



THE PHILIPPINES

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	8	10
Total (0-100)	23	25

POPULATION: 96 million
INTERNET PENETRATION 2012: 36 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

* 0=most free, 100=least free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- The Cybercrime Prevention Act of 2012, currently suspended by the Supreme Court, would allow authorities to block online content without a warrant, facilitate government surveillance, and punish online libel with up to 12 years’ imprisonment (see **LIMITS ON CONTENT** and **VIOLATIONS OF USER RIGHTS**);
- Civil society activism fuelled 15 petitions to the Supreme Court to suspend the new Cybercrime law; its status going forward is unclear (see **LIMITS ON CONTENT**).
- As of March 2013, there were eight proposed bills in the Senate calling for regulation of online child pornography, gambling, and phishing, which could add to overbroad restrictions on cybercrime (see **LIMITS ON CONTENT**).

INTRODUCTION

People in the Philippines enjoy nearly unrestricted access to the internet. There have not been any reports of the government systematically blocking access to online content. This excellent record was marred in September 2012 by the passage of an anti-cybercrime law boosting official powers to censor and monitor internet users without judicial oversight.

The Philippines first connected to the internet almost twenty years ago via the Philippine Internet Foundation, but experienced very low penetration until the government deregulated the industry in the 1990s, allowing new players to compete with the dominant Philippine Long Distance Telephone Company (PLDT). Recent mergers and acquisitions, however, mean PLDT controls 70 percent of the market and still lacks the kind of competition that would spur it to innovate or become more efficient for the end user. In addition to this the de facto monopoly, lack of infrastructure and bureaucratic government regulation continue to slow penetration. Mobile phone use is more widespread, though this has yet to result in higher mobile internet use.

During the coverage period for this report, the senate approved the notorious Cybercrime Prevention Act, which President Benigno Aquino Jr. signed into law in September. Civil society groups and lawyers immediately petitioned the Supreme Court to issue a restraining order against it, particularly provisions that allow the government to block content without a court order, monitor online activities with the help of service providers, and classify libel—already criminalized under the penal code to the detriment of free expression—as a cybercrime punishable by harsher jail terms than the same offence committed offline. The court, under newly-appointed Chief Justice Maria Sereno, suspended the law’s implementation indefinitely on grounds that it may be unconstitutional. Sereno’s predecessor was unseated in an impeachment trial related to corruption allegations in May 2012.

This suspension, while positive, left the status of the law ambiguous, and drew attention to its creators’ intent in ways that are already chilling online expression. In oral arguments defending it, a government lawyer warned that “liking” a defamatory Facebook post is tantamount to committing libel. A libel complaint over a YouTube video is pending, since the investigation cannot continue until the status of the law is clarified. Meanwhile, the Philippine National Police formed an Anti-Cybercrime Group based on one of the act’s provisions in early 2013; it is unclear how the law’s suspension will affect the group’s activities.

OBSTACLES TO ACCESS

Internet penetration in the Philippines stood at 36 percent in 2012.¹ Usage is concentrated in urban areas, with rural areas largely underserved.² A significant number of users still rely on dial-up connections, as just two percent of the population had fixed broadband subscriptions in 2012.³

Mobile phone subscriptions, on the other hand, have increased significantly in recent years, with penetration reaching 107 percent in 2012, indicating that some users have more than one device.⁴ SMS has been hugely popular for 2G cell phone users since the mid-2000s. Penetration of 3G devices enabling internet access remained comparatively low, at 11 percent, at the end of 2012.⁵ In the first quarter of 2013, leading mobile service providers Globe Telecommunications and PLDT wireless subsidiary Smart Communications began expanding 4G LTE coverage outside the metropolitan area surrounding the capital, Manila.⁶ Smart was also reportedly testing to improve mobile data speeds.⁷

The government does not place any known restrictions on internet connectivity. Indeed, bridging the digital divide through development of ICT infrastructure is one of the goals of the government's Philippine Digital Strategy for 2011 to 2016. As a result, it is now testing TV White Space technologies—which tap previously unused frequencies and overcome physical obstacles like concrete or dense foliage—to increase connectivity in poor rural areas.⁸ However, steep broadband subscription fees still stand in the way of higher penetration in a country where 42 percent of the population lives on US\$2 a day.⁹ In 2013, even as legislators urged telecoms to cut rates by 50 percent in order to promote universal access,¹⁰ the average cost of broadband subscriptions remained between \$7 and \$19 a month.¹¹

An industry monopoly has contributed to these inflated costs. In the 1990s, government legislation allowed competitors a foothold in the market, previously dominated by the PLDT, a company that

¹ International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

² Tam Noda, "Phl to Test TV White Space Technology in Rural Areas," February 1, 2013, *Philippine Star*, <http://www.philstar.com/nation/2013/02/01/903696/phl-test-tv-white-space-technology-rural-areas>.

