://albrhan.org/
	http://www.ansarh.com/
Google searches for the terms ‘gay’ and ‘lesbian,’ which are categorized as pornography	http://www.google.com/search?q=gay
	http://www.google.com/search?q=lesbian
Websites that have content critical of Islam	http://www.faithfreedom.org
LGBT news and opinion site	http://gaytoday.com
Media affiliated with Lebanon’s Hezbollah	http://www.almanar.com.lb/

Table 2.7. URLs identified as being blocked in Bahrain

2.4 India

Worldwide Governance Indicators for India		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	0.41	58.62
Political stability and absence of violence/ terrorism	-0.95	14.29
Government effectiveness	0.10	57.21
Regulatory quality	-0.31	41.35
Rule of law	-0.07	52.40
Control of corruption	-0.30	47.12

Table 2.8. World Bank Worldwide Governance Indicators for India (2016 data) Source: World Bank Worldwide Governance Indicators, 2017

2.4.1 Background

Various social minorities and other vulnerable groups in India—including members of certain castes, religious minorities, indigenous people, women, and LGBT individuals—suffer from persistent human rights violations. Such violations include vigilante violence, discrimination, and demonization by dominant social groups. In some cases, security forces are responsible for committing these kinds of abuses. Indian security forces have used excessive force against protestors, prisoners, and others resulting in deaths.

2.4.2 Information controls in India

Indian citizens face notable challenges in the area of freedom of expression. Four journalists were killed in the country in 2017 and others were attacked, detained, or prosecuted, according to the Committee to Protect Journalists. India also maintains criminal defamation and sedition laws that have been used against journalists.

The same laws have also been used to punish free expression advocates, activists, protesters, and members of the public. In separate incidents in 2017: 30 people were arrested for organizing a press conference about caste-based violence; 20 people were arrested for allegedly celebrating Pakistan's victory over India in a cricket match; eight university students were detained for almost a month for protesting against the state government; and four people were held for more than three months for attempting to commemorate Tamils killed in Sri Lanka.

The government has also acted to chill critical speech by using strict legal controls on foreign funding of civil society groups to punish groups that scrutinize official actions. The UN Special Rapporteurs on the situation of human rights defenders, on freedom of opinion and expression, and on the rights to freedom of peaceful assembly and of association have called on the Indian government to end this practice.

In 2017, the NGO SFLC.in filed a request under right to information laws to obtain details about the country's website blocking regime. In response, the Ministry of Electronics and Information Technology stated that 23,090 websites/URLs were blocked in the country but withheld all other requested information under a legal provision that provides for "strict confidentiality…regarding all the blocking requests and complaints received and actions taken thereof."

The NGO Access Now documented that authorities in India forced Internet and mobile providers to disable their networks 44 times in 2017 and 11 times in 2016.

2.4.3 Data analysis

2.4.3.1 Evidence of Netsweeper presence

We found 42 IP addresses in India that were part of Netsweeper installations (shown in **Table 2.9**). Behavioral validation results are shown in **Table 2.10**.

AS Name	AS Number	IP Address	Date first seen	Date last seen
BHARTI Airtel Ltd.	9498	182.79.218.98	2017-08-31	2017-09-07
BHARTI Airtel Ltd.	9498	182.79.218.38	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.35	2017-11-21	2017-11-29
BHARTI Airtel Ltd.	9498	182.79.218.34	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.198	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.197	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.196	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.167	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.166	2017-08-31	2018-04-04
BHARTI Airtel Ltd.	9498	182.79.218.106	2017-08-31	2018-04-04
Bharti Airtel Ltd. AS for GPRS Service	45609	223.239.13.254	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	203.163.229.27	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	202.88.190.35	2017-09-26	2018-04-04

AS Name	AS Number	IP Address	Date first seen	Date last seen
Hathway IP Over Cable Internet	17488	202.88.158.98	2017-09-26	2018-04-04
Hathway IP Over Cable Internet	17488	202.88.152.20	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	202.88.149.42	2017-09-26	2018-04-04
Hathway IP Over Cable Internet	17488	125.99.99.125	2017-10-04	2018-04-04
Hathway IP Over Cable Internet	17488	125.99.99.124	2017-10-04	2018-04-04
Hathway IP Over Cable Internet	17488	125.99.99.123	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	125.99.99.122	2017-10-04	2018-04-04
Hathway IP Over Cable Internet	17488	125.99.64.67	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	125.99.170.27	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	116.74.81.11	2017-08-31	2018-04-04
Hathway IP Over Cable Internet	17488	116.74.105.29	2017-09-26	2018-04-04
HUGHES ESCORTS COMMUNICATIONS LIMITED IS A SATELLITE BASED BROADBAND ISP & ASP	17648	110.50.49.27	2018-01-31	2018-04-04
National Internet Backbone	9829	218.248.233.12	2017-08-31	2018-04-04
Net4India Ltd	17447	202.71.145.253	2017-08-31	2018-04-04
Pacific Internet India Pvt. Ltd.	9625	203.123.187.26	2017-08-31	2018-04-04
Pacific Internet India Pvt. Ltd.	9625	203.123.180.38	2017-08-31	2018-04-04
Pacific Internet India Pvt. Ltd.	9625	203.123.136.50	2017-08-31	2018-04-04
Primesoftex Ltd	17426	203.115.96.147	2017-08-31	2018-04-04
Primesoftex Ltd	17426	203.115.127.156	2017-08-31	2018-04-04
Primesoftex Ltd	17426	203.115.112.138	2017-08-31	2018-04-04
Primesoftex Ltd	17426	203.115.102.145	2017-08-31	2018-04-04
Reliance Communications Ltd.DAKC MUMBAI	18101	115.248.224.97	2017-09-26	2018-04-04
Reliance Jio Infocomm Ltd	55836	49.44.18.34	2017-08-31	2018-04-04

AS Name	AS Number	IP Address	Date first seen	Date last seen
TATA Communications formerly VSNL is Leading ISP	4755	59.165.131.53	2017-08-31	2018-04-04
TATA SKY BROADBAND PRIVATE LIMITED	134674	103.195.200.53	2017-08-31	2018-04-04
Telstra Global	4637	210.57.203.2	2017-08-31	2018-04-04
Telstra Global	4637	210.57.201.2	2017-08-31	2018-02-07
Telstra Global	4637	203.123.157.38	2017-08-31	2018-04-04
Telstra Global	4637	203.123.146.126	2017-08-31	2018-04-04

Table 2.9. Netsweeper devices identified in India

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr hostname
182.79.218.106	BHARTI Airtel Ltd.									Policy11-Chennai
182.79.218.166	BHARTI Airtel Ltd.									Policy12-Mumbai
182.79.218.167	BHARTI Airtel Ltd.									Policy13-Mumbai
182.79.218.196	BHARTI Airtel Ltd.									Policy01-Delhi
182.79.218.197	BHARTI Airtel Ltd.									Policy02-Delhi
182.79.218.198	BHARTI Airtel Ltd.									Policy03-Delhi
182.79.218.34	BHARTI Airtel Ltd.									
182.79.218.35	BHARTI Airtel Ltd.									webadmin02
182.79.218.38	BHARTI Airtel Ltd.									logger01
182.79.218.98	BHARTI Airtel Ltd.									Policy03-Chennai
223.239.13.254	Bharti Airtel Ltd. AS for GPRS Service									Wifi_Content
116.74.105.29	Hathway IP Over Cable Internet									surat-policy01
116.74.81.11	Hathway IP Over Cable Internet									goa-policy01
125.99.170.27	Hathway IP Over Cable Internet									indore-policy01
125.99.64.67	Hathway IP Over Cable Internet									pune-policy01
125.99.99.122	Hathway IP Over Cable Internet									policy01
125.99.99.123	Hathway IP Over Cable Internet									web01
125.99.99.124	Hathway IP Over Cable Internet									policy02
125.99.99.125	Hathway IP Over Cable Internet									policy02
202.88.149.42	Hathway IP Over Cable Internet									mohali-policy01
202.88.152.20	Hathway IP Over Cable Internet									chennai-policy01
202.88.158.98	Hathway IP Over Cable Internet									bangalore-policy01
202.88.190.35	Hathway IP Over Cable Internet									hyderabad-policy01
203.163.229.27	Hathway IP Over Cable Internet									kolkata-policy01
110.50.49.27	HUGHES ESCORTS COMMUNICATIONS [...]									
218.248.233.12	National Internet Backbone									
202.71.145.253	Net4India Ltd									dnsserver
203.123.136.50	Pacific Internet India Pvt. Ltd.									Policy02-Mumbai
203.123.180.38	Pacific Internet India Pvt. Ltd.									policy01-Bangalore
203.123.187.26	Pacific Internet India Pvt. Ltd.									webadmin01
203.115.102.145	Primesoftex Ltd									ngurapps1.primenet.in
203.115.112.138	Primesoftex Ltd									localhost.localdomain
203.115.127.156	Primesoftex Ltd									localhost.localdomain
203.115.96.147	Primesoftex Ltd									localhost.localdomain
115.248.224.97	Reliance Communications Ltd.DAKC MUMBAI									
49.44.18.34	Reliance Jio Infocomm Ltd									
59.165.131.53	TATA Communications formerly VSNL [...]									netsweepernrs2.vsnl.in
103.195.200.53	TATA SKY BROADBAND PRIVATE LIMITED									suspend.tataskybb.com
203.123.146.126	Telstra Global									policy03-noida
203.123.157.38	Telstra Global									policy04-chennai
210.57.201.2	Telstra Global									bomnswa01
210.57.203.2	Telstra Global									MASNSPS01

Table 2.10. Behavioural validation tests in India.

Thirty-three of the 42 identified devices returned a positive result for at least one of the behavioural tests. Of the remaining nine devices, seven returned SNMP sysdesc values which were consistent with other Netsweeper installations, such as "hyderabad-policy01" and "webadmin02." The two devices that did not return sysdescr values did provide other indications they were Netsweeper installations. Censys results for 110.50.49.27 showed that it returned a page title of "Netsweeper Manager" on port 8080 and the second device returned a 'Netsweeper Cloud Manager' login page (http://115.248.224.97:8080/webadmin/start/).

During Host Header testing, we saw injected replies from three Indian ASNs: Spectranet, Hathway IP over Cable Internet, and Telstra Global.

An example of a blockpage in one case merits further discussion. An attempt to access the URL http://genderandaids.unwomen.org (the UN Women Gender Equality and HIV/AIDS Web Portal) returned the following blockpage on one occasion:

```
<iframe src="http://125.99.99.123:8080/webadmin/deny/index.php?dpid=4&dpruleid=2&cat=
101&ttl=0&groupname=default&policyname=-&username=[REDACTED]&userip=[REDACTED]&
connectionip=127.0.0.1&nsphostname=bangalore-policy01&protocol=policyprocessor&dplan
guage=-&url=http%3a%2f%2f117%2e18%2e232%2e200%2f" width="100%" height="100%"
frameborder=0></iframe>
```

Interestingly, the URL parameter '&url=http%3a%2f%2f117%2e18%2e232%2e200%2f', indicates that the Microsoft Azure IP address 117.18.232.200 is blocked, perhaps due to erroneous categorization by Netsweeper or erroneous operator intervention. Blocking an Azure IP address would inevitably cause significant collateral damage given the volume of content the service hosts.

2.4.3.2 Examples of blocked content

India was unique among the countries measured in that all blocked URLs appeared to belong to the 'Custom' category. In total, 1,158 unique URLs were found to be blocked.

Websites related to the Rohingya refugee issue, and the deaths of Muslims in Burma and India more generally, were blocked. Such websites included:

Website Description	URLs
Al Jazeera coverage of this topic	http://www.aljazeera.com/indepth/features/2012/08/201281572950685537.html
	http://www.aljazeera.com/video/asia/2012/07/20127271263669558.html;http://www.aljazeera.com/news/asia/2012/08/2012816135757977843.html

Website Description	URLs
The Telegraph's coverage of violence in Burma	http://www.telegraph.co.uk/news/picturegalleries/worldnews/9324473/Tensions-rise-in-Burma-as-Rakhine-Buddhists-and-Rohingya-Muslims-clash.html
A Tribune of Pakistan story about social media coverage of deaths in Burma	https://blogs.tribune.com.pk/story/12867/social-media-is-lying-to-you-about-burmas-muslim-cleansing/
An ABC News (Australia) story about this topic	http://www.abc.net.au/news/2012-08-01/burma-zoe-daniels/4170140
Facebook groups discussing this topic	http://www.facebook.com/crisis.in.burma
	http://www.facebook.com/savemuslimscommunityinburma
	http://www.facebook.com/realityofindia
	http://www.facebook.com/why.always.muslims
A Reddit thread discussing a BBC article on violence in India	http://www.reddit.com/r/worldnews/comments/xc4er/hindus_kill_muslims_in_india_44_dead_170000_made/

Table 2.11. Summary of Rohingya-related URLs that were seen blocked in India

A series of Twitter accounts, Facebook groups, and YouTube channels were also blocked. Some of these pages contain information about religious minorities:

- http://twitter.com/tajinderbagga
- http://twitter.com/redditindia
- http://twitter.com/ekakizunj
- http://twitter.com/barbarindian
- http://twitter.com/anilkohli54
- http://twitter.com/i_panchajanya
- http://youtube.com/user/ajitkumar2350/
- http://youtube.com/user/aslam5535/
- http://youtube.com/user/cancerian809/
- http://youtube.com/user/glakoriz/
- http://youtube.com/user/iqbal1996ful/
- http://youtube.com/user/karsevakindia1/
- http://facebook.com/#!sonniyya/photos
- http://facebook.com/albaik1/
- http://facebook.com/amir.khan.18294053/
- http://facebook.com/amirkhan.bah/
- http://facebook.com/charitha.rathnasekara/posts/335064959919472/
- http://facebook.com/crisis.in.burma/

- http://facebook.com/events/334762509950039/
- http://facebook.com/groups/222847551172001/<
- http://facebook.com/groups/300203800077335/
- http://facebook.com/groups/326961567395994//
- http://facebook.com/groups/410690962321650/
- http://facebook.com/hindujagruti/
- http://facebook.com/ishfaqmatoo/
- http://facebook.com/media/set/?set=a.228899373874308.46433.100002627423113&type=3
- http://facebook.com/mujammil143143/
- http://facebook.com/mushahid.ali.566/
- http://facebook.com/realityofindia/
- http://facebook.com/savemuslimscommunityinburma/
- http://facebook.com/sonowal.niranjan1/
- http://facebook.com/tpsbagga/
- http://facebook.com/why.always.muslims/

Religious content:

- https://hinduexistence.org/
- http://www.formercatholic.com
- http://www.hindujagruti.org/news/14781.html

Other:

- The Wayback Machine from Archive.org, which allows users to search for archived versions of web content (http://wayback.archive.org/)
- A substantial number of file-sharing websites, particularly those sharing Bollywood music and movies

It is important to emphasize that for many of these blocked URLs, particularly those noted above that are hosted on Facebook, Twitter, YouTube, and Reddit, they would likely be accessible if the user attempted to access the HTTPS version. Since HTTPS obscures the specific path visited by a user, a censor would only be able to choose between blocking all of Facebook (to give one example) or none of it.

