GOING OFFLINE?
THE THREAT TO CAMBODIA’S NEWFOUND INTERNET FREEDOMS

A report issued in May 2015
GOING OFFLINE?
The Threat to Cambodia’s Newfound Internet Freedoms

A report issued in May 2015

Cambodian League for the Promotion and Defense of Human Rights

 LICADHO
LICADHO is a national Cambodian human rights organization. Since its establishment in 1992, LICADHO has been at the forefront of efforts to protect civil, political, economic and social rights in Cambodia and to promote respect for them by the Cambodian government and institutions. Building on its past achievements, LICADHO continues to be an advocate for the Cambodian people and a monitor of the government through wide ranging human rights programs from its main office in Phnom Penh and 13 provincial offices.

MONITORING & PROTECTION

Monitoring of State Violations and Women’s and Children’s Rights:
Monitors investigate human rights violations perpetrated by the State and violations made against women and children. Victims are provided assistance through interventions with local authorities and court officials.

Medical Assistance & Social Work:
A medical team provides assistance to prisoners and prison officials in 14 prisons, victims of human rights violations and families in resettlement sites. Social workers conduct needs assessments of victims and their families and provide short-term material and food.

Prison Monitoring:
Researchers monitor 18 prisons to assess prison conditions and ensure that pre-trial detainees have access to legal representation.

Paralegal and Legal Representation:
Victims are provided legal advice by a paralegal team and, in key cases, legal representation by human rights lawyers.

PROMOTION & ADVOCACY

Supporting unions and grassroots groups and networks:
Assistance to unions, grassroots groups and affected communities to provide protection and legal services, and to enhance their capacity to campaign and advocate for human rights.

Training and Information:
Advocates raise awareness to specific target groups, support protection networks at the grassroots level and advocate for social and legal changes with women, youths and children.

Public Advocacy and Outreach:
Human rights cases are compiled into a central electronic database, so that accurate information can be easily accessed and analyzed, and produced into periodic public reports (written, audio and visual) or used for other advocacy.

For More Information Contact:

Dr. Pung Chhiv Kek, President
LICADHO
#16, Street 99
Phnom Penh, Cambodia
Tel: (855) 23 72 71 02/216 602
Fax: (855) 23 727 102/217 626

E–mail: contact@licadho-cambodia.org
# TABLE OF CONTENTS

## Part 1: Introduction - A digital dawn

- Politics, money, & fear: Cambodia’s traditional media
- Restrictions on the internet in Cambodia
- The rise of digital activism

## Part 2: New media under fire

- The draft Cybercrime Law
- The draft Law on Telecommunications
- Additional threats to internet freedom

## Part 3: A new legal arsenal

- A Cambodian man uses the Facebook Social Media app on his smartphone, May 2015

## Part 4: Conclusion

## Recommendations
Part 1: Introduction- A digital dawn

OVER THE PAST FEW YEARS, Cambodia has experienced a boom in web connectivity—a development which has transformed the country’s information environment. In 2010 just 320,000 Cambodians had access to the internet; by the end of 2013 that number had climbed more than tenfold to 3.8 million—nearly a quarter of the country’s population. Driven by the increasing availability of cheap web-enabled smartphones and extensive mobile networks, young Cambodians—mostly in urban areas—have embraced social media networks like Facebook and YouTube. There are now approximately 1.76 million Cambodians on Facebook, with an estimated 1,100 new users joining every day.

Because of its late and sudden emergence, the internet is one of the few spaces left for free expression in Cambodia. Since the collapse of the Khmer Rouge regime in 1979, the ruling Cambodian People’s Party (CPP) has maintained a tight grip on the traditional print and broadcast media. Journalists have been killed, threatened, and sued for crossing invisible lines. Independent and opposition-aligned media outlets have been co-opted and forced into closure. Government broadcast licenses have been denied to independent broadcasters and the political opposition, except for one recent notable exception which arose out of secretive political negotiations that have also resulted in the passage of two highly controversial election laws. A window of free expression was opened with the arrival of the United Nations (UN) mission of the early 1990s, but was slowly forced closed during the two decades that followed.

While internet penetration in Cambodia remains low by regional standards, the spread of smartphones and digital technologies has given many Cambodians better access to information than ever before. The web, relatively free from government control, has become an essential tool through which citizens can share information on the social and political issues that affect their lives. Since 2012, web-based social media networks have been taken up enthusiastically by bloggers, monks, community activists, and opposition politicians, who have used them to circumvent government media controls and disseminate information about problems like land-grabs, police violence, corruption, and deforestation. Though the internet has also fostered the dissemination of rumor and prejudice, the rise in the use of new media including mobile phones and social media has empowered citizens...
to take part in public debate more than ever. Cambodia’s internet boom has the potential to usher in a new dawn of free and open expression.

The power of social media was on display during the national election of July 2013, which saw large and unexpected gains for the opposition Cambodia National Rescue Party (CNRP).3 Throughout the election campaign and the protracted deadlock that followed, during which the CNRP boycotted parliament over accusations of voter fraud, the internet became a critical hub for the dissemination of critical news and information. The opposition, shut out of the government-aligned broadcast media, used web-based social media networks to spread its message and organize large public rallies calling for an investigation of the election. The election was also marked by an increase in community activism and citizen journalism, as ordinary people filmed protests and police crackdowns on their phones and then uploaded them online. Starved of information from the state-controlled media, Facebook and other social networks have become one of the main alternative sources of information for a large part of the country’s population.

But Cambodia’s new-found internet freedom is under threat. Over the past few years websites have been blocked and human rights activists harassed for their online activities. Web users have been sued for views they have expressed online. New legislation has now been proposed, which seeks to control not just the content of what Cambodians post online, but also envisions central control over the very architecture of the internet itself. Since the early 1990s the government has used formal and informal methods of control to harmonize the traditional media with a stifling political consensus. Now, the very success of new media in mobilizing popular opposition to the government is spurring official efforts to curb internet freedom using the same methods as it uses to control the traditional media.4

As the government moves to extend its controls online, the future of internet freedom in Cambodia hangs in the balance.