³ International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2012."

⁴ International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2012."

⁵ Mary Meeker and Liang Wu, "2012 Internet Trends," Kleiner Perkins Caufield and Byers, <http://kpcb.com/insights/2012-internet-trends-update>.

⁶ Marlon C. Magtira, "Globe, Smart Activate New LTE Sites," February 20, 2013, *Manila Standard Today*, <http://manilastandardtoday.com/2013/02/20/globe-smart-activate-new-lte-sites/>.

⁷ "Philippines Network Tests Huawei Supplied TDD-LTE Infrastructure," *Cellular-News*, March 21, 2013, <http://www.cellular-news.com/story/59148.php>.

⁸ Tam Noda, "Phl to Test TV White Space Technology in Rural Areas."

⁹ Oxford Poverty and Human Development Initiative, "Philippines Country Briefing," Multidimensional Poverty Index Data Bank, (University of Oxford, 2013) <http://www.ophi.org.uk/wp-content/uploads/Philippines-2013.pdf?cda6c1>.

¹⁰ Newsbytes.ph, "79% of Philippines Homes no Internet, Telcos Urged to Cut Rates," January 21, 2013, *Digital News Asia*, <http://www.digitalnewsasia.com/digital-economy/79percent-of-philippines-homes-no-net-access-telcos-urged-to-lower-rates>

¹¹ Based on current rates published by the three biggest providers: Sun Broadband (owned by Digitel and acquired by PLDT in October 2011), PLDT, and Globe Telecom as of March, 2013.

had been US-owned and Philippine government-owned before its current incarnation as a private entity.¹² However, in the absence of antitrust laws to promote healthy competition between businesses, the PLDT has retained its dominance through a series of mergers and acquisitions. After acquiring majority shares in rival Digitel Telecommunications in 2011, it now controls 70 percent of the country's ICT sector.¹³

Although the industry appears to have diversified, some of these changes are superficial: The most recent government statistics reported 304 registered internet service providers (ISPs) as of 2010,¹⁴ yet most connect to the international internet through the PLDT. The company still owns the majority of fixed-line connections—and consequently the most stable backbone—as well as the 10,000-kilometer domestic fiber optic network that connects to several international networks. It also owns or manages several international cable landings,¹⁵ and offers the highest total bandwidth capacity of 250 Gbps.¹⁶

By the end of 2012, the only remaining challenger to PLDT's Smart was Globe Telecommunications, which purchased debts amounting to billions of Philippine pesos from struggling competitor Bayan Telecommunications in 2013 with a view to acquiring the company.¹⁷ The rivalry has not resulted in the kind of competition which reduces costs and increases efficiency for the end user. Instead, Smart and Globe have been mired in negotiations over interconnecting their networks for several years, which has also delayed the development of broadband services in many areas.¹⁸ Interconnection allows customers to communicate with users on rival networks without incurring extra costs.

Companies entering the market go through a two-stage process. First, they must obtain a congressional license that involves parliamentary hearings and the approval of both the upper and lower houses. Second, they need to apply for certification from the National Telecommunications Commission, which has regulated the industry with quasi-judicial powers and developed tariff and technical regulations, licensing conditions, and competition and interconnection requirements since its creation in 1979. The constitution limits foreign entities to only 40 percent ownership of a business to be established in the country. Internet service is currently classified as a value-added service and is therefore subject to fewer regulatory requirements than mobile and fixed phone services.

¹² Mary Ann Ll. Reyes, "PLDT: From Voice to Multi-Media (First of Two Parts), *Philippine Star*, <http://www.philstar.com/business-usual/2012/10/22/859665/pldt-voice-multi-media-first-two-parts>.

¹³ Winston Castelo, "Controversy on PLDT-Digitel Merger," The Official Website of Congressman Winston "WINNIE" Castelo, November 22, 2011, <http://www.winniestel.net/controversy-on-pldt-digitel-merger/>.

¹⁴ National Statistics Office, "Philippines in Figures 2012," Republic of the Philippines, accessed July 2013, http://www.census.gov.ph/old/data/publications/pif2012_in_CD.pdf.

¹⁵ Erwin A. Alampay, "ICT Sector Performance Review for Philippines," in *Sector Performance Review (SPR)/Telecom Regulatory Environment (TRE)* (LIRNEasia, 2011).

¹⁶ Darwin G. Amojelar, "PLDT says Internet Bandwidth Capacity Up More than Half with Asia Submarine Cable Project," *InterAksyon*, February 22, 2013, <http://bit.ly/1bmgY0r>.

