Excerpts from

Mapping Global Surveillance and Proposing Solutions to Respect Human Rights

A capstone project for Access (www.accessnow.org) by students at the Columbia University School of International and Public Affairs

Authors

Nina Agrawal
Aliza Goldberg
Raffi Wartanian
Keisuke Yoshino

Advisor

Anya Schiffrin

Spring 2015

COLUMBIA | SIPA
School of International and Public Affairs
www.sipa.columbia.edu

Table of Contents

Executive Summary

This report documents surveillance laws around the globe to facilitate future advocacy regarding human rights and communications surveillance. The project provides a snapshot of the current legal structures in place across the globe permitting domestic surveillance, and analyzes how these legal frameworks are applied in practice.

Research methodology consisted of reviewing primary legal sources (statutes, constitutions, international conventions, court cases) and secondary sources (advocacy materials, academic papers, media articles), as well as conducting interviews with lawyers, human rights activists, scholars, and journalists. Foreign legal research databases, such as **GlobaLex, the Library of Congress, and the Columbia, Georgetown, and Harvard Foreign Legal Research Guides**, directed us to descriptive sources on countries' legal landscapes, as well as to primary sources. Interviews in particular helped provide country-specific context and a fuller picture illustrating the implementation of existing laws.

We recommend contacting some of our contacts on digital rights. Agnes Callamard, former head of Article 19, now directs Columbia University President Lee Bollinger's Global Freedom of Expression & Information program. The most helpful global organizations we looked at were **Article 19, Citizen Lab, Electronic Frontier Foundation, Human Rights Watch, Privacy International, Reporters Without Borders, Committee to Protect Journalists, Freedom House, Global Information Society (GIS) Watch, and DLA Piper Global Law Firm**.

The selected countries represent all regions of the world and a variety of approaches to government surveillance. Although each country has different kinds of laws, some common trends include:

- Nations create new and often more restrictive surveillance laws citing counterterrorism and **national security efforts**.
- Countries frequently violate international commitments they have made regarding the International Covenant on Civil and Political Rights (ICCR) and other international statues.
- Governments demonstrate secrecy, outright deception, and/or indifference towards Internet users.
- Ambiguous and **vague legal language leads to various interpretations** of the laws.

Based on these trends, we drafted country reports that offer a current picture of surveillance laws and, where possible, some indication of where they are headed in the future. Some general recommendations for future advocacy efforts include:

- Requesting primary government documents through **access to information laws** to create a complete picture of the scope of government surveillance activities; supporting the development and/or maintenance of access to information laws in target countries.
- **Clearly defining terms** such as sensitive data, privacy, terrorism, and security to assure more effective advocacy.
- Understanding court decisions that have/have not permitted monitoring personal information to create useful guidelines for government and private-sector agencies—and to direct future legal strategy.
- Understanding the **historical and cultural context** of each country to shape human rights advocacy in a culturally appropriate and realistic manner.

Country-specific recommendations are as follows:

- China: Use cultural understanding in communicating with Chinese diplomats about Internet freedom. Also work with American and Canadian technology companies that help China censor its citizens.
- Vietnam: Encourage access to information and government transparency and should work with the United Nations Human Rights Council, of which Vietnam is a member.
- Argentina: Encourage government surveillance oversight, resurrection of the Freedom of Information Act, and fair coverage of the October 2015 presidential elections.
- Chile: Encourage constitutional revisions, data transfer oversight, media diversity, and educational campaigns about surveillance precautions.
- Turkey: Encourage Turkey to adopt norms of tolerance and free speech, and specifically target revisions of Law 5651, Law 6532, and monitor the upcoming parliamentary election in June 2015.
- Syria: Encourage norms of *jus en bello*, resistance to hacktivist groups connected to the government, revisions to the penal codes (Articles 23 and 29), and engage western companies whose technologies are used by the government for surveillance.
- Russia: Encourage an open media landscape, revision of the 1995 SORM Law, revision of the Blogger Law, revise the law banning swear words in the arts, and request public disclosures from Roskomnadzor to justify website blocks.

- Burma: Advocate for amendments to allow Aung San Suu Kyi to run for president, monitor the 2015 General Elections, unshelf the Public Media Bill, amend the Electronic Transaction Law, and oppose trends in online hate speech.
- Canada: Monitor pending court cases and upcoming anti-terrorism and digital privacy legislation. Work with local civil society organizations and legal activists to influence outcomes.
- Mexico: Support local NGOs in their efforts to increase transparency and public awareness about government requests for communications data. Support legal activists in *amparo* court cases (cases defending individuals' constitutional rights), helping to raise the public will for cases to continue on to higher courts.
- India: Support local NGOs' efforts to increase transparency about the government's use of surveillance, and about the Central Monitoring System in particular. Support development and passage of a personal data protection law.
- Singapore: Focus efforts on increasing awareness within Singapore about the potential harms of government communications surveillance. Singapore is essentially a surveillance state, which most of the country's citizens seem not to object to, seeing it as part of a trade-off with greater security and social harmony.

This report highlights key findings and recommendations. Look for more of the research and results from this study throughout 2015-2016 from Access (www.accessnow.org).

China

China's vague legal framework can be interpreted in many ways and does not address data transfer and data storage. Hong Kong lawyer Margaret Ng said, China "has the power to interpret black as white, and then black becomes white."[1] The way the judicial branch handles legislature "undermines the rule of law and undermines the law itself,"[2] Ng continued.

The surveillance techniques used by government officials are sophisticated, widespread, and invasive. Many citizens feel at risk and a sense of fear is reported to pervade the Chinese cyberspace. Over 500 people have been arrested since Xi Jinping's instatement in 2012, according to former human rights lawyer Teng Biao.[3] Biao believes this is "the worst crackdown on lawyers, activists and scholars in decades,"[4] with the inevitably unstoppable rise of social media as China's savior.

Though China's legal framework has been under constant reform since the Open Door policy was instated in 1978 after the death of Mao Zedong, Chinese-American lawyer Christopher Kwok has viewed legislative actions as "three steps forward and one step back,"[5] with the Constitution as a document created to appease Westerners. Additionally, the Communist Party now reportedly has more authority than the official government, adding increased tension and confusion.

Recommendations for Future Advocacy Efforts

Access should use cultural understanding in communicating with Chinese diplomats about Internet freedom. Diplomatic negotiations and assurance by Access that the country will not be at risk with an open search engine or online sharing platforms is the best way to promote digital freedom in China. The Communist party rose to power after rescuing China from foreign intrusions, mainly Japan--understanding how the Communist party views interventions from abroad may be helpful in fostering a dialogue.

The government uses censorship, blocking, and data retention methods for the purported purpose of protecting its citizens. Access should demonstrate the economic benefits of an

[1] Ng, Margaret. "Speech and Media Freedom: New Lessons of the Umbrella Revolution" Columbia University Law School. 23 Feb. 2015. Lecture.
[2] Ibid.
[3] Biao, Teng. "What Will This Crackdown on Activists Do to China's Nascent Civil Society?" *The Guardian*, 24 Jan. 2015. Web. 10 May 2015. <http%3A%2F%2Fwww.theguardian.com%2Fcommentisfree%2F2015%2Fjan%2F24%2Fcrackdown-activists-china-nascent-civil-society-pu-zhiquaing>.
[4] Ibid.
[5] Kwok, Christopher. Personal interview. 28 Feb. 2015.

unrestricted Internet by partnering with technology companies, such as Cisco Systems, Inc. If key companies learned of the long-term benefits of refusing to help censor China, perhaps the companies would temporarily discontinue business until China revised its treatment of human rights.

Vietnam

Vietnam's economic reform policy of 1986, known as "Doi Moi," was a catalyst for economic development. The Internet was introduced to Vietnam in November 1997 and has seen exponential growth. Approximately half of Vietnam's population is under the age of 25 is now online,[6] which may help modernize the country.