---

3 The CNRP was created in 2012 through the merger of two major opposition parties, the Sam Rainsy Party (SRP) and the Human Rights Party (HRP).
4 https://freedomhouse.org/report/freedom-net/2013/cambodia
Part 2: New media under fire

POLITICS, MONEY, & FEAR: CAMBODIA’S TRADITIONAL MEDIA

On the surface, the Cambodian media appears one of the freest in the region. The country’s Constitution guarantees “freedom of expression, press, publication, and assembly.” Pre-publication censorship by the state is rare. Two main English-language daily newspapers, the Phnom Penh Post and Cambodia Daily, publish reports on sensitive issues like government corruption, political violence, and illegal logging, while two US-funded broadcasters, Radio Free Asia and Voice of America, beam critical reports deep into the country.

But Cambodia’s openness can be deceptive. In reality, dissenting views can only be aired within certain prescribed boundaries. Freedom of the press is permitted to the extent that it does not touch upon the entrenched economic and political interests of those in power. Behind this façade of tolerance, the Cambodian government maintains a firm grip on the country’s newspapers, radio stations, and television broadcasters. In 2008, the Cambodian League for the Promotion and Defense of Human Rights (LICADHO) reported that despite its air of apparent diversity, the Cambodian press remains “closely controlled by politics, money and fear.”

An impartial press has never really existed in Cambodia. Even after 1992-93, when the arrival of the United Nations Transitional Authority in Cambodia (UNTAC) fostered the creation of a rambunctious media, most of the publications that emerged acted as mouthpieces for the political factions and personalities that owned them. In the same sense, the current Cambodian government has never accepted the legitimacy of a neutral press, a loyal opposition, or independent civil society groups. Nor has it admitted any real distinctions between these different groups: all are seen simply as “opposition.” Since it took power in 1979, “non-government” has been CPP code for “anti-government.” As the CPP has marginalized its opponents and consolidated its control over the political landscape, the number of critical news outlets has dwindled accordingly.

2 LICADHO, Reading Between the Lines: How Politics, Money & Fear Control Cambodia’s Media (Phnom Penh, May 2008), 1.
3 For a good historical overview of the Cambodia media since independence, see Harish C. Mehta, Cambodia Silenced: The Press Under Six Regimes (Bangkok: White Lotus, 1997).
Today, most of the Cambodian press is under the de facto control of the ruling party. The English-language print media remains free and vocal, but its effectiveness is hampered by the low level of literacy in rural areas and the lack of distribution outside Phnom Penh and the large provincial towns.9 Most Khmer-language newspapers, meanwhile, are owned by business interests that are friendly to the CPP.

With the potential to effectively reach rural Cambodians, broadcast media like radio and television are subject to much tighter controls. The state broadcaster TVK is run by the ruling party, showcasing official ribbon-cuttings and speeches, but offering no airtime to opposition activities with the exception of a 30-day period during previous election campaigns. In the past, while new television and broadcast licenses have been handed out to CPP-friendly firms and businesspeople, the Ministry of Information has repeatedly refused opposition parties’ requests for bandwidth of their own.10 The press also operates on principles of payola in which cash bribes are offered publicly at press conferences in the expectation of positive coverage, or privately as an inducement for journalists willing to sidestep sensitive stories. As LICADHO has previously reported,

The partisan ownership of Cambodia’s media produces institutionalized political bias in news reporting. This bias is reinforced by a culture of corruption in which journalists are regularly bribed to attend press conferences and photo opportunities, a practice so common it isn’t even considered corruption by most Cambodian reporters. The result is news coverage weighted heavily in favor of those who can pay, namely the government and the CPP.11

Independent voices which resisted the government consensus have been subject to bribes, threats, intimidation, and other forms of official pressure. Twelve journalists have been murdered since 1993, and most of the killings remain unsolved.12 As violence has declined in Cambodian politics, and the ruling party has strengthened its control over the judiciary, critics have been increasingly subject to dubious lawsuits utilizing legal provisions governing criminal defamation and incitement. A new Penal Code, which came into force in December 2010, contains a range of provisions which criminalize various forms of expression, including “incitement,” which is so broadly defined that it can mean pretty much anything.13 Meanwhile, the government is preparing laws to regulate trade unions and non-governmental organizations (NGOs), which threaten to further undermine freedoms of association and expression in Cambodia.14

The government’s attitude towards non-government media is encapsulated well by the twisting story of Mam Sonando, the director of Beehive Radio, one of Cambodia’s only independent broadcasters. As a critical voice beamed into Phnom Penh and rural areas surrounding the capital, the former French disco owner has come under frequent attack. His radio station has been attacked by armed goons. He has fled the country, had his radio license suspended, and has been jailed on three occasions on a range of charges including incitement (2003), criminal defamation and disseminating false information (2005), and insurrection (2012)—the latter under the terms of the new Penal Code.15 These sorts of legal assaults, which take place against a background thrum of violence, serve to strongly discourage individuals from speaking out openly, fostering fear and encouraging self-censorship in a media environment that appears open, but in reality is anything but.

RESTRICTIONS ON THE INTERNET IN CAMBODIA

Unlike the traditional media, the Cambodian web remains relatively free of restrictions. However, as internet access has expanded and become a potent political tool for opponents of the ruling party, the authorities have begun applying pre-existing media controls to the online sphere. At the beginning this campaign proceeded in an ad hoc manner. Laws and restrictions were announced and then abandoned. The government attempted to block a number of critical or sensitive websites, but did so on the apparent whim of government leaders rather than according to any discernible set of criteria. Community activists and opposition supporters who are active online have been

---

1 One 2003 survey found that just 9% of respondents read a newspaper regularly. See LICADHO, Reading Between the Lines, 8-9. The adult literacy rate in Cambodia is estimated at 77.6%. Statistics available at http://www.unesco.org/new/en/phnompenh/education/learning-throughout-life/literacy/ (last accessed December 28, 2014).

2 In November 2014, Prime Minister Hun Sen announced that as part of a political agreement with the CNRP, the government would finally grant the opposition party the right to operate an analogue TV station. However, it remains too early to say how much freedom this station will enjoy if and when it goes to air. See Kuch Naren, “Hun Sen, Rainsy Settle Differences in Reform Deal,” Cambodia Daily, November 29, 2014.