2.5 Kuwait

Worldwide Governance Indicators for Kuwait		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-0.69	28.08
Political stability and absence of violence/terrorism	-0.15	41.43
Government effectiveness	-0.18	46.63
Regulatory quality	-0.07	52.88
Rule of law	0.03	56.73
Control of corruption	-0.20	50.00

Table 2.12. World Bank Worldwide Governance Indicators for Kuwait (2016) Source: World Bank Worldwide Governance Indicators, 2017 data)

2.5.1 Background

Kuwait systemically ill-treats and discriminates against certain social groups. Thousands of stateless people, known as *Bidun*, continue to be excluded from full citizenship status despite their deep-seated roots in Kuwaiti territory. Human Rights Watch has expressed concern about the exploitation and abuse of migrant workers, who comprise more than two-thirds of the population. Under the official immigration sponsorship system, workers face restrictions on their ability to change jobs or leave the country without their employer's permission.

Same-sex relations between men are punishable by up to seven years in prison in Kuwait. Human Rights Watch reported that authorities deported 76 men on suspicion of being gay in 2017. Transgender people can be arrested under a law that prohibits "imitating the opposite sex in any way."

2.5.2 Information controls in Kuwait

While Kuwaiti law offers some meaningful protections to the media, it restricts freedom of speech through prohibitions on criticism of the Emir, the release of secret or private information, comments promoting overthrow of the regime, and criticism of Islam. A 2016 cybercrime law included broad prohibition of criticizing religion or the Emir online, with punishments ranging from fines to prison sentences.

In January 2016, the government revoked the publishing license of the newspaper *Al-Watan*. This action was condemned by international media watchdogs because

it appeared that the Kuwaiti administration was punishing the newspaper for its critical coverage of the government.

2.5.3 Data analysis

2.5.3.1 Evidence of Netsweeper presence

We found five IP addresses in Kuwait that were part of Netsweeper installations (shown in **Table 2.13**). Behavioral validation results are shown in **Table 2.14**.

AS Name	AS Number	IP Address	Date first seen	Date last seen
Fast Telecommunications Company W.L.L.	21050	62.215.3.135	2017-08-31	2018-04-04
Fast Telecommunications Company W.L.L.	21050	62.215.3.133	2017-08-31	2018-04-04
Fast Telecommunications Company W.L.L.	21050	62.215.188.52	2017-11-29	2018-04-04
Fast Telecommunications Company W.L.L.	21050	62.215.161.222	2017-08-31	2018-04-04
Mobile Telecommunications Company	42961	212.43.17.6	2017-08-31	2018-04-04

Table 2.13. Netsweeper installations located in Kuwait

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr hostname	reverse dns	deny page title
62.215.161.222	Fast Telecommunications Company W.L.L.									SKB-NS-PS01		
62.215.188.52											blocked.fasttelco.net	
62.215.3.133												Access Denied
62.215.3.135												Access Denied
212.43.17.6	Mobile Telecommunications Company										restrict.kw.zain.com	Welcome to Zain

Table 2.14. Netsweeper installations located in Kuwait

Notably, reverse DNS lookups of two of these five devices returned “blocked.fasttelco.net” and “restrict.kw.zain.com.” Fasttelco and Zain are the names of the two ISPs on whose network we found Netsweeper devices.

An attempt to access the World Health Organization’s HIV/AIDS site (http://www.who.int/topics/hiv_aids/) on the ISP Zain was categorized as Pornography and

blocked using the following iframe:

```
<iframe src="http://restrict.kw.zain.com:8080/webadmin/deny/index.
php?dpid=1&dpruleid=3&cat=23&ttl=-200&groupname=Subscribers&policyname=s
ubscribers&username=[REDACTED]&userip=[REDACTED]&connectionip=127.0.0.1&n-
sphostname=SSB-NS-PS01&protocol=policyprocessor&dplanguage=-&url=http%3a%2f%
2f205%2e185%2e216%2e10%2ftopics%2fhiv%5faids%2f" width="100%" height="100%"
frameborder=0></iframe>
```

Visiting the domain restrict.kw.zain.com from the iframe returns the blockpage in **Figure 2.3**.

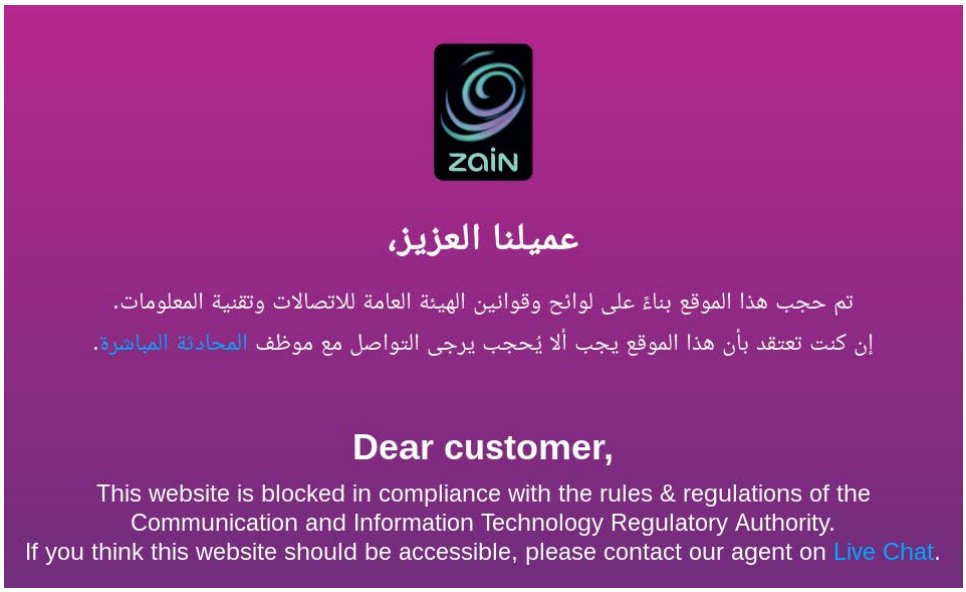

Figure 2.3. Blockpage returned on the ISP Zain in Kuwait in April 2018.

An attempt to access LGBT news and opinion site Vanguard Blog (https://vanguardnow.org/) was blocked on Fasttelco as follows:

```
<iframe src="http://blocked.fasttelco.net/?dpid=27&dpruleid=77&cat=23&ttl=-
200&groupname=FT_CLIENTS
&policyname=FT_CLIENTS_Policy&username=[REDACTED]&userip=
[REDACTED]&connectionip=127.0.0.1&nsphostname=localhost.localdomain&protocol=polic
yprocessor&dplanguage=-&url=http%3a%2f%2f104%2e28%2e28%2e43%2f" width="100%"
height="100%" frameborder=0></iframe>
```

The blockpage in **Figure 2.4** was displayed when accessing the domain seen in the iframe: http://blocked.fasttelco.net.

Figure 2.4. Blockpage displayed from the ISP Fasttelco in Kuwait.

2.5.3.2 Examples of blocked content

Blockpages were returned mentioning the following categories in Kuwait:

- Abortions
- Alcohol
- Custom
- Gambling
- Hate Speech
- Multiple
- Nudity
- Phishing
- Pornography
- Sex Education
- Substance Abuse
- Viruses

Kuwait is the only country case in our data set where we found blockpages mentioning the 'Abortions' category.

In total, 437 URLs were found to be blocked at least once on a network in Kuwait. We observed a large number of obvious miscategorziations, particuarly in the

'Pornography' category. In many cases, these blocks were intermittent.

Miscategorizations

Four URLs on the World Health Organization's website were blocked as a result of being categorized as 'Pornography':

- http://www.who.int
- http://www.who.int/influenza/human_animal_interface
- http://www.who.int/reproductivehealth
- http://www.who.int/topics/hiv_aids/

A number of other sites appear to have been miscategorized as 'Pornography':

Website Description	URLs
Bing Search Engine	http://www.bing.com
	http://www.bing.com/translator/
The Christian Science Monitor	http://www.csmonitor.com
Center for Health and Gender Equity	http://www.genderhealth.org/
International Institute for Counter-Terrorism	http://www.ict.org.il
Islamic Relief Worldwide	http://www.islamic-relief.org/
Islam Today	http://www.islamtoday.net/
Jewish Defense League	http://www.jdl.org
News Agency Reuters	http://www.reuters.com
Radio France Internationale	http://www.rfi.fr
The Times of Israel	http://www.timesofisrael.com
LGBT news and opinion site Gay Today	http://gaytoday.com/
Middle East Transparent	http://metransparent.net/
	http://metransparent.net/forum/
Jainism Global Resource Center	http://jainworld.com/
LGBT site Vanguard Blog	http://vanguardnow.org
Linux distribution site Backtrack Linux	http://www.backtrack-linux.org
Environmental organization Earth Action	http://www.earthaction.org/
World Union for Progressive Judaism	http://wupj.org

Table 2.15. Non-pornographic websites observed categorized as Pornography in Kuwait

The following Arabic websites were also miscategorized as 'Pornography.' Some of these websites have political content.

Website Description	URLs
News portal about Islamist groups	http://islamion.com/
Egypt-focused news portals	http://omeldunya.com/
	http://www.caironewss.com/
Iraq-focused news portal	http://saymar.org/
Kuwait Progressive Movement	http://taqadomi.com/
A regional human rights monitor website	http://humum.net/
Arabic news portal	http://kitabat.com/

Table 2.16. Arabic websites observed categorized as Pornography in Kuwait

A series of blogspot URLs were categorized as 'Viruses' in some measurement tests and 'Custom' in others. It is unclear why such miscategorizations were observed. Kuwait results show that out of the total 437 URLs, there were 45 URLs (10 percent) where iframe injections had the same URL being categorized as more than one category. This high rate of categories per URL is unusual in our data and the only other country in which we observe a similar rate is the United Arab Emirates, where we see 12 percent of blocked URLs being associated with more than one category.

The website of Arabic Network for Human Rights Information website, which is a regional free speech advocacy group critical of human rights records in the Arab world, is blocked (http://www.hrinfo.net). The Kuwait page on the website is also blocked (http://www.hrinfo.net/kuwait/). Both of these URLs were categorized as 'Nudity.'

The website of the LGBT personals application Scruff (http://www.scruff.com/) was blocked, categorized as 'Phishing,' 'Pornography,' and 'Custom.'

Testing of a non-existant Tumblr page (http://thiswebsitedoesnotexistyet.tumblr.com) was found to be blocked in the 'Custom' category.

2.6 Pakistan

Worldwide Governance Indicators for Pakistan		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-0.69	28.57
Political stability and absence of violence/ terrorism	-2.47	1.43
Government effectiveness	-0.64	28.85
Regulatory quality	-0.64	27.40
Rule of law	-0.83	20.19
Control of corruption	-0.86	19.23

Table 2.17. World Bank Worldwide Governance Indicators for Pakistan (2016 data)
Source: World Bank Worldwide Governance Indicators, 2017

2.6.1 Background

The military continues to exercise undue influence over the civilian government of Pakistan, especially since the ouster of Prime Minister Nawaz Sharif on corruption charges in July 2017. In March 2017, the parliament reinstated secret military courts to try people accused of terrorism. These terrorism courts have been used to prosecute cases unrelated to terrorism, including that of a man who was sentenced to death for blasphemy after engaging in an online debate about Islam with an undercover counterterrorism agent.

Members of religious minorities face severe legal discrimination, including a ban on propagating their faith and building houses of worship. There have also been incidents of mob violence and other vigilante attacks against religious minorities.

Transgender women, especially those who advocate for their community, face a high risk of violence or murder. Homosexual sex remains criminal. The government took modest steps towards recognizing the existence of transgender people in 2017 by issuing the first ID with a transgender category.

2.6.2 Information controls in Pakistan

A 2016 law strengthened Pakistani authorities' powers to detain and punish individuals for critical online speech. Since 2017, dozens of people have been interrogated, arrested, or abducted by security forces for posting critical comments about dominant religious groups or state authorities.

NGOs and independent news media are subject to violence and harassment by state and private actors, which prompts self-censorship. In July 2017, the UN Committee on Economic, Social, and Cultural Rights expressed deep concern over the treatment of human rights defenders in Pakistan; just a few months later in November 2017, the government expelled 29 international NGOs from the country.

Religious expression is severely constrained by criminal laws. Violation of such laws can result in a death penalty decision in some cases. Nineteen people were under death sentences for blasphemy in 2017 and hundreds more awaited trial. State authorities sent a mass text message to millions of citizens in May 2017 that warned them that uploading or sharing blasphemous content was a crime. In April 2017, a mob seized and murdered a 23-year-old university student, Mashal Khan, after rumours circulated that he had criticized Islam.

The NGO Access Now reported two national Internet shutdowns and four regional shutdowns in 2016 and three local or regional shutdowns in 2017. According to Access, shutdowns are most often justified on national security grounds and affect wireline Internet service in most cases—wireless data, SMS, and telephone services were sometimes interrupted.

Previous research has identified Netsweeper installations in Pakistan that were used to implement political and social Internet filtering, including blocking independent news websites, religious content, and human rights information.

2.6.3 Data analysis

2.6.3.1 Evidence of Netsweeper presence

We found 20 IP addresses in Pakistan that were part of Netsweeper installations (shown in **Table 2.18**). Behavioral validation results are shown in **Table 2.19**.