Many Vietnamese laws address Internet usage, but the legislation is often used as an excuse for officials to violate human rights, not as a means of protecting citizens. Blogs are Vietnam's version of an independent press, since all official news organizations are state-owned—though some outlets are freer than others. Bloggers are legitimate journalists who report the news without government supervision. Media scholars Catherine McKinley and Anya Schiffrin explained in the 2013 book, *State Power 2.0: Authoritarian Entrenchment and Political Engagement Worldwide*, that bloggers who are critical of the government usually come from the educated upper class, which helps explain their influence and widespread readership.[7]

A *New York Times* article on January 15, 2015, suggests progress on the future of unfettered online access. Prime Minister Nguyen Tan Dung has accepted the inevitable sharing of information through social media, saying that "'You are all on social media, checking Facebook for information...It's impossible for us to ban it," and instead, the Vietnamese government should focus efforts on fact checking content.[8] The Vietnamese Constitution should be revised to reflect changes in Vietnamese society since 1992, including addressing digital freedoms.

Recommendations for Future Advocacy Efforts

The Party Congress leadership change in 2016 is an apt time for Access to draft and submit laws for review by government officials. Access can partner with a political candidate, facilitated by Access employees in the field or by the local pro-democracy NGO, Viet Tan. The United States State Department's Bureau of Democracy, Human Rights, and Labor (DRL) may be able to help in the legal aspects of communication. Duy

[6] "The Country: Vietnam." Public Broadcasting Service. N.p., n.d. Web. 10 May 2015. <http://www.pbs.org/hanoi/vietnam.htm>.
[7] McKinley, Catharine and Anya Schiffrin. From Leninist Lapdogs to Bothersome Blogger in Vietnam." *State Power 2.0: Authoritarian Entrenchment and Political Engagement Worldwide*. Farnham: Ashgate, 2013. 125-38.
[8] "Vietnamese Leader Says Banning Social Media Sites Impossible." The New York Times. Associated Press, 15 Jan. 2015. Web. 10 May 2015. <http://www.nytimes.com/aponline/2015/01/15/world/asia/ap-as-vietnam-facebook.html?_r=1>.

Hoang of Viet Tan, advises that the "issues with legal reform is that it's used when there is a technical problem, but we have more of a political problem in Vietnam."[9]

With a history filled with French and Portuguese colonialism and Chinese and American military invasions, defending Vietnam's right to privacy should not suggest Western intrusion. Since Vietnam is a member of the 2014-2016 UN Human Rights Council, perhaps Access can partner with UNHRC for advocacy on negotiating digital rights.

Saigon Media Research Group, a group of journalists and lawyers sponsored by the World Bank to research freedom of the press, recommends strengthening "existing regulations on information openness and transparency into law" with more oversight on legal implementation in order to achieve better access to information.[10] The challenge is to ensure that the "words g[o] along with actions."[11]

[9] Ibid.
[10] Chanh, Dong Tam et al. "The Press and the Right of Access to Information." The Saigon Media Group, 2014. *Microsoft Word* file.
[11] Ibid.

Argentina

Digital surveillance pervades Argentine society through the biometric identification program, SIBIOS, which President Cristina Fernández de Kirchner created through executive order in 2011.[12] Each citizen has an identification card with a unique number, picture, and fingerprint. A data breach in 2013 compromised thousands of citizens' information during a voting registration. So far that digital information has not been used maliciously,[13] but the website's source code could have been downloaded by anyone. The use of biometrics information must be monitored to ensure the data is used only in essential situations.

Additionally, journalists covering protests may face persecution. Juan Pablo Suárez, a news editor at *La Última Hora*, was detained for 10 days in December of 2013 and formally prosecuted on May 13, 2014 for terrorism charges after covering a policemen's protest.[14] The charges were dropped,[15] but the trial indicates that journalists who write articles that criticize the government could be considered terrorists under the Penal Code in the future. Argentinian President Kirchner has also pursued charges against media organizations, such as the *Clarin Group*.[16]

According to Ramiro Ugarte, an Argentine lawyer formerly at the Buenos Aires-based human rights NGO, Asociación por los Derechos Civiles (ADC), pro-government journalists often have a relationship with intelligence officers, who divulge information from government surveillance to benefit the Kirchner administration.[17] Journalists can also sell information they gathered from sources to the government,[18] which is the largest advertiser in Argentine media.

Recommendations for Future Advocacy Efforts

[12] Argentina. Ministry of Economics and Public Finance. *Creation of the Federal System of Biometric Identification for Security*. 7 Nov. 2011. Web. 9 May 2015. <http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm>.
[13] Ugarte, Ramiro. Personal interview. 26 Mar. 2015.
[14] "Newspaper Editor Facing 12 Years In Prison Under Anti-Terrorism Law." *Reporters Without Borders*. N.p., 14 May 2014. Web. 9 May 2015. <http://en.rsf.org/argentina-newspaper-editor-facing-12-years-14-05-2014,46281.html>.
[15] "Juan Pablo Suárez no está acusado de sedición." *Día a Día*. 28 May 2014. Web. 9 May 2015. <http://www.diaadia.com.ar/argentina/juan-pablo-suarez-no-esta-acusado-sedicion>.
[16] Nejamkis, Guido, and Anthony Esposito. "Argentina's Supreme Court Upholds Controversial Media Law." *Thomson Reuters*. N.p., 29 Oct. 2013. Web. 12 May 2015; Romero, Simon, and Emily Schmall. "Battle Between Argentine Media Empire and President Heats Up Over a Law." *The New York Times*. N.p., 30 Nov. 2012. Web. 12 May 2015. <http://www.nytimes.com/2012/12/01/world/americas/media-law-ratchets-up-battle-between-kirchner-and-clarin-in-argentina.html?_r=0>.
[17] Ugarte, Ramiro. Personal interview. 26 Mar. 2015.
[18] Ibid.

More oversight within the intelligence and executive branches that use surveillance technology, along with the judicial branch that grants surveillance warrants will help protect the right to privacy and limit data transfers. Since President Kirchner replaced the Intelligence Secretariat with a new intelligence service in February 2015,Access can work with local NGOs to recommend control mechanisms in the organizational structure and structure of this new agency. Access can also point out if President Kirchner does not follow her promise of more transparency in government intelligence.

Access should bring awareness to Argentina's Freedom of Information Act, which stalled in Congress for three years before expiring in 2013.[19] Reviving this Freedom of Information Act and making sure the law is passed could bring more transparency to the executive branch.

After eight years in office, President Kirchner will not run in the October 2015 election. Access should watch the election coverage closely for signs that journalists and intelligence officers are working together to portray certain candidates in a biased way with information from surveillance.

[19] "Freedom in the World: Argentina." *Freedom House*. Freedom House, n.d. Web. 8 May 2015. <https://freedomhouse.org/report/freedom-world/2015/argentina#.VVFb8Vxsqn8>.

Chile

Chile was the first country to establish net neutrality, passing Law 20453 in August 2010. Net neutrality gives all online users an equal platform and prevents Internet service providers (ISPs) for charging for faster uploads or controlling content. The activist group Neutralidad Sí! petitioned for net neutrality, which demonstrates that the executive branch listens to protests.

The Chilean legal framework addresses privacy and assures data protection. According to the American think tank, the Council on Hemispheric Affairs, the Senate approved an electoral reform bill on January 14, 2015 that can help distribute state power, now dangerously concentrated as a duopoly. Journalists who try to cover protests, common occurrences in Chile, are often threatened by the police, according to French press freedom group, Reporters Without Borders (RSF).[20]

Chile is a democratic republic, but some of its laws still bear remnants of Augosto Pinochet's dictatorship. Pinochet prohibited criticism of the government, as written in the Code of Military Justice, the Penal Code and the State Security Law.[21] After Chile's restoration to democracy in 1990, Pinochet's "reign of terror" toward any opposition ended. The Penal Code was revised in December 2000, but the Code of Military Justice and the State Security Law remain dormant.[22]

Recommendations for Future Advocacy Efforts

The Constitution needs to be revised to accurately reflect technological innovations. President Michele Bachelet has promised constitutional reform in order to fully separate Chile from its history as a dictatorship from 1973 to 1990. Access can work with local NGOs and political activists to offer support for these legal changes.

Law 19628 allows access to databases with an authorization request, which involves a degree of trust between the judicial branch and the data collector: it is impossible to ensure the collector follows his stated intent and abides by the law after obtaining the data.[23] Appointing officials to oversee the complete usage of any personal data can help track transfers and limit the number of warrants.