3 LICADHO, Reading Between the Lines, 1.

4 See http://cgj.org/killed/asia/cambodia/ (last accessed January 26, 2015).


subject to the same menu of threats and inducements as their counterparts in the traditional media. Taken as a whole, however, these scattered attempts represent a steady trend towards increasing control over what Cambodians read and post online.

The first instance of online censorship in Cambodia took place in early 2009, with the blockage of reahu.net, a site belonging to the Khmer-American artist Koke Lor. The website came to local attention after a Khmer-language newspaper published pictures from the website including artworks featuring topless Apsara dancers and scantily-clad Khmer Rouge soldiers. Government officials, including Women’s Affairs Minister Ing Kantha Phavi, quickly condemned the images as immoral and insulting to Cambodian culture. In late January 2009, the website was reportedly blocked to users on a number of local Internet Service Providers (ISPs).

Shortly afterwards the website of the London-based anti-corruption watchdog Global Witness (www.globalwitness.org/index.php) was also briefly unavailable for some users on the AngkorNet ISP. The loss of access followed the organization’s release of Country For Sale, a hard-hitting report on corruption in Cambodia’s oil and mining industries. AngkorNet representatives confirmed that Global Witness’s website was barred to their customers, but could not provide further details as to the reasons for the restricted access. A company official later claimed the blockage was a result of technical issues. The official also denied the company blocked websites, “except what the government requests officially”—a comment that suggested such requests had been made in the past.

Since then both websites have been widely available to internet users in Cambodia.

The following year saw a number of aborted government initiatives to interfere with internet access and censor controversial web content. In February 2010, the government announced that a “morality committee” would begin reviewing websites and “consider blocking access to those deemed in conflict with national values.” At around the same time, the Ministry of Posts and Telecommunications (MPT) announced a scheme to introduce a state-run exchange point run by the state-run Telecom Cambodia (TC), which all ISPs would be forced to use as a central relay point, giving the authority de facto control over all local ISPs. Granted such powers, a TC official told the Phnom Penh Post that it would seek to block access to websites it deemed “inappropriate.”

Nothing much came of the plan to block “immoral” websites, while the centralization plan was eventually dropped after arousing strong opposition from ISPs, who were concerned about the economic impacts of the move. But the reprieve seemed to reflect a lack of technological know-how rather than any commitment to the principles of freedom of expression and opinion. This became clear on December 17, 2010, when Seng Kunnakar, a Cambodian employee with the United Nations World Food Programme...
in Phnom Penh, was arrested after he printed out an article from the web and shared it with two co-workers. The content of the article was unclear, but it was taken from KI-Media (ki-media.blogspot.com), a Cambodian diaspora blog which published news and cartoons that were harshly critical of the government and its leaders. At the time, the site featured a banner insulting leading government officials and accusing them of ceding territory to Vietnam.

The authorities wasted no time making an example of Kunnakar. In less than 48 hours Phnom Penh Municipal Court convened, convicted him of incitement, and sentenced him to six months’ jail.24 Though Kunnakar was not jailed for online communications as such, his conviction showed that the government would treat web-based dissent no differently to other forms of criticism. LICADHO Director Naly Pilorge described Kunnakar’s conviction as “groundless,” arguing that it was “further proof of the growing crackdown on freedom of expression by the Cambodian government.”25 Human Rights Watch described the case as “a profound setback for free expression in Cambodia.”26

KI-Media had clearly touched a nerve. The day before Kunnakar’s arrest, Senior Minister Var Kimhong, the chairman of the government’s Border Committee (one of those Cambodian officials referred to on the KI-Media banner), told Radio Free Asia that he had asked the government to shut down the website by the end of December.27 Sure enough, a month later, some Cambodian web users began noticing that the popular blogspot.com domain, which hosted KI-Media and other political blogs, was no longer accessible on certain ISPs, including Metfone and Ezecom. Other anti-government sites, including that run by Ung Bun Heang, the late Khmer-Australian political cartoonist whose “Sacrava Toons” creations poured invective on the CPP and the Vietnamese, also seemed to have dropped offline.

At first, ISPs denied blocking the websites and government officials denied ordering it. Ezecom stated that it experienced a technical problem which “could have potentially caused some users issues”28 and access to the websites was temporarily restored. This cover story was shot in mid-February, when users of the WiCam ISP attempting to access KI-Media were redirected to a message stating that the site had been “blocked as ordered by the Ministry of Post and Telecommunications of Cambodia.” A WiCam employee then confirmed that MPT had ordered his company to block the site, on the grounds that it “impacts the government.”29

As officials from several ministries issued denials,30 the English-language press published the leaked minutes from a meeting chaired by then Minister of Posts and Telecommunications, So Khun, on February 10, during which he asked mobile phone operators to “co-operate” in blocking certain internet sites which “affect Khmer morality and tradition and the government.”31 This was further confirmed by leaked emails from a senior MPT official in which he congratulated 10 ISPs, including Ezecom, for blocking access to a list of websites. These included KI-Media and two associated blog sites, Khmerization and Sacrava Toons. The official also explicitly named three ISPs—TeleSurf, WiCAM, and Hello—who had not yet blocked the sites and urged them to do so. “We found that you are not yet taken an action, so please kindly take immediate action,” the official wrote.32 When a reporter from the Cambodia Daily called up Ezecom CEO

---

31 Ibid.
32 Ibid.
Paul Blanche-Horgan, one of the recipients of the email, for comment, he said, “Can’t hear you,” and hung up the phone.33

In due course the controversy about the website blockages died down, but a number of affected websites—including KI-Media and Khmerization—remain inaccessible in Cambodia on some ISPs as of December 2014. But the censoring of controversial websites, however piecemeal, marked a significant milestone in the government’s attempts to muzzle an expanding Cambodian web.

Despite their denials that there was any scheme to gag critical websites, many government officials seemed to view internet freedoms in a similar way to those from more repressive neighboring countries, including Vietnam, Myanmar, and China, all of which have imposed severe restrictions on what can be accessed or expressed online. This view was encapsulated by a Chinese presentation during a February 2012 panel discussion at the UN Human Rights Council in Geneva, titled “Freedom of Expression on the Internet.” During the session, China’s delegate Xia Jingge delivered a statement on internet freedom representing the view of 29 countries including China, Vietnam, North Korea, Myanmar, Iran… and Cambodia.