AS Name	AS Number	IP Address	Date first seen	Date last seen
Pakistan Telecommunication Company Limited	17557	202.125.134.154	2017-08-31	2018-04-04
Paknet Limited Merged into PTCL	9557	119.159.224.77	2017-08-31	2018-04-04
Paknet Limited Merged into PTCL	9557	119.159.224.76	2017-08-31	2018-04-04
Paknet Limited Merged into PTCL	9557	119.159.224.75	2017-08-31	2017-11-01
Paknet Limited Merged into PTCL	9557	119.159.224.74	2017-08-31	2017-09-07

AS Name	AS Number	IP Address	Date first seen	Date last seen
Paknet Limited Merged into PTCL	9557	119.159.224.73	2017-08-31	2017-11-01
Paknet Limited Merged into PTCL	9557	119.159.224.72	2017-08-31	2017-11-15
Paknet Limited Merged into PTCL	9557	119.159.224.70	2017-08-31	2017-11-15
Paknet Limited Merged into PTCL	9557	119.159.224.69	2017-08-31	2017-11-01
Paknet Limited Merged into PTCL	9557	119.159.224.68	2017-08-31	2018-04-04
Paknet Limited Merged into PTCL	9557	119.159.224.109	2017-08-31	2017-11-01
Paknet Limited Merged into PTCL	9557	119.159.224.108	2017-08-31	2017-10-25
Paknet Limited Merged into PTCL	9557	119.159.224.107	2017-08-31	2017-09-27
Paknet Limited Merged into PTCL	9557	119.159.224.106	2017-09-27	2017-11-01
Paknet Limited Merged into PTCL	9557	119.159.224.105	2017-08-31	2017-09-27
Paknet Limited Merged into PTCL	9557	119.159.224.104	2017-08-31	2017-11-01
Paknet Limited Merged into PTCL	9557	119.159.224.103	2017-08-31	2017-09-27
Paknet Limited Merged into PTCL	9557	119.159.224.102	2017-09-27	2017-10-18
Paknet Limited Merged into PTCL	9557	119.159.224.101	2017-08-31	2017-09-27
Paknet Limited Merged into PTCL	9557	119.159.224.100	2017-09-27	2017-10-04

Table 2.18. Netsweeper installations identified in Pakistan

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr hostname
202.125.134.154	Pakistan Telecommunication Company Limited									
119.159.224.100	Paknet Limited Merged into PTCL									KHI494-NSP-01
119.159.224.101										KHI494-NSP-02
119.159.224.102										KHI494-NSP-03
119.159.224.103										KHI494-NSP-04
119.159.224.104										KHI494-NSP-05
119.159.224.105										KHI494-NSP-06
119.159.224.106										KHI494-NSP-07
119.159.224.107										KHI494-NSP-08
119.159.224.108										KHI494-NSP-09
119.159.224.109										KHI494-NSP-10
119.159.224.68										KHI275-NSP-01
119.159.224.69										KHI275-NSP-02
119.159.224.70										KHI275-NSP-03
119.159.224.72										KHI275-NSP-05
119.159.224.73										KHI275-NSP-06
119.159.224.74										KHI275-NSP-07
119.159.224.75										KHI275-NSP-08
119.159.224.76										KHI275-NSP09
119.159.224.77										KHI275-NSP-10

Table 2.19. Behavioural validation test results from Pakistan

All 20 devices produced a positive result to at least one of the behavioural tests. Notably, the 19 devices on ASN9557 (PTCL) returned similar SNMP sysdesc values that contained text referring to Netsweeper ("netsw"); this indicated that each were part of a larger Netsweeper installation on that ISP.

2.6.3.2 Examples of blocked content

Network measurement data from Pakistan produced nine observed cases of filtering. Blockpages were returned mentioning the following categories:

- Pornography
- Custom

Our 2013 report on the use of Netsweeper in Pakistan found 123 URLs blocked, far more than those found in this most recent round of testing. A 2017 report published by OONI identified 210 websites blocked through methods including DNS tampering and transparent HTTP proxies. OONI's report did not identify Netsweeper products or those of any other vendors as being used to implement censorship. Given that our Netsweeper signatures were limited to transparent blockpages and excluded DNS tampering, this could explain the lower number of URLs we found blocked. It is possible that censorship in Pakistan has shifted to a different method (i.e., DNS tampering) or is being implemented with alternative systems. Further research is required to identify any additional vendors responsible for censorship in Pakistan.

2.7 Qatar

Worldwide Governance Indicators for Qatar		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.20	15.76
Political stability and absence of violence/ terrorism	0.87	76.19
Government effectiveness	0.75	74.52
Regulatory quality	0.70	74.04
Rule of law	0.86	79.33
Control of corruption	0.92	79.81

Table 2.20. World Bank Worldwide Governance Indicators for Qatar (2016) Source: World Bank Worldwide Governance Indicators, 2017 data)

2.7.1 Background

Human rights groups have raised concerns around political rights and free expression in Qatar and over discrimination against certain social groups. Independent political parties are illegal in Qatar, as are most workers' associations. Qatari nationals can form associations under certain conditions. Migrant workers, who do not have nationality, are prevented from organizing unions or other organizations to advocate for their rights. Partly as a result of their lack of representation, these workers have experienced abuse and exploitation — despite some steps in the direction of workers' rights. The State of Qatar also discriminates against women and LGBTQ people. Women do not have equal rights regarding marriage, freedom of movement, and the ability to pass nationality on to their children. Qatar punishes sodomy with one to three years in prison.

2.7.2 Information controls in Qatar

The law in Qatar criminalizes expressions considered offensive to the Emir of the state. The censors ban citizens from accessing various web content categories that the government deems objectionable. In 2009, as part of our participation in the ONI project, Citizen Lab documented that the blocked content categories included political criticism, pornography, websites deemed offensive to Islam, LGBT, dating, escorting services, sex education, and online privacy and circumvention tools. In March 2011, we provided evidence that Netsweeper technology was used by the national ISP Qtel. In May 2011, we revealed more evidence that showed that the national ISP used Netsweeper technology and its URL database.

Reports of Internet blocking continue to emerge. In November 2016, the ISPs Vodafone and Ooredoo blocked the English news website Doha News (https://dohanews.co). Amnesty International officials described the blocking as "an alarming setback for freedom of expression in the country" and an "outright attack on media freedom." Reporters Without Borders reports that journalists in Qatar practice self-censorship because of the "draconian system of censorship." Criticism of the government, royal family, and Islam can lead to imprisonment. Moreover, a 2014 cybercrime law criminalizes posting "false news" online.

2.7.3 Data analysis

2.7.3.1 Evidence of Netsweeper presence

We found eight IP addresses in Qatar that were part of Netsweeper installations (shown in **Table 2.21**). Behavioral validation results are shown in **Table 2.22**.

AS Name	AS Number	IP Address	First seen date	Last seen date
Ooredoo Q.S.C.	8781	82.148.98.222	2017-08-31	2018-04-04
Ooredoo Q.S.C.	8781	82.148.98.218	2017-08-31	2017-11-29
Ooredoo Q.S.C.	8781	82.148.98.210	2017-08-31	2018-04-04
Ooredoo Q.S.C.	8781	82.148.116.98	2017-08-31	2018-04-04
Ooredoo Q.S.C.	8781	82.148.116.110	2017-08-31	2018-04-04
Ooredoo Q.S.C.	8781	82.148.116.106	2017-08-31	2018-04-04
Ooredoo Q.S.C.	8781	82.148.116.102	2017-08-31	2018-04-04
Ooredoo Q.S.C.	8781	82.148.100.101	2017-08-31	2018-04-04

Table 2.21. Netsweeper installations identified in Qatar

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	snmp sysdescr hostname	rdns
82.148.100.101	Ooredoo Q.S.C.										mail.dreamsgroup.com.qa
82.148.116.102										WAC-NSW2-CLU3	ge-wac-nsw.qatar.net.qa
82.148.116.106										KTC-NSW1-CLU3	ge-ktc-nsw1.qatar.net.qa
82.148.116.110										KTC-NSW2-CLU3	ge-ktc-nsw2.qatar.net.qa
82.148.116.98										WAC-NSW1-CLU3	ge-wac-nsw.qatar.net.qa
82.148.98.210										WAC-NSW1-CLUSTER4	
82.148.98.218										REC-NSW1-CLUSTER4	
82.148.98.222										REC-NSW2-CLUSTER4	

Table 2.22. Behavioural validation test from Qatar

As shown above, most of the non-blank SNMP sysdesc values followed a relatively consistent naming scheme which included a reference to Netsweeper ("ns"). The blocking behaviour further confirmed that these devices were in use on a consumer-facing ISP. Blocking was implemented through an iframe redirection, as shown in this example of an attempt to access circumvention tool Hotspot Shield:

```
<iframe src="http://www.censor.
qa/?dpid=1&dpruleid=78&cat=105&ttl=
0&groupname=filter&policyname=default&username=[REDACTED]&userip=[REDACTE
D]&connectionip=127.0.0.1&nsphostname=rec-nsw1-clu2&protocol=policyprocessor&-
dplanguage=-&url=http%3a%2f%2fwww%2ehotspotshield%2ecom%2f" width="100%"
height="100%" frameborder=0></iframe>
```

This iframe would return the following blockpage from the URL http://www.censor.qa:

Figure 2.5. Blockpage from Qatar.

2.7.3.2 Examples of blocked content

Blockpages were returned mentioning the following categories in Qatar:

- Custom
- Pornography

The URLs added to the 'Custom' category included Hezbollah-affiliated satellite television station Al Manar (http://www.almanar.com.lb), circumvention tool Hotspot Shield (http://www.hotspotshield.com), and a site critical of Islam (http://www.prophetofdoom.net).

2.8 Somalia

Worldwide Governance Indicators for Somalia		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.83	2.96
Political stability and absence of violence/terrorism	-2.33	2.86
Government effectiveness	-2.18	0.48
Regulatory quality	-2.27	0.96
Rule of law	-2.37	0.00
Control of corruption	-1.69	0.48

Table 2.23. World Bank Worldwide Governance Indicators for Somalia (2016 data) Source: World Bank Worldwide Governance Indicators, 2017

2.8.1 Background

Somalia continues to suffer what the UN Office of the High Commissioner for Human Rights describes as a "human rights crisis." This crisis is characterized by serious violations of human rights and humanitarian law. Millions of people in Somalia lack basic physical security, food, and access to humanitarian aid, in part because of ongoing armed conflict within the country.

Within this context, free expression and access to information are severely constrained, both by lack of resources and by the actions of the government and other groups. A 2017 Amnesty International report indicated that Al-Shabab has continued to prevent journalists from working in regions under its control through strategies of detaining, threatening, and harassing media workers throughout Somalia.

2.8.2 Information controls in Somalia

The government of Somalia passed a new law in 2017 that gave it broad and vague powers to prohibit "propaganda" and false news. The law has been used against critical journalists and as justification to arrest more than 30 journalists last year. In the autonomous region of Somaliland, the Somaliland Journalist Association stated that more than 30 journalists were arrested and detained by Somaliland authorities on charges of criticizing the government in 2017.

Authorities in Puntland have also arbitrarily detained journalists and other civilians for denouncing the region's leadership and judicial decisions. In July 2017, journalist Ahmed Ali Kilwe was detained by counter-terrorism police and held for two weeks without charge, allegedly on the grounds of criticizing the president.

In 2016, Somali ISPs blocked 29 websites, most of which are owned by members of the Somali diaspora and had been critical of leaders of the Federal Government of Somalia and government practices. Prior Citizen Lab research in 2014 found Netsweeper installations on three Somali ISPs, and demonstrated that one of these installations was used to block pornography and anonymization and circumvention tools. Internet penetration in Somalia remains below 2 percent and has grown slowly over the last decade.

2.8.3 Data analysis

2.8.3.1 Evidence of Netsweeper presence

We found seven IP addresses in Somalia that were part of Netsweeper installations

(shown in **Table 2.24**). Behavioral validation results are shown in **Table 2.25**.

AS Name	AS number	IP address	Data first seen	Data last seen
Golis-Telecom-AS	328250	41.223.109.101	2018-03-14	2018-04-04
HORMUUD	37371	41.78.75.140	2017-08-31	2018-04-04
HORMUUD	37371	41.78.74.138	2017-08-31	2018-04-04
HORMUUD	37371	41.78.72.115	2017-08-31	2018-04-04
HORMUUD	37371	41.78.72.114	2017-11-24	2018-04-04
HORMUUD	37371	41.78.73.113	2017-08-31	2018-04-04
O3b Limited	60725	41.223.111.147	2017-08-31	2018-04-04

Table 2.24. Netsweeper devices identified in Somalia

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr hostname
41.223.109.101	Golis-Telecom-AS									Linux bosaso-ns-ps01
41.78.73.113	HORMUUD									hormuud_ps02
41.78.72.114										
41.78.72.115										Linux netsweeper2.hortel.net
41.78.74.138										Linux hormuud_ps01
41.78.75.140										Linux hormuud-remote_nsps01
41.223.111.147	O3b Limited									Linux Golis-NS3

Table 2.25. Behavioural validation tests in Somalia

All of the devices identified returned a true value for at least one of the behavioural tests. Five of the six SNMP sysdesc values referenced Netsweeper-related terms and the names of the affected ISPs.

Censorship was implemented through an iframe redirection, as shown in this example of a block delivered to a request for peer-to-peer file sharing site http://www.bittorrent.com:

```
<iframe src="http://41.78.72.114:8080/webadmin/deny/?dpid=75" width="100%"
height="100%" frameborder=0></iframe>
```

During testing, we were unable to retrieve the injected blockpage, although we did see this same IP address in our 2014 report on Somali Netsweeper installations. The image presented to users in 2014 is shown in **Figure 2.6**.

Figure 2.6. A blockpage on Somali IP 41.78.72.114 as seen in 2014.

2.8.3.2 Examples of blocked content

There were no category codes present in any blockpage collected. Only three URLs were identified as blocked in Somali measurement data: a file-sharing site (http://www.bittorrent.com), a gambling website (http://www.clubdicecasino.com), and a circumvention tool website (http://hidemyass.com).