---

[20] "Chile." *World Report*. Reporters Without Borders, July 2013. Web. 11 May 2015. <http://en.rsf.org/report-chile,171.html>.
[21] Chile. *Ley 12927 Sobre Seguridad del Estado*. N.p.: n.p., 26 Aug. 1975. Web. 11 May 2015. <http://www.leychile.cl/Navegar?idNorma=16080>
[22] Kauffman, Katherine. "Chile's Revamped Criminal Justice System." Georgetown Journal of International Law 40 (2010): n. pag. Web. 11 May 2015.
[23] Chile. Congress. *Ley 19628*. N.p.: n.p., n.d. 28 Aug. 1999. Web. 9 May 2015. <http://www.leychile.cl/Navegar?idNorma=141599&r=1>.

Chile's media is dangerously concentrated. Two major conglomerates with the same right-wing political agenda dominate the industry: *El Mercurio* and *La Tercera*. As private companies, owned by the Edwards family and Alvaro Saieh, respectively, Chilean media must focus on readership and revenue and cannot rely on government support, as it does now. If Access were to survey the wealthy media supports and statistically prove that reporting on left-wing politics, such as wealth distribution, will not affect funding, perhaps Chilean news would have more diversity.

Access can run educational campaigns to raise awareness about digital privacy and surveillance precautions. Miguel Paz, founder of Poderopedia, a crowd-sourced database website to identify the relationships among Chile's business and political leadership, says that "for encryption to work, it needs to be end-to-end."[24] Paz continues, "the police, the Carabineros, do a lot of monitoring with warrants, especially when it involves them"[25] and the officers feel threatened by what investigative journalists or curious activists might uncover about the police. Reassuring the police and providing perspective can help investigators work unmolested.

[24] Paz, Miguel. Personal interview. 6 Mar. 2015.
[25] Ibid.

Turkey

President Recep Tayyip Erdogan became Prime Minister in 2003 and has pivoted Turkey in a more conservative and repressive direction, centralizing power and cultivating an environment where nationalism has repressed free speech. At the beginning of 2014, Turkey released dozens of prisoners (and detained a few others), making it the world's tenth most frequent jailer of journalists.[26] The International Telecommunications Union reported that in a population of 76.1 million citizens, Internet penetration rates are at 46% in 2013.[27] As a member of the Council of Europe, Turkey has signed the European Convention on Human Rights and Fundamental Freedoms.

The recent centennial anniversary of the Armenian Genocide in April 2015 underlined major tensions Turkey faces with regard to free speech. As Germany's government, Russia's government, the Vatican, the European Parliament, and many others publically recognized the genocide, Turkey doubled down on its denial and showed hostility toward those opposing its narrative (in the form of withdrawing ambassadors, issuing public condemnations, and more). In the international area, Turkey equates genocide denial with the democratic ideal of free speech, though domestically, opposing genocide denial publically is considered a criminal offense. These tensions and double standards extend into the space of private and digital communications.

Some of the major focal points of Turkey's legal framework for government surveillance revolve around the legal and logistical instruments:

- **Law 5651** – Enacted in 2007, this law blocks foreign-hosted websites alleged to host illegal content, including child abuse images, content enabling drug use, obscene language, prostitution, gambling, suicide encouragement, and crimes committed against the founder of the modern Turkish state, Mustafa Kemal Ataturk.[28]
- **Law 6532** – Also known as the "Law Amending the Law on State Intelligence Services and the National Intelligence Organization", this law was enacted in April 2014 and enhances the surveillance powers of Turkey's National Intelligence Organization (MIT) by increasing its data collection powers to gather without a court order private data, documents, and information from public

[26] Committee to Protect Journalists. "China is world's worst jailer of the press; global tally second worst on record". December 2014. https://www.cpj.org/reports/2014/12/journalists-in-prison-china-is-worlds-worst-jailer.php
[27] International Telecommunication Union (ITU), "ICT Facts and Figures 2014". http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[28] Human Rights Watch. "Turkey: Internet Freedom, Rights in Sharp Decline". September 2014. http://www.hrw.org/news/2014/09/02/turkey-Internet-freedom-rights-sharp-decline

authorities, professional organizations, banks, archives and private companies while giving immunity to MIT personnel.[29]

- **Article 301 of the Turkish Penal Code** – This controversial article was enacted in 1926 and revised for the ninth time in 2008. It deems public insults to the Turkish nation, state, grand national assembly, government, and judicial bodies punishable with imprisonment for up to two years.[30]

The June 2015 General Election will choose 550 members of the Grand National Assembly and President Erdogan has signaled a desire to change Turkey's parliamentary system into a presidential system. This would require a three-fifths majority – or 330 seats – and would significantly increase his power.[31]

Recommendations for Future Advocacy Efforts

Going forward, we suggest the following policy and advocacy recommendations:

- Reduce from 138 to 80 the number of Turkish or English words forbidden for use in domain names. The TIB issues the list of words under the scope of Law 5651.
- In Article 301, reduce the prison term from two years to one year, and provide a specific and narrow definition for "publicly denigrates" since this is the undefined standard used to apply the law.
- Revise Article 9/A of Law 5651 to require judicial approval before the TIB can gain authorization to block access to content.
- Revise Law 5651's to reduce the imprisonment penalty from a maximum of two years to a maximum of one year for ISP personnel's refusal to comply with implementing a block.
- Require police to show warrants whenever approaching companies to see user information on servers.
- Under Law 6532, remove the provision that calls for the imprisonment of journalists and editors who publish leaked intelligence material.

[29] Herguner Bilgen Ozeke. "Turkey: Effects Of The New National Intelligence Organization (MIT) Law on Privacy". *Mondaq.* July 2014. http://www.mondaq.com/x/328912/Data+Protection+Privacy/Effects+Of+The+New+National+Intelligence+Organization+Mit+Law+On+Privacy

[30] Bulent Algan. "The Brand New Version of Article 301 of Turkish Penal Code and the Future of Freedom of Expression Cases in Turkey.".*German Law Journal*. 2008. https://www.germanlawjournal.com/pdfs/Vol09No12/PDF_Vol_09_No_12_2237-2252_Developments_Algan.pdf

[31] Tulin Daloglu. "Turkey's next election could shape more than the next four years". *Al-Monitor*. November 2014. http://www.al-monitor.com/pulse/originals/2014/11/turkey-next-election-erdogan-constitution-opposition.html#

- Monitor the June 2015 election ensuring it is free and fair. If Erdogan gains the parliamentary majority he needs to further centralize power, develop safeguards against abuse and a balance of power across all branches of government.

Syria

The Syrian Arab Republic's legal system is influenced by Islamic Law and French Civil Law. However, the integrity and applicability of this legal framework has weathered four years of a civil war that has seen 7.6 million people internally displaced and over 3 million refugees who have escaped to neighboring Turkey, Lebanon, Jordan, Egypt, and Iraq.[32] The conflict remains violent, with government forces maintaining authority in and around Damascus as opposition fighters ravage northern territories, notably Aleppo, and ISIL implements war tactics so brutal that the Syrian government's own war crimes seem more palatable.

The Syrian government has often resorted to Internet black outs to stymie opposition communication. The International Telecommunications Union reports that in a population of 21.9 million citizens, Internet penetration rates are at 26% in 2013. [33] Internet penetration rates in neighbouring Lebanon (71% in 2014) and Jordan (44% in 2014) are considerably stronger.[34] Telecommunications infrastructure, or lack thereof, remains a key tool in the civil war, and, as such, a key target to disorient enemy fighters.

The abuses committed by the government and other major powers are rarely documented. Syria's ability to develop any sort of legal framework or architecture to promote rights and civil society online or offline are severely restricted by the daily realities of a four-year-old civil war that sees no end in sight.

The Law for the Regulation of Network Communication Against Cyber Crime restricts any online expression that violates another person's privacy or any online expression that violates Syria's penal code. It also requires websites to display the names and details of website owners, and to save a copy of content and traffic data to monitor content contributors.

Branch 225 is an arm of the Syrian intelligence apparatus focused on telecommunication networks. Their activities include instructing mobile phone operators on text messages to block, building and deploying mission-driven viruses, and stealing online identities. Additionally, the pro-government "hacktivist" group known as the Syrian Electronic Army has conducted documented attacks on the websites of Syria's opposition and other western countries.