While the “right to freedom of expression is one of the fundamental human rights and should be respected and protected,” Xia said, the internet is “often used to propagate terrorism, extremism and racism, xenophobia, even ideas of toppling legitimate authorities.” As a result, all internet stakeholders “should make concerted efforts to prevent and combat the abuse of Freedom of Expression on the Internet. Internet users of all countries should respect the right and dignity of others; contribute to maintaining social stability and safeguarding national security.”34

Though the methods of control differ, the rationale is much same in Cambodia. The right to free expression must be balanced against nebulous concepts like “social order” and the “reputation” of senior government officials. One official in the Ministry of Information declared that “if people love technology, they should not use technology to affect someone, especially leaders.”35 Another at the Ministry of Interior denied knowledge of any policy to block KI-Media in early 2011, but said the site deserved to be shut down in any case.36 In April 2012, the Council of Ministers Press and Quick Reaction Unit reported on a meeting between Deputy Prime Minister Sok An and European Union Ambassador Jean-Francois Cautain, during which the two discussed the government’s plan to introduce a Cybercrime Law (more on this below). “[P]eople use modern technology to spread false information,” Sok An was quoted as saying, “so we need a law to regulate them.”37

33 “E-mails Point to Collusion in Gov’t Censorship,” Cambodia Daily, February 18, 2011.
THE RISE OF DIGITAL ACTIVISM

Despite the government’s deep suspicion of the internet, its early, scattered attempts at control failed to keep pace with the rapid spread of ICTs and web access. The watershed moment was the national election of July 2013. When Cambodians went to the polls on July 28, 2013, they voted overwhelmingly for change. According to the official results released by the CPP-dominated National Election Committee (NEC), the ruling party’s share of seats was cut from 90 out of 123 to just 68, its worst electoral showing since 1998. Even then, the result was hotly disputed by the CNRP and heavily criticized by civil society organizations, who argued that the poll was marred by high levels of voter fraud and manipulation of voter lists. The CNRP announced a boycott of the newly-elected National Assembly, calling for a UN-backed probe into the conduct of the election.38

Throughout the election campaign, the CNRP had cleverly harnessed the simmering discontent about the CPP’s three-decade-plus rule. Shut out of the government-controlled traditional media, the party established a strong online presence, using social media networks to spread the party’s message and organize public rallies. When CNRP president Sam Rainsy returned to Phnom Penh on July 19, after nearly four years of self-exile, word quickly spread by Facebook and mobile phone. On arrival he was greeted at the airport by hundreds of thousands of supporters, many of whom filmed the event on their mobile phones and tablets. Mu Sochua, the CNRP’s director-general for public affairs, told the Cambodia Daily that throughout the campaign “85 to 90 percent of [CNRP] youth in the city areas were able to mobilize every day, and they were all organizing on Facebook.”39

By the time of the 2013 election, internet use in Cambodia had reached a critical mass. The number of Cambodian web users had increased more than tenfold since 2010, driven largely by the availability of affordable web-enabled smartphones and cheap mobile data.40 Community activists, citizen journalists, and urban land rights protesters began using the internet to disseminate footage of human rights abuses and police crackdowns. The internet challenged the government’s control of the political narrative, circumvented its control of the traditional media, and made it easier for a frustrated public to share and access critical information.

Of course, not everything shared online was accurate or enlightened. Supporters of both parties used Facebook and other social media networks to insult political leaders and spread baseless innuendos about the other side. CPP supporters posted lewd photos of CNRP lawmaker Mu Sochua and compared Sam Rainsy to Pol Pot, the leader of the Khmer Rouge regime. Another post claimed (falsely) to show a prominent activist monk, Venerable But Buntenh, kissing a woman.41 Facebook users and supporters of the CNRP, reflecting a widespread sentiment by Cambodians from all walks of life, also disseminated material accusing the CPP of being too close to Vietnam—the country which had installed the party in power in 1979. At times social media users, including some CNRP supporters, worked to stir up racist animosities against Vietnam, a country seen by many Cambodians as an existential threat. But even if the discussion was often messy and heated, the internet

38 In November 2013, an alliance of Cambodian NGOs including LICADHO released a report on the conduct of the election which alleged “significant challenges that undermined the credibility of the process”: Chief among them were the exclusion of eligible citizens from voter lists; the inclusion on lists of invalid or duplicate names; the failure to update the number of seats in each constituency in line with electoral laws; and the wide distribution of alternative documents for voting. See Electoral Reform Alliance, Joint Report on the Conduct of the 2013 Cambodian Elections (Phnom Penh, November 2013).
40 According to the MPT, the number of Cambodian internet users increased from 320,190 in 2010 to 3.8 million in 2013. See Sokhean, “Mobile Users Top 20 Million, Internet Usage Still Rising.”
at least gave people a forum in which to debate these issues openly.

In a broader sense, the spread of anti-government sentiment fed into a growing sense that local grievances—land-grabs, corruption, and other government abuses—were a result of systemic problems linked to the dramatic social and economic changes that have taken place since the late 1990s. The stagnation of the rural economy and the growth of Cambodia’s garment and construction industries have attracted hundreds of thousands of rural dwellers to urban areas like Phnom Penh, where they are free from the influence of the CPP’s village and commune authorities and able to access new sources of information, including the internet, which they then spread back to their villages during trips home.

The thirst for alternative sources of news was demonstrated by the sudden popularity of “I Love Cambodia Hot News,” a Facebook page founded in early 2013, which by the time of the election had attracted hundreds of thousands of followers. The “multi-media monk” Venerable Loun Sovath, an internationally-recognized human rights defender known for his active support of communities fighting land evictions, attracted nearly 100,000 followers on Facebook. Thy Sovantha, a Phnom Penh high school student who voiced strong support for Prime Minister Hun Sen himself, Oun Vansak, one of the founders of I Love Cambodia Hot News, said that before the poll, “not many people clicked ‘like’…they were still afraid. Only during the election campaign many people started [to get] involved in public issues and click ‘like’ on my page.”