2.9 Sudan

Worldwide Governance Indicators for Sudan		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.80	3.45
Political stability and absence of violence/terrorism	-2.38	2.38
Government effectiveness	-1.41	7.21
Regulatory quality	-1.49	4.81
Rule of law	-1.26	9.13
Control of corruption	-1.61	1.44

Table 2.26. World Bank Worldwide Governance Indicators for Sudan (2016 data) Source: World Bank Worldwide Governance Indicators, 2017

2.9.1. Background

The government of Sudan represses and violates basic civil and political rights and restricts religious freedoms.

The country's security agency has detained student activists, human rights defenders, journalists, and opposition members, and prevented opposition political groups

and civil society organizations from holding meetings and peaceful assemblies. The authorities restrict the construction of new churches and have closed one church over a dispute over administration of churches.

2.9.2. Information controls in Sudan

Sudanese authorities severely restrict journalists from covering any issue the government deems to create a security threat. On dozens of occasions in 2017, authorities confiscated copies of newspapers as they came off the presses in order to prevent their distribution.

Journalists are regularly investigated and summoned for questioning by the country's intelligence agency. Some have been convicted of covering topics that threaten security. In September 2017, the editor-in-chief of *Akhbar Alwatan* newspaper was arrested and beaten by intelligence forces after his paper reported on a land dispute.

In early 2018, 18 journalists were arrested while covering a protest and an independent radio station was forced to shut down. Sudanese journalists have turned to online publications and social media to avoid restrictions on print and broadcast media.

Sudan's National Telecommunication Corporation (NTC) maintains and openly acknowledges a filtering process under which a special unit screens web content and handles blocking requests. In 2009, NTC stated that it blocks pornography and sites "related to narcotics, bombs, alcoholics, gambling, and blasphemous sites normally offensive to Islam." Authorities have also pursued individuals who posted critical comments online.

2.9.3 Data analysis

2.9.3.1 Evidence of Netsweeper presence

We found four IP addresses in Sudan that were part of Netsweeper installations (shown in **Table 2.27**). Behavioral validation results are shown in **Table 2.28**.

AS Name	AS number	IP address	Date first seen	Date last seen
KANARTEL	33788	197.254.192.38	2017-08-31	2018-04-04
KANARTEL	33788	197.254.192.34	2017-08-31	2018-04-04
KANARTEL	33788	196.29.164.27	2017-08-31	2018-04-04
Sudatel	15706	196.1.211.4	2017-08-31	2018-04-04

Table 2.27. Netsweeper devices identified in Sudan

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	sysdescr_hostname
196.29.164.27	KANARTEL									
197.254.192.34										NSPS01
197.254.192.38										NSPS02
196.1.211.4	Sudatel									NS-PS01

Table 2.28. Behavioural validation tests on devices in Sudan

All four of these devices returned true values for at least one of our behavioural tests and three of four had SNMP sysdesc values that referenced Netsweeper (e.g. “NSPS01” which could stand for Netsweeper Policy Server).

Blocking was implemented through an injected iframe on both ISPs, such as this example of a blockpage returned in response to an attempt to access a gambling website (http://www.monacogoldcasino.com):

```
<iframe src=”http://196.29.164.27/ntc/ntcblock.html?dpid=1&dpruleid=3&cat=10&ttl=-
200&groupname=Canar_staff&policyname=canar_staff_policy&username=[REDACTED]&
userip=[REDACTED]&connectionip=127.0.0.1&nsphostname=NSPS01&protocol=policyp
rocessor&dplanguage=-&url=http%3a%2f%2fwww%2emonacogoldcasino%2ecom%2f”
width=”100%” height=”100%” frameborder=0></iframe>
```

Attempting to access the blocked page returned the blockpage seen in **Figure 2.7**.

Figure 2.7. A blockpage seen on Kanartel in Sudan.

On Sudatel, an injected iframe was also returned, such as this example of requesting the URL of a file sharing site http://thepiratebay.org:

```
<iframe src="http://196.1.211.4:8080/webadmin/deny/index.
php?dpid=4&dpruleid=1&cat=23&ttl=-200&groupname=Sudatel_
subscribers&policyname=sudatel_subscribers&username=[REDACTED]&userip=[REDAC
TED]&connectionip=127.0.0.1&nsphostname=NS-PS01&protocol=policyprocessor&dpla
nguage=-&url=http%3a%2f%2fthepiratebay%2eorg%2f" width="100%" height="100%"
frameborder=0></iframe>
```

Attempting to access the file sharing site delivered the blockpage in **Figure 2.8**.

2.9.3.2 Examples of blocked content

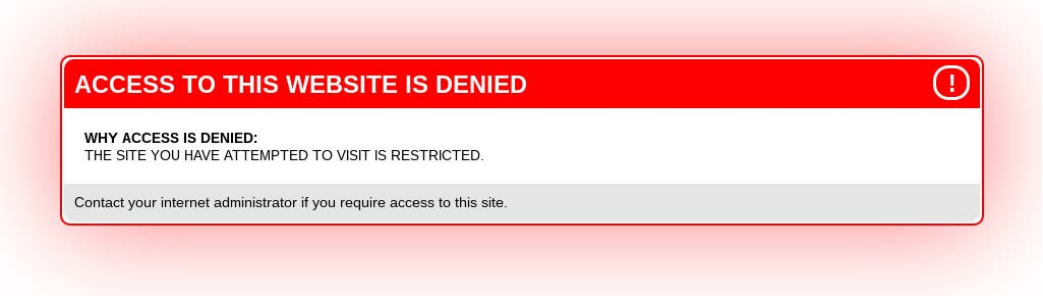

Figure 2.8. Blockpage displayed on Sudatel in Sudan.

Blockpages were returned mentioning the following categories:

- Alcohol
- Gambling
- Pornography
- Web Proxy

In addition to the above categories, we also used Netsweeper's Deny Page Test tool. This is a web application made for administrators of Netsweeper installations to verify which categories are being blocked. We accessed the web application on February 25, 2018 within Sudan and determined these additional categories as being blocked:

- Nudity
- Occult
- Profanity
- Sex Education

2.10 UAE

Worldwide Governance Indicators for UAE		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.12	19.21
Political stability and absence of violence/terrorism	0.44	60.95
Government effectiveness	1.41	90.87
Regulatory quality	0.97	80.29
Rule of law	0.89	79.81
Control of corruption	1.28	88.46

Table 2.29. World Bank Worldwide Governance Indicators for UAE (2016 data) Source: World Bank Worldwide Governance Indicators, 2017

2.10.1 Background

The UAE is a member of the Saudi-led military coalition operating in Yemen, which has carried out attacks on civilians that Human Rights Watch says likely amount to war crimes. The UAE also supports Yemeni counterterrorism operations, during which Yemeni forces have perpetrated human rights abuses against the civilian population. The UAE runs informal detention centres in Yemen, where suspects are arbitrarily detained. There have been reports of torture and extremely harsh treatment of prisoners in these detention centres and in the UAE's domestic prisons.

Certain social groups in the UAE face similar conditions to those in other countries in the region. International watchdogs remain concerned about ongoing exploitation of migrant workers, although the government has implemented laws around working conditions. Workers are not permitted to organize for their rights or form unions.

Legal protections against violence against women in the UAE, especially abuse by family members, fall short of international standards. Women remain subject to legal discrimination in marriage, inheritance, and custody matters. Same-sex relations and extramarital sex carry prison terms under "indecency" laws.

2.10.2 Information controls in UAE

UAE authorities restrict the rights to freedom of expression and association, and detain and prosecute government critics, opponents, and foreign nationals under criminal defamation and anti-terrorism laws.

The UAE also prohibits a broad range of vaguely worded online activities that can fall within internationally-protected expression. For example, Federal Decree Law no. (5) of 2012 criminalizes the publication of "information, news, statements or rumors on a website or any computer network or information technology means with intent to make sarcasm or damage the reputation, prestige or stature of the State or any of its institutions or its president, vice-president, any of the rulers of the Emirates, their crown princes, or the deputy rulers of the Emirates, the State flag, the national peace, its logo, national anthem or any of its symbols."

The same law also prohibits using the Internet to plan, organize, promote, or call for demonstrations or protests without license from the competent authority. The law also bans religious criticism such as insulting Islamic or other religious sanctities or rituals. In this restrictive context, the state censors in the UAE are believed to use Netsweeper Internet filtering technology to enable mass filtering of a broad range of content categories and prevent citizens from exercising their right to free access to information online. Among the content blocked using Netsweeper is political dissent, news websites, religious criticism, and tools that provide for anonymous browsing of the Internet. In addition, there are documented electronic spyware attacks against UAE dissidents, including the internationally-recognized human rights activist Ahmed Mansoor, who in April 2018 was brought to trial in the UAE after more than a year in prison.

2.10.3 Data analysis

2.10.3.1 Evidence of Netsweeper presence

We found three IP addresses in the UAE that were part of Netsweeper installations (shown in **Table 2.30**).

ISP	AS Name	IP Address	AS Number	Date first seen	Date last seen
du	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	5.32.4.201	15802	2017-11-24	2018-04-04
du	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	5.32.6.164	15802	2017-11-24	2018-04-04
du	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	94.206.70.244	15802	2017-08-31	2018-04-04

Table 2.30. Netsweeper devices identified in the UAE

These three devices returned no results for a single behavioural validation test. However, all were observed in OONI measurement data sending blockpage responses.

Blocking was implemented through an HTTP 302 redirect. For example, an attempt to access LGBT civil rights organization the Human Rights Campaign (http://www.hrc.org) would result in a 302 redirect to the URL:

http://lighthouse.du.ae/?dpid=1&dpruleid=3&cat=41&dplanguage=-&url=http%3a%2f%2fwww%2ehrc%2eorg%2f

Accessing the URL contained displays the blockpage seen in **Figure 2.9**.

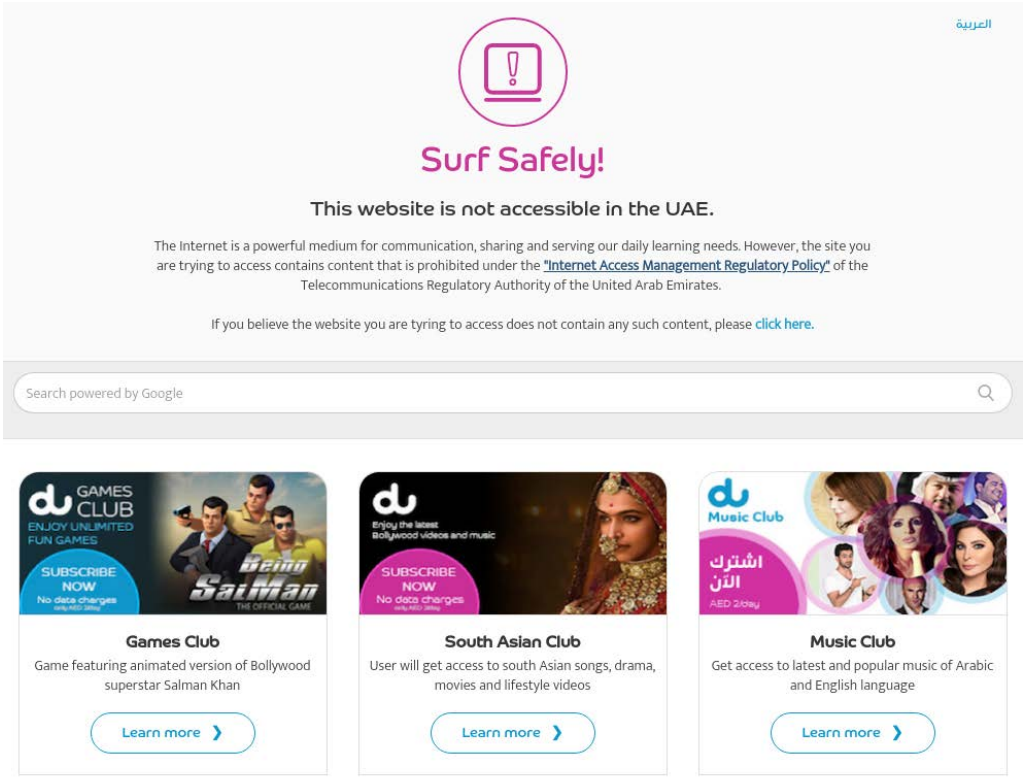

Figure 2.9. Blockpage displayed to users of UAE-based ISP du

The blockpage contains du branding, contains a link to the UAE Telecommunications Regulatory Authority's "Internet Access Management Regulatory Policy," and links to a form that allows a user to flag a website believed to be blocked in error.

2.10.3.2 Examples of blocked content

In total, we found 548 unique URLs to be blocked with blockpages mentioning the following categories:

- Alternative Lifestyles
- Custom
- Pornography
- Web Proxy
- Multiple

In addition to looking at measurement data, we conducted user testing of certain URLs. The URLs that were determined to be verified blocked through this method are denoted with an asterisk (*).