[32] United Nations Office for the Coordination of Humanitarian Affairs. "Syria". http://www.unocha.org/syria
[33] International Telecommunication Union (ITU), "ICT Facts and Figures 2014". http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[34] Ibid.

Recommendations for Future Advocacy Efforts

Going forward, we suggest the following policy and advocacy recommendations:

- Revise Article 23 of Syria's Penal Code to more narrowly define another person's privacy.
- Revise Article 29 of Syria's Penal Code to delineate between crimes committed online or offline, or consider creating a penal code specialized for online activity.
- In Article 2 of the Law for the Regulation of Network Communication Against Cyber Crime, limit to two years the length of time owners of websites or online platforms are required to save a copy of content and traffic data.
- Disclose the nature of the security clearance that ISPs and Cybercafes must pass in order to operate, ensuring it meets international security clearance norms
- Pressure companies in Dublin to develop internal protocol opposed to supporting oppressive regimes, and to publicly disclose any knowledge they might have that their technologies are being used for war time surveillance. This includes developing a Memorandum to the Public Trust, that if such companies learn their technologies are being used in a war zone to harm and oppress innocents, they commit to dismantling their technologies in those settings, and prevent future sales black market intermediaries.
- Develop international counter-hacking norms to resist attacks by groups like the SEA and viruses put out by surrogates like Branch 225 and others in order to minimize damage to civilians, businesses, governments, and beyond.

Russia

The Russian Federation's legal system draws influence from the tradition of Civil Law. President Vladimir Putin wields tight control in an environment in which opposition leaders and activists are regularly deprived of their rights, threatened, or even, as in the recent case of Boris Nemstov**,** murdered. The International Telecommunications Union reports that in a population of 143.5 million citizens, Internet penetration rates are at 61% as of 2013 (a slight drop from 64% in 2012). As a member of the Council of Europe, Russia has signed the European Convention on Human Rights and Fundamental Freedoms.

Some of the major focal points of Russia's legal framework for government surveillance revolve around the legal and logistical instruments:

- **Law 139-FZ** – This law, also known as the Russian Internet Restriction Bill, was passed in 2012 and established a list of Internet sites containing child pornography, drug related content, extremist content, and other illegal content in Russia.
- **1995 SORM Law** – This law allows Russia's System for Operative Investigative Activities, or SORM, to monitor via the Federal Security Service (FSB) Internet and telephone communications, including a new wiretapping system requirement for all telecommunications operators to install as of March 2015.
- **The "Blogger Law"** – Passed in May 2014, this law considers all bloggers or social media user with over 3,000 daily views to be "mass media" requiring hosts to register with the government, have their information kept on servers for a minimum of six months by ISPs, and to maintain accurate information.

Despite claiming independence from the government, the Kremlin-aligned Russian Safe Internet League has launched campaigns against Tor, a software enabling anonymous communication, calling it a safe-haven for the diffusion of western values and spy agencies.

Recommendations for Future Advocacy Efforts

Going forward, we suggest the following policy and advocacy recommendations:

- Encourage an open media landscape that allows for voices critical to the Kremlin and its policies. A good starting point would be with coverage related to Crimea.
- Revise the 1995 SORM Law by removing the newly instated requirement for all telecommunications operators to install wiretapping softwares. If that is not

possible, then create an amendment to the law that requires the FSB to obtain a court order in order to conduct wiretapping. Ensure the court's decision is made publically available.

- Amend the "Blogger Law" by changing the number of daily views requiring bloggers or social media users to register with the government from 3,000 daily views to 10,000 daily views.
- Repeal the May 2014 law banning swear words in film, theater, literature, and other art forms. If it cannot be repealed, then limit the number of swear words to three.
- Request public disclosures from Roskmonadzor to report on what they block with a justification citing a specific Russian law or laws.

Burma

The legal system of the Republic of the Union of Myanmar, or Burma, is based on English Common Law. Since 2011, Burma has undergone a gradual transition away from the military's brutal, repressive rule of the previous fifty years toward democratic political reforms. These reforms have introduced the multinational telecommunications industry to help bolster a severely underdeveloped infrastructure and industry.

The International Telecommunications Union reports that in a population of 53.3 million citizens, Internet penetration rates are at a mere 1.2% in 2013, the highest rate in Burma's history.[35] Most citizens of Burma cannot afford the costs of Internet installation and monthly fees. Indeed, it is critical note that the legal and cultural framework surrounding the Internet is still in development, just like the country's pivot towards a democratic foundation.

Hate speech, particularly the kind that plays on the tensions between Buddhist and Muslim Burmans, has flourished on the Internet, inspiring an anti-hate speech movement to take hold across the country.

Some of the major focal points of Myanmar's legal framework for government surveillance revolve around the legal and logistical instruments:

- **The Electronic Transaction Law** – Passed in 2004, this law criminalizes sending or receiving detrimental information concerning state security, law and order, community and national solidarity, culture, and economy. Prison sentences range from three to seven years.
- **Public Media Bill** – A proposed bill that would facilitate the transition of newspaper into non-profit organizations with independence from the state, diverse content reflecting Burma's own diverse populations, and inclusion of minority languages. The bill was up for adoption but has been shelved by the Ministry of Information.
- **May 2015 Referendum** – Articles from the 2008 Constitution, drafted by the military, will go through a referendum, though they are unlikely to be implemented until after the 2015 general election. Of note are Article 59(f) and Article 436, which bar Aung San Suu Kyi from running for president and deliver to the military veto power over constitutional amendments.[36]

[35] International Telecommunication Union (ITU), "ICT Facts and Figures 2014". http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[36] Snaing, Yen. "No Constitutional Amendments Before Election: Shwe Mann." *The Irrawaddy.* November 2014. http://www.irrawaddy.org/burma/constitutional-amendments-election-shwe-mann.html

In early November, Burma will hold an election to vote for members of the parliament.

Recommendations for Future Advocacy Efforts

Going forward, we suggest the following policy and advocacy recommendations:

- To increase Internet penetration, develop strategies to lower Internet prices for Internet installation and computer and smartphone monthly access.
- Publically recognize and award anti-hate speech activists.
- Encourage international condemnation of the incendiary Buddhist monk Wirrathu.[37]
- Encourage Yi Htut and other prominent locals to push anti-hate speech campaigns
- Ensure Aung San Suu Kyi can run in the next presidential election, specifically targeting Article 59(f) and Article 436 of the 2008 Constitution.
- Monitor the 2015 General Elections. Train local stakeholders on election monitoring best practices.
- Amend the Electronic Transaction Law to more narrowly define violations. For example, in Clause 68, those who receive punishable content should demonstrate further evidence of subversion beyond simply receiving punishable content.
- Ensure protection for advertisers with *The New Light of Myanmar* and *The Mirror* by penalizing the papers whenever they change advertising content without the advertiser's consent.
- Unshelf the Public Media Bill and accelerate its adoption in accordance with international democratic media norms.

[37] Editorial. "Time to Stamp out Hate-Speech." *The Irrawaddy*. January 2015. http://www.irrawaddy.org/editorial/time-stamp-hate-speech.html

Canada

Canada's Constitution, Charter of Human Rights and Freedoms, and case law have clearly established Canadians' right to privacy and to private communications, including metadata. However, recent legislation expanding the powers of security and law enforcement agencies along with broad interpretations of the law by those same agencies and voluntary disclosures by major Canadian telecommunications firms have undermined that right in the years after 9/11. The Supreme Court of Canada has, for the most part, ruled in favor of privacy; the Court appears to be one of the few remaining means available to combat the expansion of communications surveillance by government agencies.

Media reports following the Edward Snowden leaks in the U.S. documented how the Communications Security Establishment (CSE), Canada's national security agency, warrantlessly tracked Canadian users' movements, file downloads, and emails to government agencies; the agency has also built up an arsenal of cyberwarfare tools. Recent transparency efforts and activism have revealed that telecommunications companies transferred user data to government agencies without warrants at voluminous rates—and charged the government for it.