Social media and citizen journalism continued to flourish throughout the tense deadlock that followed the election, when the opposition held large public rallies and garment workers took to the streets demanding higher wages. In September 2013 the CNRP established the web-based CNRP TV, which helped it circumvent the official media blackout on opposition activities. When government-employed goons were deployed against protestors, activists and citizen journalists videotaped the crackdowns and uploaded them to Facebook and YouTube. One video posted to YouTube was titled “Fight, Fight, Fight,” and featured security forces beating young men offering no form of obvious resistance.

In the more shadowy recesses of the web, “hacktivists” belonging to the Cambodian arm of the global cyber-activist network Anonymous even launched their own cyber-war against the Cambodian authorities. As part of what it termed “Operation Cambodia Freedom,” Anonymous Cambodia hacked into several dozen government websites and posted hundreds of mostly innocuous government documents online. For many different people, and in many different ways, the 2013 election marked the point at which the Cambodian web turned political.

Since then, the number of Cambodian internet users has only risen further. A survey conducted in August 2014 found that 26.1% of Cambodians owned a smartphone capable of accessing the internet, a 31.5% increase on 2013. The survey also found that just over half of people owned cellphones capable of displaying the Khmer script, the lack of which was previously a considerable barrier to access.
In response to this surge of online dissent that followed the 2013 election, the government and its supporters employed a wide range of tactics. At public demonstrations, district security guards appeared to physically target people filming violent crackdowns by the security forces, resulting in the destruction of video equipment and injuries to a number of bystanders, including accredited journalists. Similarly aggressive approaches were employed online. LICADHO understands that the government’s online campaign centered on a “cyberwar room” situated at the Council of Ministers, set up to counter the opposition’s online activities. At the same time, the government ramped up its own web presence, establishing new Facebook profiles for a number of prominent government offices and ministries.

The campaign also took more menacing forms. Activists and political figures who were active online at the time of the election report receiving threats and bribes from mostly anonymous senders, which came via phone calls and text messages, Facebook messages posted from fake accounts, and videos posted to the Facebook profiles of CPP supporters. Thy Sovantha, the high school student who rose to prominence during the election for her feisty Facebook posts, said she “cannot count” the number of times she received threats by phone or Facebook, warning her of jail or worse. Ren Chanrith, a youth activist who has been active in the vocal NGO campaign to halt the construction of the Stung Chhay Areng dam in the Cardamom Mountains, recalled that “a fake person who used a fake account threatened to kill me.”

One of the main government targets has been the monk activist Venerable Loun Sovath. Since he began documenting land rights issues in 2009, Venerable Sovath has been subject to a range of government pressures: in 2011 he was expelled from Wat Ounalom, a pagoda in Phnom Penh, because of his critical activism, followed by a generalized ban preventing him from staying in any pagoda. Later he was threatened with being defrocked and ordered to sign a statement promising to end his support of community activists. In November 2014, he appeared at Phnom Penh Municipal Court on a number of charges related to his political activism, including incitement.

Alongside threats, some individuals have also received inducements. Venerable Prim Huon, a monk and online...
activist, says he was contacted by an anonymous Facebook user who offered him US$1,000 in exchange for shutting down his profile page and stopping his posts of critical news and information.53 As with the anonymous threats and bribes offered to journalists investigating sensitive topics, there is little hard evidence that these were authorized by the highest levels of government. They have nonetheless cast a pall of fear over the new information landscape. Kem Monovithya, the CNRP’s deputy director-general for public affairs, said the government’s aim was to create a zone of chaos online, flooding the Cambodian web with rumors and insults, so that nothing could be trusted.56

At the same time as the post-election deadlock was playing out, a string of landmark cases were quietly working their way through the Cambodian courts, involving communications made on the internet. These all demonstrated the slow extension of offline control tactics to the digital media:

►►► On February 23, 2013, Phel Phearun, a teacher, was summoned to court after criticizing the Phnom Penh traffic police on his Facebook profile.55 One police officer claimed the post was “written with the intention of defaming the police. It affects my reputation and my organization.” The charges were eventually dropped.56

►►► On November 20, 2013, Cheth Sovichet, a 23-year-old marketing manager, was detained in Stung Treng province after posting a photo of the provincial military police commander on Facebook, accusing him of extortion. “It is defamation and disinformation which affects my dignity,” said Colonel Ieng Vandy, the target of the post. Sovichet was questioned and then released after he “admitted his mistake.”57

►►► On February 6, 2014, Phnom Penh Municipal Court fined Duong Solida, a 29-year-old hairstylist and make-up artist, 2 million riels (about $500), and ordered her to pay 5 million riels (about $1,250) to a rival beauty parlor owner she accused of stealing her staff in 2012.58 The Cambodian Center for Independent Media described the verdict as “a troubling development for internet freedom and freedom of speech in Cambodia.”59

►►► On July 23, 2014, the court found the British journalist Rupert Winchester guilty of defaming Etienne Chenevier, a French property developer, in a post on his personal blog. Winchester was ordered to pay $25,000 in damages to Chenevier and fined a further $2,000.60 Bob Dietz of the Committee to Protect Journalists, said that the case “could have a chilling effect on online speech in Cambodia, which is already at risk.”61 The case is currently under appeal.

While the number of cases relating to freedom of expression on the internet remains small, they demonstrate the courts’ willingness to criminalize even the most innocuous forms of online content. Indeed, these cases have been accompanied by signs that the government is preparing to establish a more comprehensive legal control of what Cambodians post and read online.