Local and UAE-focused websites

The UAE's government censors block websites that have critical political content and websites run by local activists. Some of these activists conduct campaigns to free people who they describe as political prisoners or advocates for political reform.[5]

Local political websites with critical content include:

- EMASC (*http://www.emasc-uae.com/)
- Al-Islaah (*http://alislaah.net/site/)
- Emirati Affairs (*http://emirati-affairs.com/)

Campaign websites, which demand the release of political prisoners, include:

- The Seven Emiraties (*http://sevenuae.blogspot.com/)
- UAE71 (*http://www.emirates71.org/)

Websites that discuss human rights practices in UAE prisons include:

- UAEDetainees (http://www.uaedetainees.com)
- UAEPrison (*http://www.uaeprison.com)
- UAETorture (http://www.uaetorture.com)

Regional news websites include:

- NoonPost (*http://www.noonpost.net/)
- SasaPost (*http://www.sasapost.com/)
- Watan (*http://www.watan.com)
- Arab Times (*http://www.arabtimes.com/)
- Arabi 21 (*http://arabi21.com/)
- Asrar Arabiya (*http://asrararabiya.com/)

5 The URLs in this section were found blocked using the ad-hoc censorship testing methodology

- The New Khalij (*http://www.thenewkhalij.net/)
- Al Araby (*http://www.alaraby.co.uk/)

Religious criticism, conversion, and atheism

The censors also block Arabic websites that are critical of Islam and websites that discuss other religious issues, including atheism. Among the religious criticism and conversion websites[6] are:

- The Good Way (*http://www.the-good-way.com)
- The Koran (*http://www.thekoran.com)<
- The Religion of Peace (*http://www.thereligionofpeace.com)

Arabic atheist websites include:

- Arab Atheist Broadcasting (*http://arabatheistbroadcasting.com)
- Ladeeni (*http://www.ladeeni.net)

Other sites in this category include:

- The Debate (http://www.debate.org.uk)
- St Columba's Parish Church (http://www.stcolumbas.org)
- Submission (http://www.submission.org)
- Trinity Lutheran.org (http://www.trinity-lutheran.org)

Alternative Lifestyles

The Netsweeper device installations we found in UAE were the only installations identified that blocked the 'Alternative Lifestyles' category. This content category is described by Netsweeper as follows:

> **"This includes …sites that reference topics on habits or behaviors related to social relations, dress, expressions, or recreation that are important enough to significantly influence the lives of a sector of the population. It can include the full range of non-traditional sexual practices, interests and orientations. Some sites may contain graphic images or sexual material with no pornographic intent."**

As discussed in subsection 1.2, Netsweeper's decision to include this as a category in their system has facilitated the wholesale blocking of non-pornographic LGBT content. In testing on the ISP du, we saw the following websites blocked as a result of their categorization as "Alternative Lifestyles" content:

6 The URLs in this section were found blocked using the ad-hoc censorship testing methodology

- Gay & Lesbian Alliance Against Defamation (http://www.glaad.org/)
- Human Rights Campaign (http://www.hrc.org/)
- The International Lesbian, Gay, Bisexual, Trans and Intersex Association (http://ilga.org/)
- The Los Angeles LGBT Center (http://www.gay.com)
- Gay Men's Health Centre (http://www.gmhc.org)
- The International Foundation for Gender Education (http://www.ifge.org)
- Kwir Media, an LGBT news and culture site (*https://www.kwirmedia.com/)
- Queerty, an LGBT online magazine (http://www.queerty.com)

A number of other websites were blocked as a result of their categorization as 'Alternative Lifestyles,' although they do not appear to contain content that matched the category description:

- Caritas International, a Catholic relief, social services, and development organization (http://www.caritas.org)
- Freeservers web-hosting (http://www.freeservers.com/)

The 'Custom' list

The category most observed in the data for UAE was 'Custom' (44 percent). Within this category, a number of sites offering VoIP services were found to be blocked, including:

- Vonage (http://www.vonage.com)
- VoicePulse (http://www.voicepulse.com)
- MyWebCalls (http://www.mywebcalls.com)
- fring (http://www.fring.com/)
- Efonica (http://www.efonica.com)

The blocking of VoIP services in the country has been widely reported dating back to 2007.

In addition, websites that offer censorship circumvention or anonymization were also blocked, including:

- IPVanish (https://www.ipvanish.com/)
- Hotspot Shield (https://www.hotspotshield.com/)

- HTTP Tunnel (*http://www.httptunnelclient.com/html/)
- Anonymizer (https://www.anonymizer.com/)
- Ultrasurf (http://ultrasurf.us)
- Freegate (http://download.cnet.com/freegate/3000-2085_4-10415391.html)
- BTGuard (https://btguard.com/)

Three URLs of dictionary and translation sites were also blocked. The translation features of such sites have been used as a form of censorship circumvention. Those URLs are:

- Dictionary.com (http://dictionary.reference.com)
- Reference.com (http://translate.reference.com)
- Dictionary.com (http://www.dictionary.com/)

Miscellaneous

The following URLs were included in the 'Custom' category and thus access to them was blocked:

- Greenpeace (http://www.greenpeace.org; http://www.greenpeace.org/international/)
- Square Enix, a video game developer (http://www.square-enix.com)
- Equal Marriage for Same-Sex Couples (http://www.samesexmarriage.ca)
- Cocaine.org, a drug rehabilitation service (http://cocaine.org/)

Intermittent blocking

Some websites were found as being blocked during some test runs but were accessible during later tests. Examples include the website of The Telegraph (https://www.telegraph.co.uk/), which was found blocked in October 2017, but was later found to be accessible. It is not clear why the blocking occurred and why it ceased.

Miscategorization

Among the blocked websites are some that appear to be blocked as a result of miscategorization by the Netsweeper categorization services. Notable examples include the website of the World Health Organization (http://www.who.int), which was found blocked during a November 2017 test. The test showed that it was miscategorized as 'Pornography' at the time. Later test runs showed that the website has been made accessible.

The reasons behind these miscategorizations are unclear. Within the data, we see 68 out of 548 URLs (12 percent) where a given URL is assigned to more than one category. This is a high percentage of cases, which is similar only to the Kuwaiti installation results (10 percent). Among all the injections we have seen, the who.int URLs were only seen blocked in both Kuwait and UAE.

2.11 Yemen

Worldwide Governance Indicators for Yemen		
Indicator	**Governance Score (-2.5 to +2.5)**	**Percentile rank**
Voice and accountability	-1.65	5.91
Political stability and absence of violence/ terrorism	-2.79	0.48
Government effectiveness	-1.82	2.40
Regulatory quality	-1.48	5.29
Rule of law	-1.60	4.81
Control of corruption	-1.67	0.96

Table 2.31. World Bank Worldwide Governance Indicators for Yemen (2016 data) Source: World Bank Worldwide Governance Indicators, 2017

2.11.1 Background

Since 2015, Yemen has been engaged in a civil war during which more than 15,000 civilians have been killed or wounded causing a grave humanitarian disaster. On one side of the conflict are the Houthi rebels and forces loyal to former president Ali Abdullah Saleh, with the other consisting of forces loyal to the internationally-recognized president Abd-Rabbu Mansour Hadi, who is supported by a Saudi-led multinationalmilitary coalition. Amnesty International reported that all parties have committed war crimes and other serious violations of international laws. The Houthi-Saleh Forces have bombed civilian residential areas indiscriminately, which has led to deaths and injuries among civilians. The Yemeni government, Yemeni forces aligned with the UAE, and Houthi-Saleh forces are all engaged in illegal detention practices, enforced disappearance, and torture.

2.11.2 Information controls in Yemen

Citizens' access to information, online and off, has been significantly disrupted since the beginning of the war. A 2015 Citizen Lab report found that Netsweeper filtering technology was being used by the national ISP, Yemennet, to filter critical political content, independent media websites, and all URLs belonging to the Israel (.il)

top-level domain. Following the Houthis' capture of the capital Sana'a, Yemennet has been under their control, with the Houthis acting as the *de facto* government of Yemen. Citizen Lab has monitored Internet censorship in Yemen since the publication of the 2015 report and has found that the Houthis have expanded Internet filtering by adding a number of local and regional news websites.

Yemeni media organization and news portal Sahafa.net has complained about Internet censorship, raised the issue of the use of Netsweeper technology to filter political content, and demanded that the Hadi government communicate with Netsweeper, Inc. about the use of its products in Yemen and request that the company discontinue its filtering services. The demand came in a December 2017 press release in which Sahafa.net condemned the significant increase in blocking of websites by the Houthis during their armed clashes with forces loyal to their former ally president, Saleh. Sahafa.net wrote in their press release: "We call on Netsweeper, the company which provides Internet blocking technology, to discontinue its services in Yemen because its product is being used by the armed militia to block social media websites, to violate human rights, and to oppress freedom of opinion and expression and exploit the technology for military purposes."

In December 2017, the *New York Times* reported that "[t]o keep their enemies from conspiring against them, the Houthis have used their control of Yemen's communications infrastructure to shut off access to the Internet for days and to block social media sites like Facebook." The *New York Times* described an admission by a Houthi commander that his group controls the Internet and manipulates it for military purposes. The commander was quoted as saying, "It is not hard … We have telecommunication companies in Sana full of people who have been educated abroad. We had to stop our enemies from communicating with each other."

The use of Netsweeper for military-aligned censorship by the Houthis is supplemented by oppressive legal regulations. The Houthi-controlled Ministry of Information in Sana'a introduced legal restrictions on electronic journalism in October 2017. The act bans operating a news website without a prior license from the ministry and states that websites that publish objectionable content will be banned.

The deployment of Netsweeper technology on Yemen's national Internet network precedes the war and we have previously documented that the company's devices and technologies have been used for political and social filtering and to block Internet privacy and circumvention tools. The use of Netsweeper products during

the war has taken a significant turn: it has been used where warring parties have been accused of violating human rights and blacklisted by the UN for committing war crimes against children. Some of the actors have been sanctioned by the United Nations Security Council, including the Houthi rebel group leader whose group controls the Internet and enforces media and Internet censorship in Yemen. Moreover, results from continued network measurements indicate the use of Netsweeper technology in war propaganda. Specifically, Netsweeper enables Internet censorship that prevents citizens from accessing information related to the war from multiple sources. The websites that remain accessible are those affiliated with the Houthis themselves or those editorially aligned with their political stance on the war.

2.11.3. Data analysis

2.11.3.1 Evidence of Netsweeper presence

We found six IP addresses in Yemen that were part of Netsweeper installations (shown in **Table 2.32**). Behavioral validation results are shown in **Table 2.33**.

AS Name	IP Address	AS Number	First seen	Last seen
Public Telecommunication Corporation	82.114.160.98	30873	2018-01-11	2018-04-04
Public Telecommunication Corporation	82.114.160.94	30873	2017-08-31	2018-04-04
Public Telecommunication Corporation	82.114.160.93	30873	2017-08-31	2018-04-04
Public Telecommunication Corporation	82.114.160.104	30873	2017-08-31	2018-04-04
Public Telecommunication Corporation	82.114.160.103	30873	2017-08-31	2018-04-04
Public Telecommunication Corporation	82.114.160.102	30873	2017-08-31	2018-04-04

Table 2.32. Netsweeper devices identified in Yemen

IP	ASN	ooni	b1	b2	b3	b4	b5	b6	snmp	denypage title	denypage mailto
82.114.160.102	Public Telecommunication Corporation										
82.114.160.103											
82.114.160.104											
82.114.160.93										Access Denied	
82.114.160.94										Untitled document	safenet@yemen.net.ye
82.114.160.98										Access Denied	

Table 2.33. Summary of behavioural validation tests in Yemen

All devices that match at least one behaviour test are on the same ASN “Public Telecommunications Corporation.” Among these, three IPs match more than a single behaviour. Throughout our testing period, the IP 82.114.160.94 displayed a blockpage that contained a link to email address “safenet@yemen.net.ye.” The domain name on this address is the official website of Yemennet and the domain deny.yemen.net.ye resolves to this same IP address.

Within measurement data, attempts to access censored content receive an injected response with an iframe. For example, an attempt to access the website of the circumvention tool Psiphon (http://psiphon.ca) would return the following iframe:

```
<iframe src=”http://82.114.160.94/webadmin/deny” width=”100%” height=”100%” frameborder=0></iframe>
```

Visiting the IP from this injected iframe returns the blockpage seen in **Figure 2.10**.

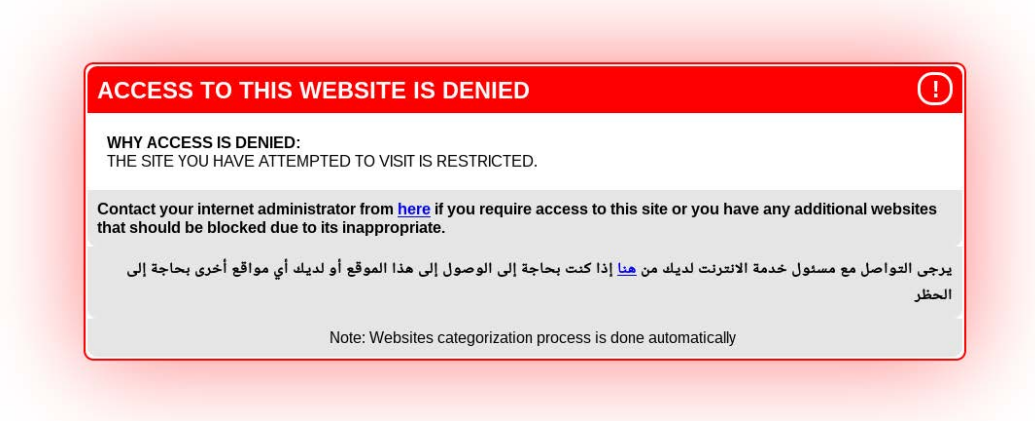

Figure 2.10. Blockpage delivered on Yemennet.

Using in-country tests, volunteers tested the websites from different locations, including areas under the control of the Houthis and others under the control of the government of president Hadi. The results from both regions were identical because all connections go through the same national ISP.

Determination of inaccessibility was straightforward because the national ISP YemenNet serves an explicit blockage for social content and some political websites, and a 404 Not Found page for most political websites. The explicit blockpage is the same that was identified earlier in **Figure 2.10** while the 404 page can be seen in **Figure 2.11**. Previous Citizen Lab research has shown that the device(s) serving the

explicit blockpage and this 404 Not Found page were likely the same device due to anomalies identified in the IPID and TTL values observed.

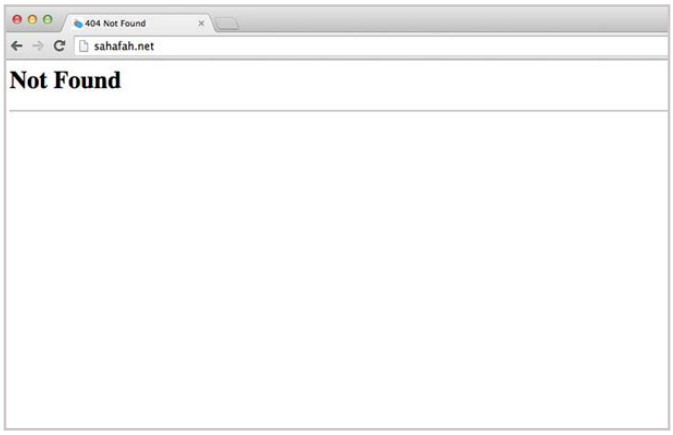

Figure 2.11. 404 Error page as seen in October 2015.