In 2013 and 2014 the Supreme Court of Canada issued a number of decisions that generally upheld the right to communications privacy. *R vs. Spencer* (2014) mandated the use of a warrant for disclosures of personal information when there is a "reasonable expectation" of privacy, and *R. vs. Vu* (2013) separated warrants for search physical premises from those for searching a computer. *R vs. Fearon* (2014), however, authorized warrantless cell phone searches incidental to an arrest—albeit with a number of caveats.

Given a climate in which communications surveillance is increasingly endorsed by government, both implicitly and explicitly, advocacy efforts tend to revolve on two axes: transparency and litigation. Non-governmental organizations, such as the Citizen Lab at University of Toronto, have focused on increasing transparency with regard to government agency requests for user data; they have issued queries to private telecommunications companies, enlisted the support of members of Parliament in obtaining information from the government, and created apps to empower citizens to make access to information requests. Legal and human rights activists, on the other hand, have sought to challenge the constitutionality of surveillance practices through Supreme Court cases like *Spencer* and *Vu*.

Other cases are currently in lower courts or in early filing stage, but may make their way to the Supreme Court. These include a challenge by two telecommunications firms to a request by Ontario police for cell phone "tower dumps" – dumps of privately held bulk cell phone data to law enforcement authorities – and a lawsuit filed by the British

Columbia Civil Liberties Association challenging the constitutionality of CSE's collection of metadata and interception of private communications.[38] The cases may serve as a useful focal point for advocacy organizations.

There have been three attempts since 2004 to pass "lawful access" legislation expanding government access to telecommunications companies' data. Bill C-13 (the Protecting Canadians from Online Crime Act) was the first to pass, in March of this year. This legislation is significant, as it expands the power of government agencies to solicit metadata. Bill S-4, the Digital Privacy Act, and C-51, the Anti-Terrorism Act, would expand the power of organizations to exchange information without users' knowledge or consent. Both bills are currently being considered by the House and expected to pass later this year—an election year in which the majority Conservative government is seeking to portray itself as tough on terrorism and crime.

C-44, the Protecting Canadians from Terrorism Act, just passed in April; the law explicitly authorizes the CSE to conduct intelligence activities at home and abroad. All three acts may eventually be challenged through the court system, offering perhaps the best hope of reining in the Canadian government's expanding surveillance powers.

Recommendations for Future Advocacy Efforts

Current advocacy efforts in Canada are motivated by two primary objectives: 1) increasing transparency about CSE and other security agencies' collection of communications data and voluntary disclosures by telecommunications companies; and 2) challenging the constitutionality of communications surveillance through the court system. While these efforts complement one another and would lend themselves to coordination, the work of advocacy groups and lawyers tends to be carried out in separate spheres in Canada.[39] Coordinating the efforts of these two groups may help to maximize impact.

Though the Office of the Privacy Commissioner has limited power (and even less so after a 2006 vote not to strengthen its authority), the OPC could help offer clarity on what companies are required to make public in terms of requests they receive from governments for personal data, strengthening transparency.

Human rights activists and lawyers should also follow upcoming legislation and court cases closely, as these will have notable impacts on communications privacy. Bill S-4,

[38] British Columbia Civil Liberties Association, "BCCLA vs. CSEC: Stop Illegal Spying," 23 May 2014, https://bccla.org/our_work/stop-illegal-spying/.
[39] Interview with Chris Parsons, 17 Apr. 2015.

the Digital Privacy Act, and Bill C-51, the Anti-Terrorism Act are both currently being considered by the House; the former could expand data sharing among private companies, while the latter would expand information sharing among government institutions at the expense of users' privacy (for example, institutions such as Health Canada and Revenue Canada could share users data with the Royal Canadian Mounted Police).[40] Both are expected to pass into law later this year, as the Harper government seeks to prove itself as "tough on terrorism" ahead of the October 2015 general election.[41] If passed, both bills are also likely to be challenged on constitutional grounds in the courts.[42] The Protection of Canada from Terrorists Act (Bill C-44), just passed in April, amends the Canadian Security Intelligence Service Act and other Acts to give the CSIS explicit authorization to conduct activities within and outside Canada, protect confidential human sources of intelligence, and amend the Immigration and Refugee Protection Act to allow the government to revoke the citizenship of dual citizens in certain circumstances.[43] The bill is also expected to become the subject of a constitutional challenge.

Two notable court cases, currently under way, are likely to have a strong impact on the debate and future direction of government communications surveillance. These include the telecoms' challenge to an Ontario police request for "tower dumps" (described above) and a lawsuit filed by the British Columbia Civil Liberties Association challenging the constitutionality of CSE's collection of metadata and interception of private communications.[44] The association filed its lawsuit in October 2013; in January 2014 the government filed a statement defending the bulk collection of metadata as essential to protecting Canadians and interception of private communications as merely

[40] Julia Alexander, "Bill C-51: What it is and controversy behind it," *Toronto Sun*, 18 Mar. 2015, http://www.torontosun.com/2015/03/18/bill-c-51-what-it-is-and-controversy-behind-it.
[41] Zi-Ann Lum, "Bill C-51, Harper's Anti-Terror Bill, Passes Second Reading Amid Criticism," *The Huffington Post*, 24 Feb. 2015, http://www.huffingtonpost.ca/2015/02/23/rafe-mair-anti-terrorism-bill-c51_n_6739034.html; Interview with Chris Parsons, 17 Apr. 2015.
[42] Interview with Chris Parsons, 17 Apr. 2015.
[43] Susan Mas and Chris Hall, "CSIS powers beefed up under new bill tabled by Steven Blaney," CBC News, 27 Oct. 2014, http://www.cbc.ca/news/politics/csis-powers-beefed-up-under-new-bill-tabled-by-steven-blaney-1.2814314; Jim Bronskill, "Tories' Anti-Terror Bill C-44 Extends CSIS Source Protection, Judicial Warrant Powers," The Huffington Post, 27 Oct. 2014, http://www.huffingtonpost.ca/2014/10/27/bill-c-44-csis-spy-watchdog-conservatives_n_6055512.html; Shelina Ali, "Anti-terror bill C-44: Pushing the limits of Canadian rights," rabble.ca, 27 Nov. 2014, http://rabble.ca/columnists/2014/11/anti-terror-bill-c%E2%80%9144-pushing-limits-canadian-rights. For complete text of law see Parliament of Canada, Statutes of Canada 2015, Chapter 9, An Act to amend the Canadian Security Intelligence Service and other Acts, http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=7935034&File=4.
[44] British Columbia Civil Liberties Association, "BCCLA vs. CSEC: Stop Illegal Spying," 23 May 2014, https://bccla.org/our_work/stop-illegal-spying/.

"incidental."[45] The case does not appear to have progressed further as yet, but may serve as a valuable focal point for advocacy efforts in the near future.

[45] James Keller, "Ottawa says CSEC's collection of Canadians' data 'incidental,'" CTV News, 24 Jan. 2014, http://www.ctvnews.ca/canada/ottawa-says-csec-s-collection-of-canadians-data-incidental-1.1655231.

Mexico

Mexico's constitution explicitly protects the privacy of communications. Yet a number of laws permit or even require the monitoring and collection of vast amounts of communications data, usually in the name of security and/or law enforcement. Communications surveillance in Mexico takes place against the backdrop of a long-running war on drugs and related cartels—in which the U.S. is a partner—and a historically weak judicial system.

Key findings about what existing laws permit or require with regard to communications surveillance include the following:

- Existing laws are extremely vague in defining what constitutes procurement of justice, national security, etc. as motivations for surveillance. This gives the government a wide berth to conduct surveillance.
- The *Ley de Telecomunicaciones* (Telecommunications Law), passed in 2014, broadened the permissible scope of communications surveillance from previous legislation (notably, a bundle of amendments to the criminal code in 2012, known as the *Ley de Geolocalización*). The law requires all telecommunications companies to register mobile phone users and collect and retain real-time geo-location data for an initial period of 12 months to be able to transfer it electronically to "competent authorities" in the government (without defining who those authorities are) and to collect and store data for an additional 12 months such that it could be handed over within 48 hours.
- Private entities, but not the government, are subject to the *Ley Federal para la Protección de los Datos Personales* (Federal Data Protection Law). This law requires companies to give notice and/or obtain consent for the collection or transfer of personal data. It is unclear whether communications data constitute "personal data."
- The *Ley Federal contra la Delincuencia Organizada* (Law against Organized Crime) permits wiretapping/surveillance of the content of communications with a judicial warrant, although a warrant is not always obtained in practice.
- The government, at all levels (federal, state, and municipal), is using spy software to track communications between private citizens. This is done in the name of security, but concerns abound that the information is and could be used for political purposes and to intimidate journalists, activists, and political opposition.