53 Interview with Ven. Prem Houn, October 22, 2014.
54 Interview with Kem Monovithya, October 28, 2014.
56 “Charges on Defamation Case Against Facebook User Dropped,” statement from the Cambodian Center for Independent Media, March 29, 2013
59 “Sentencing of Facebook User a Threat to Internet Freedom,” statement from Cambodian Center for Independent Media, February 17, 2014.
Part 3: A new legal arsenal

Until now, the Cambodian government’s approach to freedom of expression and opinion on the internet has been piecemeal, scattered, and poorly coordinated. Despite the intimidation of online activists and the recent court cases relating to online speech, there is still no central regulatory body overseeing the digital landscape in Cambodia, and there are few official restrictions on access to the internet. Such controls as do exist have been implemented on an individual-case basis, or through internal circulars—documents which are supposed to simply explain or clarify existing regulatory measures. To date, two such circulars have been issued which pertain to internet access and freedom of expression online. In February 2012, the MPT and Ministry of Interior issued a circular ordering internet cafés to install surveillance cameras to film their clients and store footage of users for a period of three months. It also ordered mobile phone shops and telecommunications operators to register subscribers’ information and provide it to government officials on request. This it justified in the interests of preserving “national security, safety and social order.”

A second circular was issued in November 2012, calling for the relocation of all internet cafés within a 500-meter radius of schools and educational institutions in urban centers, including the capital Phnom Penh. The purported reason for the circular was children’s addiction to video games and criminals’ use of the internet to commit a range of crimes including drug trafficking, extortion, and the distribution of pornography.

Cambodian NGOs argued that the November circular could potentially apply to most of the internet cafés in Phnom Penh, adding that many of the crimes it was supposedly targeting were already illegal under Cambodian law. Given the fact that internet cafés are one of the main ways in which Cambodians access the web, LICADHO described the circular as “not only legally unfounded” but also as “a transparent attempt to block part of the population’s access to independent sources of information through news sites and social media.” The circular caused an immediate backlash from internet café owners. The open-source urban mapping site Urban Voice also organized an online campaign to “Save the Internet Cafés,” So Khun later claimed that the government had no intention of closing down businesses, but would warn café owners allowing access to pornographic websites and

---

63 For a translation of the circular, see “Some Internet Cafes Ordered to Close,” statement from Cambodian Center for Independent Media, December 14, 2012.
64 ‘New Circular Aims to Shut Down Internet Cafes in Cambodia,’ statement from LICADHO, December 13, 2012.
other sensitive material.\textsuperscript{46} As far as LICADHO is aware, the first “surveillance” circular is yet to be implemented, while the second has only come into force in Siem Reap province, according to the organization’s provincial monitors. But the two pieces of regulation provided just a foretaste of the sort of provisions that would later be included in a new draft Cybercrime Law—the government’s first attempt to comprehensively regulate the digital media.

**THE DRAFT CYBERCRIME LAW**

Government plans for a Cybercrime Law were first announced in May 2012. At the time, Ek Tha, a spokesman of the Council of Ministers, described the law in familiar terms—as an attempt to “prevent any ill-willed people or bad mood people from spreading false information, groundless information that could tend to mislead the public and affect national security or our society. We need to control this.”\textsuperscript{67} Chem Sangva, director-general of the inspection department at MPT, told the Phnom Penh Post that the law “would help prevent such crimes as terrorism or from other ill-willed people stealing state secrets.”\textsuperscript{68}

A version of the draft legislation wasn’t leaked to the public until April 2014.\textsuperscript{69} The government’s justification was that the law was needed to fight online criminal activity. The purpose of the law, according to an unofficial translation of the draft, is to “determine education, provision measures, and combat all kinds of offense committed by computer system[s].” The law envisions the creation of a new National Anti-Cybercrime Committee (NACC), chaired by Prime Minister Hun Sen and stacked with high-ranking ruling party officials. Most of the draft law is taken up with provisions outlining the duties and powers of the new NACC, procedures for the seizure of computer equipment thought to be used in the commission of crimes, and provisions detailing a range of online criminal activities offenses would be punishable under the law.\textsuperscript{70} Many of these are uncontroversial. Article 27 bans child pornography; Article 31 targets online fraud. (Indeed, some articles appear to have been copied wholesale from the 2001 European Convention on Cybercrime).\textsuperscript{71} But Article 28 of the draft law has deeply troubling implications for the future of internet freedom in Cambodia. Specifically, the provision outlaws the production, publication, or sharing of any content “deemed to hinder the sovereignty and integrity of the Kingdom of Cambodia.” It also criminalizes content designed “to incite or instigate the general population that could cause one or many to generate anarchism,” any publications “deemed to generate insecurity, instability, and political cohesiveness,”\textsuperscript{72} and anything “deemed to be non-factual which slanders or undermined [sic] the integrity of any government agencies.” This provision carries harsh penalties: up to three years prison and fines of up to 6 million riels (around $1,500). Violation of any part of the law could also lead to the temporary suspension of an individual’s civil rights, according to the draft, including the ability to vote in elections.

As of publication, the future of the Cybercrime Law was uncertain. On December 11, 2014, the Council of Ministers announced that it had “scrapped” the controversial draft, with one official claiming that it was “not a priority” any longer. But Chheang Vun, a senior CPP lawmaker and National Assembly spokesman urged MPT and the Ministry of Interior to resume drafting the “very important” law. “There are many crimes involving the Internet,” he told journalists. “If we don’t have the law to control it, we will die in the future.”\textsuperscript{73}

As it stands, the provisions of the Cybercrime Law are so broad and vaguely defined that the law could be stretched to encompass nearly any form of critical online content. If
the recent cases against Phel Pearun, Duong Solida, and other web users are any indication, it is highly likely that the Cybercrime Law, if passed in its current form, would be used to stifle citizens’ freedom of expression by applying broad restrictions that could easily apply to routine news postings, citizen journalism, and online commentary. The government has misused the Penal Code and other laws to chill dissent and foster self-censorship in the traditional media; Article 28 of the Cybercrime Law could well have the same effect on online speech. Oun Vansak, the founder of the I Love Cambodia Hot News Facebook page, said he was more concerned by the law than he is by the anonymous threats he has received: “The law is different. When the law comes out, for sure I will be in trouble.”

The Draft Law on Telecommunications

In mid-July 2014, two months after the Cybercrime Law was leaked, MPT gave Cambodia’s telecommunications operators the draft of a second piece of key legislation—a new Law on Telecommunications. The new law, which was promptly leaked to the press, targets the firms operating Cambodia’s telecommunications networks. It appears to aim at nothing less than the extension of government control over the very architecture of the internet itself:

The draft envisions the creation of a Telecommunication Regulator of Cambodia, or TRC, with enhanced powers to conduct investigations into telecoms licensees, stakeholders, and more or less anyone else it chooses. If found in breach of the law, the TRC also has the power to grant, review, suspend, or revoke their permits.