During Host Header testing, we saw blockpages returned from IP addresses in one Yemeni ASN: the Public Telecommunication Corporation.

2.11.3.2 Examples of blocked content

The majority of test results from Yemen did not include a categorization. However, among those cases where categories were included, those that were returned included:

- Custom
- Multiple
- Pornography
- Web Proxy

In addition to looking at public measurement data, we did in-country testing of URLs to determine which websites were blocked in August 2017. URLs that were determined as being blocked solely through this method are denoted with an asterisk. Among all our data, the blocked websites fall into the following categories:

Local news and political opinion websites that report on the ongoing armed conflict and provide opinions different from those provided by the Houthis. The websites in this category report on political and military developments contrary to the ones provided by the Houthi-controlled media. Examples include:

- Barakish (*http://www.barakish.net/)
- al-Hekmah (*https://www.al-hekmah.net/)
- Moragboon Press (*https://www.moragboonpress.net)

Websites of Yemeni political parties, including:

- General People's Congress (*http://almotamar.net/)
- Yemen's Social Party (*http://aleshteraky.com/)
- al-Islah Party (*http://www.al-islah.net)
- Nasserist Unionist People's Organisation (*http://www.alwahdawi.net/)

Regional websites that provide pan-Arab news coverage, including that of Yemen political and military conflicts. Examples include:

- al-Araby al-Jadeed (*https://www.alaraby.co.uk/portal)
- Arabi 21 (*https://arabi21.com/)
- US government-funded Radio Sawa website (*https://www.radiosawa.com/)
- al-Hurra TV (*https://www.alhurra.com/)

Websites of Internet privacy and circumvention tools used by citizens, and especially by journalists, and activities to anonymize their communication. Examples include:

- Hide My Ass (*https://www.hidemyass.com)
- Tor Project (*https://www.torproject.org)
- Psiphon (https://psiphon.ca)

Section 3- Discussion & Conclusions

This section examines the legal, regulatory, corporate social responsibility, and other public policy issues raised by our report's findings. We focus on the responsibilities of Netsweeper, Inc. and the obligations of the Canadian government under international human rights law. We then suggest measures each could take to mitigate negative human rights impacts associated with Internet filtering technology.

3.1 Summary

This report has documented Netsweeper installations on public IP networks in ten countries presenting systemic human rights concerns. Netsweeper is a Canada-based company. Our findings raise issues of public importance regarding both Canada's and Netsweeper's compliance with international human rights law and commitment to corporate social responsibility (CSR). This section discusses these issues.

The purpose of this section is not to allege definitive violations of Canadian or

international law, but to set out responsibilities and obligations both Netsweeper and Canada have under international human rights law, how they may be falling short, and how they may do better. In fact, there are no Canadian domestic laws that apply extraterritorially to the international uses of the Netsweeper products and services discussed in this report. Nevertheless, Netsweeper has responsibilities under international law to respect human rights such as the right to freedom of opinion and expression, a right that is clearly implicated by the filtering practices discussed in Sections 1 and 2.

The corporate responsibility to respect human rights encompasses, among other things, the establishment of human rights due diligence processes to identify, prevent, and mitigate how business operations impact human rights abroad. This onus is heightened in states with conflict-affected areas– like Afghanistan, Yemen, Pakistan, and Somalia– and with track records of human rights abuses, like those discussed in the country case studies in Section 2.

Canada has an obligation to protect human rights as well, which includes enacting and enforcing laws requiring businesses to respect human rights, providing effective remedies for victims, and setting clear expectations and standards for Canadian businesses operating abroad. There are ways both Netsweeper and Canada could do better in fulfilling international human rights law, discussed in this section.

This section proceeds as follows. First, it sets out the rights framework that is applicable to filtering technologies and the issues these technologies raise under international human rights law, including protections for the freedom of opinion and expression. Second, it sets out general corporate social responsibility principles for filtering companies and the ways in which Netsweeper is falling short. And third, it sets out Canada's obligations and responsibilities for the human rights impact of Canadian businesses, including those operating abroad. We conclude this section by identifying concrete recommendations for how Canada can better meet the requirements of international human rights law.

3.2 The international human rights framework applicable to filtering technologies

The routine use of filtering technologies to mediate publicly-available Internet access by states poses a significant threat to human rights when that filtering is applied covertly, arbitrarily, without due process, or without regard for legitimate forms of

expression. Companies operating within the market for filtering technologies must be aware of the risk that their products can be used to threaten and undermine human rights.

The practice of Internet filtering most directly threatens the right to freedom of opinion and expression (UDHR Art. 19, ICCPR Art. 19). This right includes the absolute right "to hold opinions without interference" (ICCPR Art. 19(1)) as well as the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers," whether online or otherwise (ICCPR Art. 19(2)). Any state restriction on the right to freedom of expression must be provided by law and must be necessary "for respect of the rights or reputations of others" or to protect national security, public order, public health, or morals (ICCPR Art. 19(3)). The restriction must be the least intrusive measure available to achieve the intended function and proportionate when weighed against the consequences of limiting the right (ICCPR Art. 19(3), Kaye, A/HRC/32/38 at para 7). The implementation and effects of filtering technology may also impact a host of other protected human rights including, among others, the rights to liberty and security of the person (UDHR Art. 3, ICCPR Art. 9); the right to privacy (UDHR Art. 12, ICCPR Art. 17); protections against discrimination (UDHR Art. 7, ICCPR Art. 26); and minority rights (ICCPR Art. 27).

Human rights obligations are not relinquished in situations where a state contracts with a private company—such as an ISP or other digital intermediary—to provide public services or to enforce government policy (see Guiding Principles, 5). States' duty to respect these international human rights obligations will often also be reflected in domestic laws and policies, which may impose specific legal requirements on the private sector to respect human rights.

Private companies maintain an independent responsibility to respect human rights. The United Nations Human Rights Council adopted this position in endorsing the Guiding Principles on Business and Human Rights (A/HRC/17/31). While domestic law in a given jurisdiction may provide a framework for Internet censorship, private filtering technology vendors cannot rely on the contracting state's legal framework alone without also considering that state's compliance with binding international law. The corporate responsibility to respect human rights "exists over and above compliance with national laws and regulations protecting human rights" (Guiding Principles, 11 [commentary). In some countries, human rights laws and policies may not be adequately implemented in practice and domestic legal frameworks may not provide meaningful recourse to victims. For this reason, private companies have independent responsibilities, including to avoid causing or contributing to adverse human rights impacts, and to prevent or mitigate adverse impacts "directly

linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts" (Guiding Principles, 13). Depending on the context, this responsibility means business enterprises should, among other things, put in place due diligence processes to identify, prevent, and mitigate how their business operations impact on human rights (Guiding Principles, 17); provide a measure of transparency reporting on human rights policies and practices (Guiding Principles, 21); and ensure remediation for any adverse human rights impacts caused (Guiding Principles,22).

In conflict-affected areas, the risk of human rights abuses is heightened. Businesses have special responsibilities to ensure that they are not involved in facilitating such harms and states have similar responsibilities to ensure that this is the case (see Guiding Principles, 7). More fundamentally, states have responsibilities to ensure that their support for domestic business does not compromise their own international legal commitments and policies. The Guiding Principles on Business and Human Rights clarify that in addition to providing assistance to businesses navigating the challenge of operating in conflict-affected areas, states should deny "access to public support and services for a business enterprise that is involved with gross human rights abuses and refuses to cooperate in addressing the situation," and should pay special attention to the possibility of gender-based and sexual violence (see Guiding Principles, 7). Notably, censorship and surveillance technology tends to have unique and disproportionate impacts on the rights of women and girls (see Citizen Lab, 2017).

3.3 Corporate social responsibility issues for Internet filtering companies

After two decades of academic studies and regular media reporting on the use of filtering technologies for public online censorship, companies providing Internet filtering technology are or should be aware of the rights-related impacts of their products. Some companies have taken principled stands on the issues. For example, security company F5, which offers products that include web filtering capabilities, has a detailed statement and full report on the company's "Corporate and Social Responsibilities." Juniper Networks, which also includes web filtering technology among its products, likewise has a statement. OpenDNS has an anti-censorship policy concerning its security and web filtering products, as does Forcepoint.

Groups of companies have also taken part in multi-stakeholder initiatives (MSI) on this point. One example of an MSI focused on corporate social responsibility

is the Global Network Initiative (GNI), which was founded by NGOs, investors, academics, and key industry participants Google, Yahoo, and Microsoft to formulate a "code of conduct" for technology companies with an aim to promote transparency, privacy, and freedom of expression (Brown & Korf, 2012). Today, GNI-participating companies have expanded to include many key technology and telecommunications companies like Facebook, LinkedIn, Vodafone, and Nokia, among others. GNI issues guidance to participants and requires self-reporting and independent assessment of participant compliance with GNI principles and codes (GNI Accountability Framework).

Another framework for corporate social responsibility is the UN's Global Compact, which now involves over 6,000 participants, including over 5,000 businesses in 130 countries. Participants agree to a set of 10 principles concerning human rights, labour standards, environmental rules, and corporate corruption. In particular:

> **"Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and**
>
> **Principle 2: Make sure that they are not complicit in human rights abuses."**

The prospects for enhanced accountability through the Global Compact are questionable, however, for although a mechanism to "exclude" members for non-compliance with the principles exists, no country has ever been so removed.

Despite the aforementioned examples of companies taking steps towards better CSR, many companies have yet to acknowledge any responsibility for equipping autocratic regimes, or governments presiding over widespread violence and humanitarian crises, with the means to control their population's access to information.

In his 2017 report to the Human Rights Council, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, noted that filtering companies play a direct role in emerging human rights challenges:

> **"What governments demand of private actors, and how those actors respond, can cripple the exchange of information; limit journalists' capacity to investigate securely; deter whistle-blowers and human rights defenders. Private actors may also restrict freedom of expression on their own initiative. They may assign priority to Internet content or applications in exchange for payment or other commercial benefits, altering how users engage with information online. Companies that offer filtering services may influence the scope of content accessible to their subscribers…" (A/HRC/35/22 at para 1).**

> **"The private actors that make digital access possible mediate and enable the exercise of freedom of expression. To be sure, States drive most censorship and surveillance. But just as States often, but not always, rely upon providers to take the actions that make censorship possible, we as users — beneficiaries of the remarkable advances of the digital age — deserve to understand how those actors interact with one another, how these interactions and their independent actions affect us and what responsibilities providers have to respect fundamental rights…" (A/HRC/35/22 at para 3)**

Technology companies in particular tend to operate as platforms, intervenors, and mediators in the exercise of human rights in the digital age. The business decisions of Internet filtering companies like Netsweeper can have a direct, measurable, and significant impact on the ability of individuals at home and abroad to meaningfully and safely exercise their human rights. And with that impact comes important human rights responsibilities.

3.3.1 Applying human rights and corporate social responsibility considerations in the case of Netsweeper

Our findings suggest Netsweeper products and services may be contributing to adverse human rights impacts abroad, as such products and services have been used to block political discourse, political opposition websites, religious content, local and media websites, and online privacy tools. For example, Netsweeper's pre-defined "alternative lifestyle" filtering category effectively reduces for its government clients the cost, time, and complexity associated wtih censoring websites related to LGBTQ communities, gender identity, sexuality, and sexual orientation. Providing such filtering categorization, however, appears inconsistent with core corporate responsibilities to respect human rights such as freedom of opinion and expression and non-discrimination (see Guiding Principles, 11; 12).

Other findings likewise raise important human rights concerns. These include the use of Netsweeper for:

- Blocking sites across a range of political content, including websites affiliated with local political groups, opposition groups critical of government, local and foreign news portals, and regional human rights issues in countries like Bahrain, Kuwait, Yemen, and UAE
- Blocking Google searches for keywords related to LGBTQ identities such as "gay" and "lesbian" in the UAE, Bahrain, and Yemen

- Blocking a variety of non-pornographic websites in various countries on the basis of an apparent miscategorization of these sites as 'Pornography', including the websites of the World Health Organization, the Christian Science Monitor, the World Union for Progress Judaism, the Center for Health and Gender Equity, and Change Illinois
- Blocking access to news reporting on the Rohingya refugee issue, as well as violence against Muslims, from Al Jazeera, the Telegraph, ABC News Australia, and the Express Tribune for users in India
- Blocking a variety of Blogspot-hosted websites in Kuwait after categorizing them as 'Viruses', as well as a range of political content including foreign and domestic news portals, a website on the Kuwait Progressive Movement, and a website that monitors regional human rights issues
- Blocking a variety of websites that are not web proxies in various countries on the basis of an apparent miscategorization of these sites as 'Web Proxy', including the websites of Date.com, B'nai B'rith International, Gay.com (the Los Angeles LGBT Center), the World Jewish Congress, Feminist.org, Former Catholic, the Jewish Defense League, and TMZ

These and other uses of Netsweeper filtering products documented in this report implicate the right to freedom of opinion and expression (UDHR Art. 19, ICCPR Art. 19) including the freedom to seek, receive and impart information and ideas of all kinds (ICCPR Art. 19(2)). Such filtering, especially concerning content relating to national minorities and marginalized groups, may also impact rights to liberty and security of the person (UDHR Art. 3, ICCPR Art. 9); protections against discrimination (UDHR Art. 7, ICCPR Art. 26); and minority rights (ICCPR Art. 27).

It may be that some of the uses of Netsweeper installations with adverse human rights impacts result from errors or oversights, or constitute restrictions on the right to freedom of expression that are "provided for by law," necessary "for respect of the rights or reputations of others," or to protect national security, public order, public health, or morals (ICCPR Art. 19(3)), and are both "proportionate" and the "least intrusive measure available" to achieve the intended justifiable purpose (ICCPR Art. 19(3), Kaye, A/HRC/32/38 at para 7).

However, the UN Human Rights Committee, in General Comment No. 34, stated that "any restrictions" on blogs, websites, or any other "Internet-based, electronic, or other dissemination system," including systems supporting such communication like Internet service providers, are generally only permissible under Article 19(3) if they are content-specific, that is, target content on sites, not sites themselves. Generic bans on the operation of certain sites thus would not be permissible. It also stated it is impermissible under Article 19(3) to block or prohibit a site solely on the basis that the site contains content critical of the government or political and social views promoted by the government. And any restrictions, on any of the grounds in Article 19(3), must conform with the ICCPR's non-discrimination provisions.