Interviews with human rights lawyers and digital activists revealed a consistent focus on documenting the instances and uses of communications surveillance and building public awareness and public will for reform. This focus is both pragmatic and strategic: little

else can be done in the absence of a reversal of the law, but public attitudes must also change to create political will for reform.

A number of groups have brought forward cases under the constitutional provision of *amparo*, in which individuals may seek judicial redress if their constitutional rights have been violated. If a critical mass of *amparo* cases are brought to district court and carried all the way up to the Supreme Court or even, eventually, the Inter-American Commission on Human Rights, the law may have to be reversed.

The revised Transparency and Access to Information Law went into effect on May 5, 2015. The law expands the list of bodies that must comply with transparency requirements, but it also expands exceptions for security reasons, removes protections for whistleblowers, and fails to ensure there will be no further chipping away of the law in the future.

Recommendations for Future Advocacy Efforts

Interviews with human rights lawyers and digital activists reveal a consistent focus on documenting the instances and uses of communications surveillance and building public awareness and public will for reform. This focus is both pragmatic and strategic: little else can be done in the absence of a reversal of the law, but public attitudes must also change to first create political will for reform.

A central axis of these efforts consists of filing freedom of information requests to learn how often and for what purposes the government conducts communications surveillance. Activism also centers on educating the public about privacy and lobbying for local and federal data protection authorities to sign on to the International Principles for the Application of Human Rights to Communications Surveillance. In January of this year, Mexico City's data protection authority signed on.[46] Cooperation of the IFAI is critical, as reform of data practices will not happen otherwise.

In terms of available legal options, a number of individuals and groups have brought forward cases under the constitutional provision of *amparo*, in which individuals may seek judicial redress if their constitutional rights have been violated. The legal strategy of a key digital rights advocacy organization, *Red en Defensa de los Derechos Digitales* (R3D), currently consists of bringing a critical mass of *amparo* cases to district court and hoping to lead them all the way up to the Supreme Court. A case filed last September in

[46] Katitza Rodriguez, "Data Privacy Day: Mexico City's Privacy Authority Leads Latin America in Signing on to 13 Principles," *Electronic Frontier Foundation*, 28 Jan. 2015, https://www.eff.org/deeplinks/2015/01/data-privacy-day-mexico-citys-privacy-authority-leads-latin-america-signing-13.

district court was found to have standing and will now advance to a circuit court.[47] Future recourse to the Inter-American Commission on Human Rights is also an option.

[47] Zulema Oviedo, "Organizaciones presentan amparo vs la Ley Telecom," *El Universal*, 23 Sep. 2014, http://www.eluniversal.com.mx/periodismo-datos/2014/organizaciones-de-la-sociedad-civil-presentan-amparo-contra-ley-federal-de-telecomunicaciones-y-radiodifusion-94882.html.

India

India's Constitution and case law protect the right to privacy. However, Indian laws dating back to the colonial period allow for the interception of private communications if there is a sufficient national security or public safety interest at stake. Recent efforts to preserve public order and combat terrorism, particularly by Prime Minister Manmohan Singh's administration (2004–2014), have gradually broadened the scope of government surveillance—both in terms of what is legally permissible and in terms of the government's own capabilities. Key findings include:

- Under the Telegraph and Information Technology Acts, the government of India has the authority and ability to intercept and monitor the content of phone calls, mail, and electronic communications to protect the sovereignty and integrity of India, security of the state, and for other reasons. Lack of explicit privacy and data protection laws leaves the door open for possible abuse.
- The recent development and roll out of the Central Monitoring System, a centralized database of telecommunications data to which nine federal agencies have access (including agencies not involved in law enforcement), has vastly expanded the possibilities of direct government surveillance of communications content.
- Metadata enjoys even less protection than communications content. The CMS facilitates easy access to data about communications, including geo-location. Going back even further, both the Telegraph Act and telecoms licensing regulations require companies to collect and transfer "call data records" and other metadata to the government.
- The government appears to be using spyware (e.g. FinSpy and NETRA) to hack directly into computers.
- India's size and market power work for and against government surveillance. On the one hand, the Indian government has been able to force foreign companies' hand, requiring them to set up local servers and make their systems hackable. On the other, Western companies that have outsourced certain processing operations to India have increasingly raised concerns about data protection, and India will most likely need to bring its encryption requirements into line with international standards to retain their business.

Recommendations for Future Advocacy Efforts

With the recent rollout of the Central Monitoring System, one main task for privacy activists in India going forward will be to increase transparency around which government agencies are accessing the CMS, what data they're collecting, and for what

purposes. The Centre for Internet and Society is one well-known civil society group working in this vein, requesting such information under the Right to Information Act, India's access to information law.

There has also been discussion, including a draft bill, about a formal data protection law.[48] Given that work has already been done identifying the shortcomings of existing law and the scope of a potential future law,[49] this may simply be a matter of building on what already exists.

As India continues to grow economically and court foreign investment, the global business community may serve as a source of leverage for India to enhance data protection, particularly increasing the encryption permitted on personal data.

Finally, advocates should take note of the repeal of the 2002 Prevention of Terrorism Act and, more recently, a Supreme Court decision striking down Section 66A of the Information Technology Act, which punishes individuals who send, by means of a computer or communications device, "grossly offensive," "menacing" or defamatory content.[50] These cases indicate that the public is indeed engaged in these issues, and civil society can have a powerful role to play in reversing some of the more expansive laws of recent years. Indeed, with a strong common law system, Supreme Court decisions have guided much of the actual practice in India related to interception of communications ad safeguarding privacy.

[48] The Personal Data (Protection) Bill, 2013, http://cis-india.org/internet-governance/blog/the-personal-data-protection-bill-2013.
[49] See Centre de Recherche Information, Droit et Société (CRID) analysis.
[50] See Index on Censorship, "The repugnant Section 66A of India's Information Technology Act," https://www.indexoncensorship.org/2014/06/the-repugnant-section-66a-of-indias-information-technology-act/. See also http://www.firstpost.com/india/sc-strikes-down-section-66a-of-it-act-all-you-need-to-know-about-the-controversial-law-2169787.html for more details on Section 66A.

Singapore

Singapore is an authoritarian state with a culture of pervasive surveillance and censorship. Many of its laws date to the colonial period, including a Sedition Act that makes "any seditious tendency" a criminal offense—including "exciting disaffection" against the government. In addition, official concern that any given threat could wipe out the tiny nation in one fell swoop—whether it be a natural disaster, outbreak of disease, or military encroachment by a neighbor—has spurred a desire for the government of this technocratic state to explore mining big data in as many ways as possible to avert crisis.

All of these factors have combined to make Singapore a state in which citizens have few basic rights of privacy—and accept such as a necessary trade-off with security. Examples of the limited protections available to communications data include:

- Personal data, including metadata and the content of their communications, enjoys no protection from government collection, monitoring, or transfer abroad.
- Singaporeans have little ability to communicate anonymously or secretly, as the government requires Internet and cell phone users to register and ISPs to hand over decryption codes when asked.
- Not only does the Singaporean government have easy access to users' data, it has made it easy for other countries' intelligence agencies to tap under-seas fiber-optic cables; in 2013 news reports surfaced that indicated Singaporean telecommunications company SingTel had facilitated foreign access to the under-seas cable that carries communications from Japan to Northern Germany, via Singapore, Djibouti, Suez, and the Straits of Gibraltar.

Recommendations for Future Advocacy Efforts

The history of Singapore, a tiny island city-state surrounded by large powers and home to a potentially volatile mix of ethnic Chinese, Malay, and Indian citizens, has been defined by efforts to contain any suggestion of ethnic/racial tension and to deflect national security threats—as an existential matter. Whether by compulsion or natural tendency, most Singaporeans appear to be relatively sympathetic to this rationale and do not protest the government's collection, monitoring, or even transfer abroad of data about them. Indeed, the revelations that Singapore had facilitated foreign intelligence agencies' access to undersea cable sparked less public outcry than rumors that the extra-marital dating site "Ashley Madison" might launch in Singapore.[51]

[51] Jacqueline Woo, "Business of ruining marriages," *My Paper*, 23 Oct. 2013, http://mypaper.sg/news/business-ruining-marriages-20131023.