Though Article 60 proclaims users’ rights to privacy and security, this is effectively undermined by other provisions requiring telecoms operators and other stakeholders to provide the MPT with all telecoms service data and other information.

Some of the most overarching powers are contained in Article 7, which gives the MPT the power to order any telecoms operator to transfer control of its system to the ministry in order to “maintain national interest, security, stability, or public order.” These criteria are not defined in any clear or objective way. Together, Articles 6 and 7 give the legal pretext for the invasive electronic surveillance of Cambodia’s population, undermining the privacy rights detailed in Article 60.

In a similar way, the draft law also gives MPT “control” of the telecoms infrastructure and network, and all supporting infrastructure. Further provisions give the new TRC the power to decide who can sell and repair telecoms equipment, and require website hosts to obtain a TRC permit for provision of internet, radio, or television services. Failure to do so would lead to jail terms of up to 10 years.

The TRC has the power to fire and hire managers at any telecoms company deemed to have violated the law. This also gives the body the power to order licensees to stop or restrict their activities, even if they are in compliance with the law.

Further provisions would outlaw the installation of telecoms equipment that might “affect public order or national safety and security.” The punishments are harsh: up to 15 years in prison, plus a fine of up to 5 billion riels (around $1,250,000). The law also outlaws the use of such equipment for the same reasons, an offense which carries punishments of five to ten years in jail, and fines as high as 1 billion riels (around $250,000). These vague clauses could potentially encompass any telephone call or email that is viewed as hostile by the government. Even if a crime has not yet been committed, jail terms of up to ten years apply to “any threat to commit crime directly or indirectly” through electronic means. Even the unintentional damage of telecoms infrastructure is punishable by three years in prison and hefty fines.

Finally, Article 82 of the law would outlaw electronic eavesdropping, but excludes from punishment any surveillance authorized by MPT, essentially giving the ministry the legal right to the surveillance of citizens’ communications.

74 Interview with Oun Vansak, November 24, 2014.
75 This and subsequent references are taken from an unofficial translation of the Draft Law on Telecommunications, dated June 19, 2014.
76 Article 8 and Article 12 of Draft Telecommunications Law
77 Article 11 of Draft Telecommunications Law
78 Article 6 of Draft Telecommunications Law
79 Article 7 of Draft Telecommunications Law
80 Article 27 of Draft Telecommunications Law
81 Articles 15–17 of Draft Telecommunications Law
82 Article 63 of Draft Telecommunications Law
83 Article 71 of Draft Telecommunications Law
84 Article 72 of Draft Telecommunications Law
85 Article 81 of Draft Telecommunications Law
86 Article 75 of Draft Telecommunications Law
Taken as a whole, the draft Law on Telecommunications appears to be nothing short of an attempt to establish overarching central control over Cambodia’s internet and telecommunications infrastructure. As with the draft Cybercrime Law, many provisions in the draft are vague, allowing excessive discretion on the part of MPT and the law’s envisioned telecoms regulator. The law carries such harsh penalties that it would be very hard for a telecommunications company to refuse an order from the government, even if the instructions were clearly irrational or politically motivated. Speaking to the Phnom Penh Post, one industry source described it as “draconian.” “The draft is clearly out to give government total control and power over the industry and not encourage any further investment or innovation… It goes totally against any international precedent.”

In essence, the law envisions the de facto nationalization of Cambodia’s telecoms industry. Taken together, these two proposed pieces of legislation—the Cybercrime Law and the Law on Telecommunications—pose a severe threat to the freedom of expression and opinion on the internet in Cambodia. If passed in their current forms, they would create a comprehensive legal framework, which would move beyond ad hoc measures to extend the government’s control over all aspects of the online space in Cambodia.

### ADDITIONAL THREATS TO INTERNET FREEDOM

Whether or not these laws are ultimately signed into law, more recent developments testify to the priority the government now attaches to the control of the Cambodian web. In September, not long after the Law on Telecommunications was leaked, the Ministry of Information announced its own competing scheme to vet online content. According to Ouk Kimseng, who headed the ministry’s initiative, a list of “banned words” were being assembled with the aim to rid the net of obscenity, defamation, and discrimination. “We want to tell internet users to not use words relating to pornography and words relating to hatred and discrimination,” he said. He made special mention of Facebook, whose “users must know how to consider the reputation and dignity of individual people.”

Troublingly, Sok Chanda, the CEO of the MekongNet ISP told the Cambodia Daily he would comply with any government request to block certain websites. “I will follow the law if the ministry issues it,” he told the paper. “The ministry can withdraw my license if I don’t.”

Not long afterward, two computer “hacktivists” from the network Anonymous Cambodia, arrested as part of a sting operation in mid-2014, were convicted for their role in hacking government websites in the aftermath of the 2013 election. But the pair were released on suspended sentences from prison after they agreed to put their skills to work combating cybercrime in the Ministry of Interior.

One Interior Ministry official announced that the duo would be placed on probation and given the opportunity to “show that they are honest now and will really use their abilities to serve the police.”

---

89 Ibid.
90 Buth Reaksmey Kongkea, “Hackers Cut Deal To Work For Gov’t,” Phnom Penh Post, October 1, 2014.
In October 2014 the Press and Quick Reaction Unit at the Council of Ministers ordered the creation of a Cyber War Team (CWT) to monitor and collect information from Facebook and other websites in order to “protect the government’s stance and prestige.” An order signed by Sok An on October 15, states that the new body’s duty would be to monitor and disseminate information from “websites, Facebook, Twitter, Google-plus, blogs, YouTube and other media outlets.” This appeared to be a formalization of the cyber-war panel believed to have directed the government’s attempts to counter the CNRP’s online presence during the election.

Then, just a few days later, officials from the Ministry of Interior’s department of internal security—the same body which had investigated and arrested several “hacktivists” from Anonymous Cambodia—visited the headquarters of Cambodian telecoms firms and ISPs to examine their network equipment and look through their billing records and data logs. The basis for the inspection was an October 7 letter from the MPT ordering all phone and Internet providers to open their doors to the investigators so they could “study in detail the technical equipment of all the operators.” Government officials said the inspections were carried out in order to target online fraudsters using Voice over Internet Protocol (VoIP) to scam web users.