Thus, any of the findings involving entirely blocked sites– including those of political groups and critical opposition groups, news portals, and regional human rights sites– would not be permissible restrictions on freedom of expression under Article 19(3). Blocking entire sites through miscategorization would similarly not qualify as a permissible restriction. In fact, the blocking of many of the sites noted here through miscategorization– including sites affiliated with health organizations and various social, religious, and political groups– is likely impermissible on other grounds as well, as the blocking is of content critical of the political or social views of the government, or the blocking is inconsistent with the non-discrimination requirements of the ICCPR. The more content-specific filtering of Google searches on "gay", "lesbian," and "LGBT" issues, as well as of news concerning Rohingya refugees and violence against national minority populations (e.g., muslims), and various religious sites, also appears to violate the ICCPR's express non-discrimination requirements, rendering these restrictions on freedom of expression also impermissible under Article 19(3).

In short, none of these restrictions on freedom of expression appear to be permissible under Article 19(3). Indeed, there are strong international legal norms against Internet and web content filtering. As stated in the 2011 Joint Declaration on Freedom of Expression and the Internet, issued jointly by four special international mandates for protecting freedom of expression, mandatory blocking of entire websites through Internet content filtering is an "extreme" measure and content filtering systems imposed by governments or commercial service providers, which are not end-user controlled, constitute "prior censorship" and are "not justifiable as a restriction on freedom of expression."

Moreover, if these and other uses of Netsweeper filtering products documented in this report are merely errors or oversights or are legally permissible under Article 19(3), then Netsweeper should indicate as such. Netsweeper should provide information as to any errors and oversights, specify any justifications for restrictions that are authorized by law, including information as to necessity and proportionality, and detail any remedial action taken on present or past adverse human rights impacts of its products. The public reporting of such information would be facilitated if Netsweeper were to fulfill its responsibilities under international human rights law to: establish due diligence processes to identify, prevent, and mitigate how its business operations impact on human rights (Guiding Principles, 17); ensure public transparency on its human rights measures, policies, and practices, particularly in relation to groups affected (Guiding Principles, 21); ensure remediation for any adverse human rights impacts (Guiding Principles, 22); undertake special measures or attention for minority groups within national populations, to account for unique challenges these groups face such as vulnerability and marginalization, as suggested by commentary accompanying the Guiding Principles; and take into account the fact that many states with which it does business have records for human rights abuses (as discussed in the country case studies in Section 2) or conflict-affected areas, which heightens risks and thus due diligence responsibilities (Guiding Principles, 7 & 23).

Netsweeper has not to our knowledge publicly reported information as to filtering categorization errors, oversights, or applicable justifications for human rights restrictions. Nor are we aware of any human rights due diligence measures, policies, or practices that Netsweeper has in place to address these issues and heightened risks. We are also not aware of any remedial action it has taken in relation to these issues nor any special measures or attention given to the potential adverse impact on various minority groups implicated by these issues, including sexual minorities (LGBTQ content), ethnic and religious groups (Rohingya content; Jewish content), and groups focused on gender issues (feminist content), for example.

If Netsweeper was to put in place human rights due diligence processes with "clear and specific criteria" in relation to freedom of expression and other human rights; enact open CSR, anti-censorship, and human rights policies; establish measures for adverse human rights impact remediation; join MSI initiatives like the GNI or UN Compact; and, consistent with Guiding Principle 21, offer formal transparency

reporting to the general public, and especially groups affected, about these and related policies and practices in relation to its business, it would be far better placed in relation to its responsibility to respect human rights. And if Netsweeper was unaware of the uses of its products outlined in this report, and any attendant adverse impacts on freedom of expression and other human rights, they should now take remedial action to mitigate these impacts and prevent them in the future (Guiding Principles, 17).

As Amnesty International noted in a report in 2017, it is often difficult to establish human rights claims against businesses because much of the relevant information is internal to the company. Reflecting that reality, the Guiding Principles, and the international legal standards they express, require businesses to set up human rights processes and policies and offer transparency about them. In short, businesses have "to know and show" that they respect human rights (Guiding Principles, 15). Netsweeper has failed to do so.

3.4 Netsweeper's relationship with the Canadian government

Netsweeper has benefitted from substantial support from the Canadian government. This support has taken the form of financial support as well as trade promotion. Specifically, the company has been a direct recipient of financial support from the National Research Council. In 2009, Netsweeper was awarded $280,615 for support "with a research and development project." In 2012, the company was awarded an additional $46,430 for a different project.

The government of Ontario has described Netsweeper as a "success story" of its Export Market Access program, which is designed to "assist small and medium size organizations (SME) to access and expand their growth in foreign markets." Export Market Access program support included grants covering "up to 50% of eligible costs incurred to develop export sales," up to $150,000. Netsweeper is an approved business under the program since at least January 2013 and is quoted by the program as having generated a "five-fold (500%+) return on our investment within nine months of our participation of EMA."

Netsweeper has been included in international trade promotion through various levels and agencies of the Canadian government, including events and trips arranged by these agencies. For example, in December 2013 a trade mission to India was organized by the Department of Foreign Affairs, Trade and Development

(now Global Affairs Canada) and Export Development Canada. The mission included '11 top Canadian ICT companies', one of which was Netsweeper. The Ontario Government has also included Netsweeper in its promotional materials for a number of events, including a November 2015 "ICT Trade Mission" to Thailand, the August 2016 Technology in Government event in Australia, the October 2016 Gulf Information Technology Exhibition (GITEX 2016) in the UAE, the September 2016 IBC exhibition in the Netherlands, the September 2016 CTIA Super Mobility event in Las Vegas, and the 2017 Mobile World Congress in Barcelona.

In June 2017 Export Development Canada, in partnership with Wavefront Wireless Commercialization Society, announced that Netsweeper was included on a trade tour of telecommunications companies in Europe. The Trade Commissioner Service of the Government of Canada also included Netsweeper in its promotional materials for the 2013 Mobile World Congress in Barcelona. Dubai-based telecom du, a UAE sovereign-wealth-controlled enterprise that has used Netsweeper products and services to filter political and religious content, was awarded the International Business Green IT award by the Ontario Centers of Excellence. In receiving the award, a du representative noted their collaboration with "international partners like Netsweeper."

In July 2016, Export Development Canada (EDC) provided a guarantee for the Royal Bank of Canada's financing of Netsweeper's sale to Bahrain. The transaction was described as "Sale of various Canadian goods and/or services" and was valued at less than $1,000,000. In testimony to the Standing Senate Committee on Human Rights, EDC representative Christopher Pullen was asked if EDC considered the human rights implications of guaranteeing a loan to facilitate the sale of censorship technology to a rights-restricting authoritarian government. Pullen stated that in any transaction, EDC evaluates "the nature of the product, the performance of the company and the countries in which they operate." Noting previous Senate testimony from the non-governmental organization Above Ground, which criticized EDC's guarantee of this transaction, Pullen noted that "the guarantee that is the subject of the complaint is no longer in place, nor is the company a customer of EDC."

3.5 What are Canada's obligations?

Canada has international human rights obligations under the United Nations' Universal Declaration of Human Rights (UDHR); as a state party to the International

Covenant on Civil and Political Rights (ICCPR); and as a member of the United Nations (UN Charter) and the international community of states, it is bound by applicable rules of customary international law. Many rules of international law are binding domestic law within Canada. For example, a large number of international human rights treaty commitments have been implemented through binding domestic Canadian legislation (see Canada's Approach to the Treaty-Making Process), with the Rome Statute of the International Criminal Court being among the most well known. Customary international law also automatically forms part of domestic common law in Canada unless inconsistent legislation is enacted, as the Supreme Court of Canada held in *R v Hape*. Canadian courts have also held international law should inform statutory interpretation, judicial review, as well as the application of the *Canadian Charter of Rights and Freedoms*.

In fact, the *Canadian Charter of Rights and Freedoms*, with its protections for fundamental freedoms of expression, religion, thought, and peaceful assembly among others (section 2), voting and democratic rights (section 3), mobility rights (section 5), life, liberty, and security of the person (section 7), and equality (section 15) has long informed Canadian foreign policy values. Consistent with that influence, Canada claims a longstanding history of supporting the protection and promotion of human rights and democratic values abroad, including support for freedom of expression, association, and democratic participation; respect for the privacy, dignity, and security of individuals; the principle of non-discrimination on the basis of political, religious, or cultural grounds; LGBTQ rights; and support for the rights of women and girls. All of these rights are potentially at stake when Canadian companies sell products and services to governments with track records of abuse of Internet filtering technologies.

Even where the *Charter of Rights and Freedoms* does not apply directly, Canadian government decision-makers must take relevant *Charter* values and related international human rights principles into account when exercising discretionary powers. When the Canadian government provides major financial support to a private entity, that entity's conduct abroad is more readily attributable to the Canadian government directly. Canada could ensure that businesses that are domiciled in Canada and subject to its jurisdiction respect and protect human rights in the course of their operations, including those operations that take place abroad (see Guiding Principles, 2). The activities of these businesses also have an impact on both Canada's international reputation and its foreign policy objectives, making it vital to strive for policy coherence (see Guiding Principles, 8).

3.5.1 Canada's responsibility for the human rights impact of domestic companies operating abroad

International human rights law has historically focused on protecting individuals from abuses committed by states, but these laws and norms can also apply to businesses. The UDHR, for example, speaks to responsibilities of individuals and "every organ of society," which would include non-state actors like private businesses. And the ICCPR requires every state to "ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant…" Rights impacts of Canadian businesses fall within that scope. While these obligations do not require enacting specific measures to police the extraterritorial activities of businesses internationally, there is no prohibition on such measures, and it remains open for states to do so (Guiding Principles, 2). Moreover, states nevertheless also have a duty to provide an effective remedy for victims of human rights violations (UDHR Art. 8; ICCPR Art. 9; see Guiding Principles, 25). An "effective remedy" includes access to justice, compensation, and fair and respectful treatment (OHCHR, UN Doc A/RES/60/147).

Canada has a responsibility to set clear expectations and standards for Canadian businesses operating abroad (Guiding Principles, 2), including Netsweeper. The Government of Canada previously recognized this responsibility in the context of extractive companies and expressly linked it to Canadian policies on CSR:

> **"The Government of Canada expects Canadian companies operating abroad to respect human rights and all applicable laws, and to meet or exceed widely-recognized international standards for responsible business conduct. For those companies working or exploring opportunities in jurisdictions where local laws are not aligned with Canadian values, the Government of Canada encourages them to find ways to reflect Canadian values that also respect local laws. If this is not possible, companies may wish to reconsider their investment."**

In this report, we have documented uses of Netsweeper filtering products that have serious implications for a range of human rights, most notably, the right to freedom of opinion and expression (UDHR Art. 19, ICCPR Art. 19), including the freedom to seek, receive, and impart information and ideas of all kinds (ICCPR Art. 19(2)). Other rights implicated are rights to liberty and security of the person (UDHR Art. 3, ICCPR Art. 9); protections against discrimination (UDHR Art. 7, ICCPR Art. 26); and minority rights (ICCPR Art. 27). And as discussed earlier, these restrictions on freedom of opinion and expression represented by these uses are unlikely to be permissible under Article 19(3).

Moreover, we see little evidence that Netsweeper is carrying out its responsibility to respect human rights. This responsibility, as has been noted, includes putting in place human rights due diligence processes to identify, prevent, and mitigate how their business operations impact on human rights (Guiding Principles, 17); ensuring public transparency about any such measures, policies, and practices, particularly in relation to groups affected (Guiding Principles, 21); taking action to remediate any adverse human rights impacts (*Guiding Principles, 22*); taking special measures to account for minorities and marginalized groups impacted by these filtering uses; and taking into account through due diligence the fact that many of the states implicated in the filtering uses documented in this report have records for human rights abuses (Guiding Principles, 7 & 23).

The Government of Canada thus has a responsibility to address Netsweeper's role in global Internet filtering practices. In fact, this is not the first time the Government of Canada has been called upon to respond officially to uses of Netsweeper filtering products raising human rights concerns. In September 2013, Canada's Director General for the United Nations, Human Rights, and Democracy Bureau of Foreign Affairs, Trade, and Development Canada, in response to a letter about Netsweeper's international business activities, stated that, while the government did not have the legal authority to act on specific extraterritorial human rights violations, Canada "expects Canadian companies working overseas" to abide by "applicable Canadian laws, ethical standards, and corporate social responsibility (CSR) practices." She also acknowledged Canada promotes OECD guidelines for CSR that include provisions directing companies to "respect human rights" and for Canada to "assist them in doing so."

Clearly, Canada could do more to ensure Canadian "dual-use" technology companies like Netsweeper are abiding by CSR practices and respecting human rights internationally. In contexts beyond ICT-related businesses and products, the UN Human Rights Committee has in fact expressed concern in Concluding Observations on Canada's compliance with the ICCPR in July 2015, noting "allegations of human rights abuses by Canadian companies operating abroad," and the "inaccessibility to remedies by victims of such violations." In 2014, the Inter-American Commission on Human Rights (IACHR) released a statement urging the Organization of American States to "adopt measures to prevent the multiple human rights violations that can result from the implementation of development projects, both in countries in which the projects are located as well as in the corporations' home countries,

such as Canada." And in June 2017, the United Nations Working Group on Business and Human Rights noted that "cases of alleged human rights abuse by Canadian companies abroad … continue to be a cause for serious concern." While none of these statements concerned Netsweeper, they highlight how Canada could take greater action to ensure CSR and human rights are respected by Canadian companies abroad.

3.6 Recommendations for the Canadian government

Below, we set out several suggestions for how Canada can better meet and exceed its international human rights law duties and responsibilities.