Given the country's emphasis on morality, social harmony, and security—and the attendant pervasive climate of surveillance and censorship, advocacy around privacy of communications in the country may be met with skepticism—if not outright aversion. One place to start may simply be educating the public about not only the extent of government collection of data, but also the ways in which such collection could be abused and negatively affect Singaporeans in their day-to-day lives. In an authoritarian regime, the public may have little direct impact on legislation to begin with; a public that is apathetic to issues of privacy and surveillance stands even less chance.

Japan

Japan has long maintained relatively tough regulations regarding the abuse of surveillance by authorities and there is no united intelligence agency like the CIA. The Ministry of Internal Affairs and Communications, which oversees the communications industry, has respected the secrecy of communications as guaranteed in the Constitution and taken a cautious stance about requests from the National Police Agency and other ministries that would grant those agencies greater investigative authority

In April 2015, the government submitted the revised bill to expand the scope of lawful wiretapping to include crimes such as theft and fraud. Although this is officially to help increase the successful prosecution against Internet banking scams and online thieves, some point out that this could be a foundation for the surveillance society in the future.

The Ministry of Internal Affairs and Communications plans to change the rules for GPS investigation, so that people being investigated will not notice that they are being monitored. Since the change can be done at the Ministry's discretion, the new guideline could take effect as early as June. The Ministry also intends to revise the guidelines for cell-phone companies and ISPs to be able to store communication logs for a longer period of time. Currently, there is no specified period, but in practice the most common retention period is three months. The National Police Agency had asked the Ministry to clarify and expand the retention period to six months for investigative purposes. The public comment period on the proposed guideline revision will close in May 2015.

In December 2014, the Act on the Protection of Specially Designated Secrets was enforced, which allows up to ten years of imprisonment for those who attempt to induce intentional leakage or acquisition of specially designated secrets regarding diplomacy or defense. An expert criticized the law due to the ambiguity of what should be designated as "secret." The law also came under fire for the severe punishments on journalists who receive secret information from high officials, not only the officials themselves.

In March 2015, scholars and artists issued a statement claiming that the new copyright rule, which will be brought about by the conclusion of the Trans-Pacific Partnership (TPP), could destruct Japan's 'Otaku' (geek) culture. Otaku culture has been thriving in the world partly due to the distribution of derivative works, most of which are technically illegal, and unlawfully uploaded cartoon films and comics. Under the new rule, law enforcement will be able to crack down those works irrespective of a complaint from the copyright holder.

Although the need to fight against cybercrimes and protecting copyrights is understandable, we need to look critically at the behavior of investigative organizations so that there is no abuse of newly implemented regulation. Moreover, there are very few advocacy groups or organizations defending Internet freedom and the rights of users in Japan. It is also important to encourage people to form groups that can effectively protest legal changes that would compromise privacy and security for the sake of legislative convenience.

Recommendations for Future Advocacy Efforts

Although regulations on the abuse of surveillance by the government are relatively tough in Japan, they have been gradually loosening. It is true that measures against crimes using the Internet and smartphones are necessary, but we need to keep close watch so that new rules regarding wiretapping and GPS investigation are not being misused. The debates among lawmakers over the establishment of the conspiracy charge, which will not be discussed during the current diet session, requires special consideration, given its enormous potential to compromise individual privacy when combined with extensive wiretapping.

The fate of the TPP negotiations, which would have a major impact on the Copyright Act, deserves continued attention. If the new regulation is introduced, allowing authorities to crack down illegal content without the copyright holder's complaint, we should look critically at the behavior of investigative organizations. In the case of excessive apprehending of illegally uploaded content or derivative works without the copyright holder's claim are observed, it is vital to raise a voice in protest.

While there are very few advocacy groups or organizations defending the Internet freedom and the right of users in Japan, the Movements for the Internet Active Users (MIAU) is one exception. Established in 2007, they have issued statements regarding the copyright of Internet content, crowd computing, and the use of personal data.[52] Groups like this one should be encouraged and supported in Japan.

[52] Movements for the Internet Active Users official website, email: info@miau.jp <http://miau.jp/1192544100.phtml>.

South Korea

Although South Korea is known as one of the countries with the fastest Internet infrastructure in the world, censorship and excessive crackdown by the government has been intensifying in the last 7-8 years. Explicitly criticizing President Park Geun-hye online based on unsound evidence could be regarded as defamation and result in criminal charges. Another characteristic is that old laws deriving from a complicated relationship with North Korea have a pervasive influence on the present.

Following two unfavorable court decisions against cell-phone companies, the three leading firms announced in March 2015 that they would no longer voluntarily provide customers' personal information to investigative agencies. Under the current law, they "may comply with a request" from investigative authorities at their discretion even without a warrant.

Law enforcement is strengthening control over online criticism against President Park Geun-hye especially under increasing scrutiny of her response to the ferry disaster in April 2014. A Japanese journalist was indicted in August on a charge of online defamation based on 'false facts' in his article regarding President Park. At least 1.5 million users switched from Kakao Talk, the nation's top chat-app, to a German alternative for fear of punishment following prosecutors' announcement in September that they launched a team to monitor online information

There is no user notification obligation for ISPs and cell-phone companies under current laws, even when subscriber data is given to law enforcement agencies. Using the method called 'cell tower dump', law enforcement seized communication metadata for 37.3 million communication exchanges mainly from 4,616 targeted towers in 2011. The number of towers searched in South Korea in 2011 was about three times greater than the U.S. in 2012 on a per capita basis.

Older laws have had unexpected side effects for the use of technological tools in South Korea. For example, an old law that prohibits anyone from taking a map abroad so that it will not fall into North Korea's hands means that Google cannot offer competitive mapping service in South Korea because storing map information in servers located outside Korea could constitute an offence. Under Korean law, businesses that use the GPS data of their customers must submit certain information to authorities. In January 2015, Uber, the mobile-app-based transportation network service, was reported to local prosecutors for incompliance.

Recommendations for Future Advocacy Efforts

Amendments to laws relating to acquisition of users' data by law enforcement should be made to enhance user notifications. There is no user notification obligation for ISPs and cell-phone companies under the Telecommunications Business Act, even when subscriber data is given to law enforcement agencies. Although the Act on Promotion of Information and Communications Network Utilization and Information Protection guarantees users' rights to ask ISPs and cell-phone companies if their personal data was provided to a third party, these companies do not have to make a voluntary notification. Additionally, the vast majority of 37 million people whose metadata was caught by cell tower dump will never be notified. Stricter laws that favor users' privacy and control over their own information should be implemented.

Another way to increase the transparency of government surveillance is for cell-phone companies, ISPs, and Internet portals to publish a transparency report. They should disclose how many requests were made, which government authority requested the information, and what kind of data were demanded over a certain period of time, as companies like Google and Twitter currently do.

The inherent arbitrary nature of decisions made by the Korea Communications Standards Commission (KCSC) is a serious problem. Under the current law, whether certain content is deemed "appropriate" depends on KCSC's judgment. They should establish a clear set of standards so that ruling is more systematic. Adding members to the KCSC who are not government appointees could also contribute to fairer verdicts.

Nigeria

About 16 years have passed since Nigeria's first democratic presidential election, and there has been no report of explicit surveillance by the government. Chiefly on social media, people are freely talking about sensitive issues such as criticism of the President and gay marriage, which is banned in Nigeria. However, this does not mean authorities respect the rights and privacy of Nigerians. This online freedom is said to be due to fragile broadband network and the absence of specific laws directly governing censorship and interception of communications. Currently, a new law allowing interception to prevent crimes and maintain public order is about to be enacted, with harsh punishments for offenders. Moreover, it has been revealed that the government and ISPs had purchased or used a series of sophisticated surveillance systems, devices, and software.