Later, the Cambodia Daily reported that the government planned to go further still and install surveillance equipment on the networks of telecoms operators and ISPs. “[W]hat is important for us now is that we can strictly control people using the Internet and mobile [networks],” said one official from the Interior Ministry’s department of internal security, arguing that once installed, the use of surveillance equipment could only happen with the permission of the courts. While some experts say the inspection and surveillance of telecoms networks can sometimes be legitimate, the lack of judicial independence means that there are few safeguards against the abuse of these powers.

Recent telecommunications deals between China and Cambodia only underscore the concerns about government surveillance. In late 2014, Prime Minister Hun Sen visited Beijing and met with the acting CEO of Huawei, proposing a “strategic partnership” between the Cambodian government and the Chinese telecommunications giant. In January 2015, Huawei donated US$200,000 worth of IT equipment to the Ministry of Telecommunications. Then, on January 27, Cambodia and China signed a broad Memorandum of Understanding on cooperation in telecommunications and information technology. Under this deal, media outlets reported, “both sides will exchange information, experience and expertise.” Details on what forms this cooperation will take remain unknown to the public. But given China’s ambivalent attitude towards internet freedom, there is a danger that further exchanges with Beijing might help Cambodia equip itself with technologies that would give it greater control over the telecoms and online communications.

These recent developments point overwhelmingly in the direction of a greater degree of internet control and censorship in Cambodia. By hook or crook, the government seems keen to increase its control of the Cambodian web, foreclosing the possibility that it could act as a communications alternative outside of official control.

---

95 Pheap and Wilwohl, “Gov’t Plans to Install Surveillance Equipment.”
97 “HUAWEI Smartphone company donates IT equipments cost 700,000 USD to Cambodia’s Ministry of Post and Telecommunication; http://shar.es/1o7fb6
98 “Cambodia, China ink cooperation deal on telecom, ICT,” Xinhua, January 27, 2015.
An observer films crackdown on supporters of Beehive radio owner Mam Sonando in front of Ministry of Information, January 2014
Part 4: Conclusion

When the UNTAC mission arrived in Cambodia in 1992, it pried open a closed socialist system and provided the space for the creation of a media that broadcast a wide, albeit politically-tinted, range of views. In the years since, this space for expression has shrunk as the CPP has consolidated its hold on the Cambodian political landscape. The media was gradually brought to heel by a combination of threats, bribes, and intimidation, until most of the country’s print and broadcast outlets were either out of business or harmonized with the government’s political consensus. The small number of remaining non-government outlets are constantly on the defensive, awaiting the crackdowns that seem to sweep across the Cambodian political landscape every few years.

But the exponential growth of internet access and use over the past three years has opened a second window for free expression. Today—even after the drafting of new laws aimed squarely at restricting internet use in Cambodia—web users are subject to few official controls. The proper answer to this is not more controls, but more openness. Only in a climate of free expression and freedom of opinion will Cambodians be able to sift the good ideas from the bad. Only with a legally-enshrined right to free speech online will these ideas be able to be contradicted and debated openly. If views can’t be aired openly—online or elsewhere—they will only grow.

Unfortunately, the current Cambodian government appears to have set its sights in a different direction. In the past two years, the government has contrived an expanded arsenal of legal tools and embryonic surveillance schemes that seem almost tailor-made to target the expression of dissenting opinions on the internet. The past two decades have shown the government’s willingness to use such laws above, the government and its agencies have shown little hesitation to criminalize online communications or target activists who utilize social media to get their message across. Similar to leaders from more repressive countries like China and Vietnam, the government sees freedom of expression and freedom of opinion not as rights, but as indulgences which have to be subordinated to the vaguely-defined imperatives of “national security” and “social stability.”

Of course, both supporters and detractors of the CPP have used the internet to spread rumors, insults, prejudice, and misinformation. But the proper answer to this is not more controls, but more openness. Only in a climate of free expression and freedom of opinion will Cambodians be able to sift the good ideas from the bad. Only with a legally-enshrined right to free speech online will these ideas be able to be contradicted and debated openly. If views can’t be aired openly—online or elsewhere—they will remain confined to the shadows, where, in the absence of air and light, they will only grow.

Unfortunately, the current Cambodian government appears to have set its sights in a different direction. In the past two years, the government has contrived an expanded arsenal of legal tools and embryonic surveillance schemes that seem almost tailor-made to target the expression of dissenting opinions on the internet. The past two decades have shown the government’s willingness to use such laws
as it has in the service of political harmonization and the quashing of dissenting viewpoints. If passed, the draft Cybercrime Law and draft Law on Telecommunications would give the government the power to control not just what appears on citizen’s computers and smartphones, but also the very structures which deliver the information in the first place.

As with the traditional media, there would be no need to prosecute every instance of critical speech, just enough to plant the seed of doubt and fear in the minds of Facebook users, bloggers, and community activists. In this climate, freedom of expression on the internet would be held subject to a range of capricious controls. In short, it would cease to exist in any meaningful way. Internet access is spreading to more and more of the Cambodian population. But for the freedom to speak openly online, time is running out.

RECOMMENDATIONS

►►► We call upon the Royal Government of Cambodia to immediately release, for public consideration, the most recent drafts of legislation intended to regulate all forms of online activity and, more generally, to adopt and implement a transparent legislative drafting process.

►►► We urge the National Assembly to reject any legislation that seeks to impose severe restriction on fundamental rights to freedom of expression.

►►► We call upon the Cambodian judiciary to secure an independent justice system and to put a stop to the use of defamation charges to suppress the constitutionally enshrined freedom of expression in Cambodia.

►►► We urge members from the Cambodian business community and civil society to call upon the Royal Government and the National Assembly to adopt and implement a transparent legislative drafting process, including adequate time to hold public consultations and receive public comments.

►►► We urge international donors and the international community at large to recognize and acknowledge that a vital space for freedom of expression in Cambodia is under serious threat, and this space needs to be promoted and protected in better ways.