3.6.1 Greater due diligence: financial incentives and transparency

Canada has an international legal duty to protect against human rights abuses within their jurisdiction by companies (Guiding Principles, 1), which includes enforcing laws aimed at, or which have the effect of, requiring business enterprises to respect human rights (Guiding Principles, 3). Moreover, with respect to those companies "that receive substantial support and services from State agencies," the UN Guiding Principles note that Canada should encourage or require such companies to carry out human rights due diligence (Guiding Principles, 4). According to our research, however, Canada is falling short in the case of Netsweeper. Despite Netsweeper technology being used for state censorship internationally, it has received substantial trade and financial support from the governments of Canada and Ontario (notably through National Research Council grants and the Government of Ontario's Export Market Access program).

The support provided to Netsweeper by the Canadian government, and the trade-related ties established between the company and government agencies, are powerful reasons to require that the company implement rights-respecting policies and business practices (see Guiding Principle 4). Importantly, commentary within the Guiding Principles notes:

> **"[T]he closer a business enterprise is to the State, or the more it relies on statutory authority or taxpayer support, the stronger the State's policy rationale becomes for ensuring that the enterprise respects human rights.**
>
> **Where States own or control business enterprises, they have greatest means within their powers to ensure that relevant policies, legislation and regulations regarding respect for human rights are implemented. Senior management typically reports to State agencies, and associated government departments have greater scope for scrutiny and oversight, including ensuring that effective human**

> **rights due diligence is implemented. (These enterprises are also subject to the corporate responsibility to respect human rights, addressed in Chapter II.)**
>
> **A range of agencies linked formally or informally to the State may provide support and services to business activities. These include export credit agencies, official investment insurance or guarantee agencies, development agencies and development finance institutions. Where these agencies do not explicitly consider the actual and potential adverse impacts on human rights of beneficiary enterprises, they put themselves at risk – in reputational, financial, political and potentially legal terms – for supporting any such harm, and they may add to the human rights challenges faced by the recipient State.**
>
> **Given these risks, States should encourage and, where appropriate, require human rights due diligence by the agencies themselves and by those business enterprises or projects receiving their support. A requirement for human rights due diligence is most likely to be appropriate where the nature of business operations or operating contexts pose significant risk to human rights."**

Human rights due diligence can be encouraged through financial incentives, government procurement standards, as well as transparency requirements. There is a great deal of secrecy surrounding "dual-use" technology companies operating abroad, particularly concerning the products and services they provide and their end users. A lack of transparency can facilitate rights abuses and undermine accountability. This lack of transparency is especially concerning as research has shown that "dual use" products and services like Internet filtering software or digital surveillance technology are easily misused, repurposed, and abused.

As an interesting example of what is possible, Canada presently uses its Trade Commissioner Service (TCS) as a resource for Canadian extractive companies operating abroad. As part of Canada's "enhanced" CSR Strategy, Trade Commissioners are tasked to provide international contacts beyond business services to help extractive companies forge partnerships to conduct "social risk analyses" or "conflict analyses." TCS missions also provide contacts to assist companies in forming partnerships with development organizations, to better understand the communities and regions in which they are operating.

Recommendation 1:

Where Canada or Provincial Governments provide direct financial support to businesses operating abroad, that funding could be tied to clear prohibitions against unlawful and unethical activities, and effective and ongoing due diligence, public transparency reporting, and other accountability measures to ensure compliance with these prohibitions. Such requirements could be backed by effective penalties for non-compliance, including mechanisms to freeze and, where appropriate, revoke financial support and services.

Recommendation 2:

Government entities within Canada, at the federal, provincial, or local levels, could establish human rights-oriented government procurement standards for "dual-use" technology companies. These could restrict the award of government contracts to those businesses that have human rights policies and due diligence processes in place, and strong records of respect for human rights overseas.

Recommendation 3:

Canada could mandate transparency. Mandated transparency can make an important difference, for example, by requiring the regular issuance of company transparency reports. Such reports could indicate the jurisdictions in which products and services are provided, the nature and scale of such products and services, and applicable legal and regulatory requirements in the jurisdiction of operation that may negatively impact human rights. This would also be consistent with the Government of Canada's commitment to transparency and open government.

Recommendation 4:

Canada could expand the mandate of the TCS's enhanced CSR strategy beyond the extractive sector to include "dual-use" technology companies. This approach could assist companies like Netsweeper to better understand the contexts in which they are operating, including the impact of their business activities on local populations and human rights more generally.

3.6.2 Empower the new Canadian Ombudsperson for Responsible Enterprise

The Canadian Ombudsperson for Responsible Enterprise (CORE) was announced in 2018 and represents a promising means for the Government of Canada to proactively investigate corporate rights abuses abroad. The Government of Canada announcement indicated that the CORE will be "mandated to investigate allegations of human rights abuses linked to Canadian corporate activity abroad" and "empowered to independently investigate, report, recommend remedy and monitor its implementation." The Government also indicated that its focus will be "multi-sectoral," first on "mining, oil and gas, and garment sectors," and expanding after the first year to "other business sectors." The intention to make the CORE's focus multi-sectoral means that it could eventually reach "dual-use" technology companies like Netsweeper. A Government Q & A on the CORE indicates the Government is "committed" to ensuring the CORE has sufficient investigatory

powers and budgetary allotment for independent fact finding. But it will only have the power to "recommend" sanctions, changes in corporate policy, or compensation for victims. There is room for improvements here, too.

Recommendation 1:

Canada could empower the CORE to ensure it can effectively carry out its mandate. This would involve giving the CORE sufficient powers to compel both witness and document disclosure, an adequate budget, as well as the power to order effective remedies for complainants. Canada could empower the CORE to make legally binding and mandatory remedial orders, including the capacity to impose sanctions, direct businesses to cease certain activities, and compensate victims of rights abuses. These powers to issue legally binding and mandatory orders and impose fines are similar to those enjoyed by British Columbia's Information and Privacy Commissioner, as well as those the present Government of Canada has promised to confer on Canada's Information Commissioner,

Recommendation 2:

CORE could also have express authority to take proactive measures to *prevent* human rights violations and not simply investigate complaints and harms after the fact. This authority might include setting rules and guidelines for Canadian companies operating internationally, and recommendations to the Government and Parliament, as well as how federal institutions– like embassies and consulates abroad– deal with Canadian companies found to be engaged in improper or abusive practices. Such an approach would be consistent with, and arguably beyond, the recommendations of the United Nations Working Group on Business and Human Rights, which urged Canada in June 2017 to "set out clear expectations for Canadian companies operating overseas."

3.6.3 Make it easier for human rights victims to seek redress in Canada

Canada could do better in providing effective remedies for victims of corporate human rights violations, a central international human rights obligation. Essential to this obligation is ensuring that victims of human rights abuses committed by Canadian companies abroad can more easily seek legal redress in Canadian courts.[7]The UN Human Rights Committee expressed "concern" in its July 2015

7 Civil society groups and victims of Internet filtering and censorship in their home countries have *some* options to seek redress and accountability through various international avenues, including the OECD Complaints Mechanism as well as the ILO Complaints Mechanism. But there are

Concluding Observations on its Sixth Periodic Report on Canada about the "inaccessibility to remedies" for victims of Canadian corporate human rights abuses "operating abroad." The Committee also expressed "regret" about the "absence of an effective independent mechanism with powers to investigate" such complaints. Two years on, the UN Working Group on Business and Human Rights observed that international victims of Canadian corporate human rights violations were "continuing to struggle in seeking adequate and timely remedies against Canadian businesses." Similarly, Canadian human rights experts and groups like Amnesty International contend that "individuals and communities" that have "suffered human rights harms" associated with Canadian businesses operating abroad "lack of an effective remedy." Part of the challenge, as Amnesty International has noted, is that Canadian courts have historically declined to exercise jurisdiction to hear such cases, finding that the better forums to hear such claims are in the country where the alleged abuses occurred.

However, more recently, Canadian courts have shown more willingness to exercise jurisdiction and hear these claims. In *Araya v. Nevsun Resources Ltd.*, for example, the British Columbia Supreme Court allowed a lawsuit brought by plaintiff workers from Eritrea, for violations of international norms against slavery and torture, to proceed against Canadian mining company NevSun. The Court held, and the B.C. Court of Appeal would later agree, there was a "real risk" that the plaintiffs would not receive a fair trial in Eritrea. Similar claims against other Canadian companies like Tahoe Resources and Hudbay Minerals are likewise proceeding. However, the *Araya* decision is being appealed and there remains a great deal of uncertainty in this area of law, with the balance of judicial precedents weighing against victims succeeding in their claims.

significant limitations. The OECD complaints process has been successfully used by civil society groups against technology companies for facilitating human rights abuses internationally. In February 2013, a group of human rights organizations, including Reporters Without Borders International, Privacy International, and the European Center for Constitutional and Human Rights among others, filed formal complaints with the OECD National Contact Points (NCPs) in both Britain and Germany against British company Gamma Group and the German-based Trovicor for selling surveillance technology to Bahrain. The OECD NCP ultimately found in March 2015 that Gamma "breached human rights" by selling its FinFisher spyware to Bahrain. But none of the states with Netsweeper installations that we identify in this report are members of the OECD. Canada *is* a member, so a complaint might be raised against Canada for failing to properly supervise the activities of Canadian companies abroad. But even if successful, OECD findings are not legally binding and thus any of its dictates remain only "soft" international law. Complaints can be filed with the International Labor Organization (ILO) against member states for failure to adhere to the ILO Conventions, which can lead to a Commission of Inquiry and later a report with recommendations to deal with complaints. Unfortunately, only member *states* can file a complaint. So while Afghanistan, Bahrain, India, Kuwait, Pakistan, Qatar, Somalia, Sudan, South Sudan, Yemen, and UAE are all ILO member states, complaints are far less accessible to victims and civil society groups .

Recommendation 1:

Canada could take a bold step as an international human rights leader and enact a statute that provides clear legal standing and right of action for international victims of human rights abuses committed by Canadian companies abroad to proceed in Canadian courts. There is prior precedent for this in Canadian law. The Justice for Victims of Terrorism Act, for example, creates a cause of action in Canada for damage, injury, or loss, suffered anywhere in relation to an act of terrorism (with some conditions imposed). A similar statute tailored to harms and human rights violations caused by Canadian corporate practices could provide a significant incentive for companies to proactively take steps to ensure their products and services are not being used for rights abuses abroad, or face liability concerns.

3.6.4 Export transparency and controls

Narrowly tailored export controls are another policy lever that the Government of Canada can employ to prevent Canadian technology companies from exporting products, tools, and services to states with track records of human rights abuse. In Europe, export controls have been used to regulate the sale of spyware sold to foreign states that used the spyware to violate the rights of their citizens. More recently, the EU has moved to impose additional export controls on cyber-surveillance products and 11 EU countries have expressed support as of February 2018 for draft rules that would impose export restrictions on surveillance technologies. As a participating state of the Wassenaar Arrangement, the Government of Canada has put in place export controls and regulations that cover the sale of certain dual-use technologies to foreign jurisdictions, including "IP network communications surveillance systems or equipment" and items related to "intrusion software," and requires licensing to export such dual-use technology. With sufficient precision, export controls could be extended to certain other "dual-use" technologies and products.

Moreover, transparency remains a problem in export licensing. The 2016 Annual Report issued by the Government indicates, for example, that 5,978 permits were issued for exported goods defined as military and strategic technologies, while only seven were denied. Little information beyond these basics is available. No insights are provided as to how human rights impacts are considered in licensing decisions, for example.

Recommendation 1:

Canada could follow Europe's lead and clarify or amend its export controls to require licensing for Internet filtering software like Netsweeper that is provided to designated end users and/or for designated end uses that present significant human rights risks.

Recommendation 2:

Canada could provide greater transparency in how export licensing decisions are made. Very few license applications are denied. More transparency about this process, the basis for licensing decisions, and how human rights impacts are taken into account in the process would be helpful, and consistent both with Canada's international human rights duties as well as its commitment to transparency and open government.

3.7 Conclusion

Research for this report demonstrates that a combination of methods could be used to identify and then analyze Netsweeper deployments around the world. First, we gathered a list of possible Netsweeper IP addresses from Internet scanning and Internet measurement databases. We found deployments in 30 countries. We performed additional testing to determine which of these installations were deployed on consumer-facing ISPs in countries of interest, which we defined as countries ranked as "Authoritarian" by the 2017 Economist Democracy Index, as well as India, Pakistan, and Somalia, which all have a history of Internet censorship. We then measured to see what sorts of websites installations in these countries were blocking. We found widespread blocking of freedom of expression sites, as well as some problems with Netsweeper's categorization system, which allows operators of Netsweeper installations to block any of dozens of categories including "Pornography," "Alternative Lifestyles," and "Abortions." We identified miscategorizations, such as the website of the World Health Organization categorized as "Pornography," as well as problematic categories like "Alternative Lifestyles," which appears to include nonpornographic LGBTQ content. While most of our measurements involved a vantage point in a censored country, we discovered it is also possible, in some cases, to *remotely* measure censorship (e.g., our Host Header test).

The use of Netsweeper technology by governments known to conduct censorship in breach of internationally-recognized human rights raises serious issues of corporate

social responsibility and international human rights law. As set out in the UN Guiding Principles on Business and Human Rights (A/HRC/17/31), business enterprises operating abroad have a foundational responsibility to respect human rights under international law. This responsibility includes, among other things, putting in place due diligence processes to identify, prevent, and mitigate how their business operations impact on human rights, being transparent about these measures, and ensuring remediation for any adverse impacts. Other security, filtering, and technology companies have dealt with such issues by issuing corporate social responsibility statements and enacting anti-censorship policies, or have worked with other companies and civil society groups to promote human rights and provide transparency about their own human rights and corporate social responsibility practices. Netsweeper does not appear to have taken even these steps.

The Government of Canada has international obligations to protect human rights and the responsibility to set clear human rights expectations and standards for Canadian businesses operating abroad. The Government also has a duty to provide effective remedies in Canada for international victims of corporate abuses. Canada has recently taken important steps– like the move to establish the Canadian Ombudsperson for Responsible Enterprise (CORE)– which will be tasked with, among other things, investigating complaints concerning Canadian companies operating internationally, including their human rights impacts. The CORE could be given more powers and support to carry out this important mandate. But Canada could still do more, including encouraging stronger human rights due diligence practices for businesses through financial incentives, mandated transparency, funding for relevant research, statutory measures for easier victim redress, and export controls. While these would only be first steps, we argue they would be steps in the right direction.