The proposed Cybercrime Bill, which would enable authorities to intercept and record telephone calls, e-mail messages, and faxes to prevent crime and facilitate criminal investigations, has stimulated active debate over its pros and cons. In emergencies, authorities do not need to obtain a warrant for interception. The bill would prescribe the death penalty for those who commit a crime against any computer systems vital to national security. In February 2015, the bill passed the second reading in the House, bringing it closer to implementation.

Also in February 2015, a local paper revealed that in 2010 the government had purchased two sophisticated pieces of equipment capable of intercepting phone calls and other electric communications. These join a growing list of purchase/installation of surveillance systems by the government and ISPs. In March 2015, a public inquiry for the Draft of Lawful Interception of Communications Regulation was held, which aims to provide a legal and regulatory framework for future lawful interception. The bill allows anyone to intercept communication without a warrant under certain conditions, such as the case in which one party agrees to the interception. Opponents point out that the government could use the regulation to crack down on opposition figures.

The Paradigm Initiative Nigeria (PIN), an advocacy group for online freedom, is creating a draft of the Digital Rights and Freedom Bill, which covers the right of digital privacy online, anonymity, etc. After finishing the draft, the PIN will encourage lawmakers to enact the bill at the National Assembly.

Recommendations for Future Advocacy Efforts

One of the biggest problems with the Cybercrime Bill is the provision that allows the authorities to investigate without a warrant in case of emergency. What should be added to the bill is a provision like "investigative organizations must obtain a warrant within a week from the outset of the compulsory investigation." The best practice in advanced countries is to seek a court warrant by presenting evidence of the existence of a reasonable cause to the judge. If Nigeria wants to achieve its goal – to become one of the top 20 countries in terms of GDP by 2020 – its legal environment should be equivalent, or at least close, to the world standard. There is also cause to examine overly harsh penalties, such as a death sentences for those who commit crimes against critical national information infrastructure and life imprisonment for those who access any computer system or network for the purpose of terrorism.

The government should be held accountable for their actions if they were/are monitoring anyone without any judicial permission, even if those monitored are would-be criminals. Internet advocacy groups, such as Paradigm Initiative Nigeria and Fantsuam Foundation, should be aggressive in their pursuit of government responsibility and accountability. For the public, banding together on social media and making their voice heard on issues related to privacy and security would be a competitive advantage.

The Digital Rights and Freedom Bill, which the Paradigm Initiative Nigeria (PIN) is now drafting, should be promoted, involving as many stakeholders as possible. If the bill is to be enacted, the support and votes of sympathetic lawmakers will be required. Here, too, an upsurge of public interest through social media could help garner the necessary support.

Australia

Australia's surveillance laws allow the intelligence community to collect a broad range of communications data with little judicial oversight. Although the government attempts to protect privacy rights through the Australian Privacy Principles (APPs) listed in the Privacy Act of 1988, the exemptions provided to law enforcement and intelligence agencies allow for massive privacy breaches of private citizens. Businesses also suffer from these surveillance laws as communications lose control over their stored information as well as the services they provide to customers.

The nation's surveillance laws threaten privacy rights and infringe upon the beliefs espoused by the 13 APPs. However privacy advocates can look to cybersecurity as their next frontier. The newly created Australian Cyber Security Center is a potential future ally as the fight for privacy moves into cyberspace.

Recommendations for Future Advocacy Efforts

Despite the Australian government's powerful surveillance laws, there are opportunities for privacy rights advocates to limit future threats to the nation's APPs. Australia's Cyber Security Centre is a relatively new player in the government.[53] This center aims to create the nation's cyber security policy and act as the face of the nation's technological defense sector. As of spring of 2015 open source data concludes that the nation's intelligence agencies have not utilized software or hardware hacking as a means to monitor persons of interest. Privacy advocates can work with the Cyber Security Centre to establish modern APPs that address online activity, thusly preemptively creating measures to protect citizens online.

[53] "ACSC – Australian Cyber Security Centre." Australian Signals Directorate, Department of Defense. Web. 23 Mar 2015. http://www.asd.gov.au/infosec/acsc.htm

France

France has a history of protecting privacy rights; however there has been a push to increase the intelligence community's surveillance capabilities in light of recent terror attacks. These new laws seek to collect metadata and location data without judicial oversight, and there are renewed efforts to force the private sector telecoms to relinquish data stores.

Recommendations for Future Advocacy Efforts

France's historical use of case law to interpret legislation can be used to diminish the power of these regulations. Framing these laws as direct contradictions to Article 9 of the French Civil Code will allow advocates to weaken these pieces of legislation as they come into effect. Furthermore privacy advocates can influence French surveillance efforts by boycotting businesses that relinquish data stores to the DGSE or other intelligence agencies. Moreover since aggressive pieces of surveillance legislation are hidden in innocuous bills, privacy advocates should closely monitor the bills that pass in the coming months to ensure no new surveillance bill has covertly been signed into law.

Germany

The basic rights enumerated by both the European Convention on Human Rights as well as Articles 1, 2, and 10 of Germany's Constitution protect citizens from illegal data interceptions. However intelligence agencies still utilize surveillance programs to legally conduct communication intercepts. Security interests lend to a lack of judicial oversight regarding intelligence agencies' use and abuse of these technologies. This is becoming increasing problematic as the intelligence services begin using poorly designed malware to support their surveillance efforts. Overall, the popular imagination of Germany espouses a pro-privacy rights sentiment. Yet the nation's law enforcement agencies continue to utilize unlawful methods of data interception under the auspices of maintaining national security interests.

Recommendations for Future Advocacy Efforts

The German government must increase their regulations to provide safeguards for citizens against unlawful surveillance of their Internet activity. Furthermore, more powerful judicial oversight is required to limit law enforcement agencies' use and abuse of surveillance power. Current oversight authority is incredibly weak, bordering on nonexistence. Providing the judiciary with leverage over intelligence agencies will support these efforts of a stronger oversight body.

Furthermore, independent parties looking to support German privacy efforts should look to telecommunications companies as well as groups similar to the Chaos Computer Club in order to plan future action. These unconventional actors have championed the pro-privacy rights cause for political and economic reasons. Uniting these disparate groups that possess similar ideologies can provide the privacy lobby with leverage in the face of an obdurate intelligence sector.

United Kingdom

The United Kingdom's domestic surveillance laws undermine its commitment to the European Convention on Human Rights, specifically the right to privacy. The Data Protection Act, Regulation of Investigatory Powers Act of 2000, and the Data Retention and Investigatory Powers Act of 2014 permit the use of data intercepts for national security and law enforcement purposes. These pieces of legislation permit the collection of metadata, location data, and content data for communications originating in the UK.

There is very little oversight given to intelligence agencies such as the Government Communications Headquarters, who collect signals intelligence under the auspices of these laws. Entities such as the Investigatory Powers Tribunal and the Foreign and Commonwealth Office lack the power required to provide substantive oversight. Subsequently intelligence agencies overstep their boundaries and abuse their surveillance power. Some of the more controversial abuses of power include Project Tempora and the hacking of the Dutch sim card company, Gemalto. Additionally, many telecommunications companies are required by law to comply with the government's surveillance efforts; turning voluntary agreements into mandatory relationships.

Despite these setbacks, privacy advocates can find allies in these telecommunications companies. Their desire to rebrand themselves as pro-privacy in order to retain their consumers will make them valuable partners in the fight against future surveillance laws.

Recommendations for Future Advocacy Efforts

Given the powerful surveillance laws within the United Kingdom, the best way to approach future advocacy efforts is through collaboration with large telecommunication companies. Although the government may hold legal leverage over these businesses, their desire to present an increasingly pro-privacy image in the wake of Project Tempora can work in the favor of privacy advocates. These companies are cognizant that economic leverage stems from both governments and consumers. Consumers shall always be more profitable for these companies than governments. Wielding this economic leverage, coupled with their push for a pro-privacy rebranding, privacy advocates can limit future iterations of DRIP and RIPA from becoming reality.

Furthermore, a subsection within DRIP stipulates a sunset clause in 2016. This means that the law will be repealed at the end of 2016. However the government is likely to introduce another surveillance bill into Parliament to replace the powers lost when DRIP is invalidated. Now that advocacy groups are aware of the hasty process used to push

unsavory surveillance bills through parliament, they are better prepared to inject input and limit the power of future bills that threaten illegal data intercepts.