¹⁷ "Globe Used 'Excess Funds' to Buy Bayan Debt – CFO", January 7, 2013, *Rappler*, <http://www.rappler.com/business/19281-globe-used-%E2%80%98excess-funds%E2%80%99-to-buy-bayan-debt-cfo>.

¹⁸ Aya Lowe, "NTC to Intervene in PLDT-Globe Interconnection Row," March 6, 2013, *Rappler*, <http://www.rappler.com/business/23135-ntc-to-intervene-in-pldt-globe-interconnection-row>.

Institutions governing the ICT sector are highly bureaucratic, often with ambiguous or overlapping responsibilities which slow the pace of development. Successive government administrations have modified the structure of official ICT bodies, including President Benigno Aquino. His Executive Order 47 of 2011 established an Information and Communications Technology Office under the Department of Science and Technology (DOST) tasked with conducting research, development, and capacity-building in the ICT industry.¹⁹ However, the division of labor between this office and the Department of Transportation and Communications, which also deals with ICT-related communications, as well as the National Computer Center and the Telecommunications Office, was hard to perceive.

A streamlining process is anticipated. In 2012, Senate Bill No. 50 was passed to create a separate and specialized Department of Information and Communications Technology. The bill is pending before a bicameral conference committee before being transmitted to the president for approval.²⁰ If authorized, all other ICT-related agencies will be abolished and their powers and personnel transferred to the new department. Some DOST officials challenged the necessity of creating the new department.²¹

All relevant government bodies are headed by presidential appointees. Critics believe this creates a dependence on the incumbent administration and Congress, which determines their budget.²²

LIMITS ON CONTENT

In the year's most significant development, the 2012 Cybercrime Prevention Act was passed into law in September, threatening to infringe on the Philippines' otherwise open online environment by introducing content restrictions that even a government lawyer admitted are unconstitutional. Under the now-suspended act, the Department of Justice can block online information without a warrant.

While the new anti-cybercrime act remains on hold, there is no systematic government censorship of online content, and internet users in the Philippines enjoy unrestricted access to both domestic and international sources of information. A wide range of Web 2.0 applications, including YouTube, Facebook, Twitter, and international blog-hosting services, are freely accessible. No incidents of politically-motivated website blocking have been reported.²³ The OpenNet Initiative

¹⁹ Executive Order No. 47, June 23, 2011, Official Gazette, <http://www.gov.ph/2011/06/23/executive-order-no-47/>.

²⁰ Ricardo Saludo, "Will ICT finally get its own department?" *Manila Times*, April 30, 2012, <http://www.manilatimes.net/index.php/opinion/columnist1/21967-will-ict-finally-get-its-own-department>.

²¹ Patrick Villavicencio, "DOST Withdraws Support for Dept of ICT," August 23, 2012, *InterAksyon*, <http://www.interaksyon.com/infotech/dost-withdraws-support-for-dept-of-ict>.

²² Erwin A. Alampay, "ICT Sector Performance Review for Philippines."

²³ Jacques D.M. Gimeno, "Democracy as the Missing Link: Global Rankings of e-Governance in Southeast Asia," in *E-Governance and Civic Engagement: Factors and Determinants of E-Democracy* ed. A. Manoharan and M. Holzer (Hershey, PA: IGI Global, 2012), 561-583.

found no evidence of national filtering,²⁴ though several organizations reported monitoring and filtering activities in the workplace.²⁵

The Cybercrime Prevention Act, signed into law on September 12, 2012, allows the Department of Justice to “restrict or block” content without a court order, including some overly-broad categories like “cybersex,” which fails to differentiate between consensual and illegal acts.²⁶ The law’s most troubling provisions introduce punitive jail terms for online libel, outlined in Violations of User Rights.

The reaction to the passing of this punitive piece of legislation was encouraging, if full of apparent contradictions. Before it took effect, the act’s own sponsor, Senator Edgardo Angara, stated that he would amend it to require a court order in support of content restrictions: “I’m trying to trace in the record who introduced this kind of provision,” he told local journalists.²⁷ Activists moved quickly to prevent the act’s implementation, and different groups and stakeholders had filed 15 petitions with the Supreme Court to question its constitutionality by January 2013.²⁸ In response, the justices issued a 120-day restraining order to prevent the law from being acted upon, which the court extended indefinitely in February 2013; in oral arguments, the government’s lawyer acknowledged that the clauses relating to content restrictions were unconstitutional.²⁹ Meanwhile, Senator Miriam Defensor Santiago filed a rival bill with congress that, if passed, would repeal the act.³⁰ Santiago told journalists her Magna Carta for Philippine Internet Freedom bill “provides for court proceedings in cases where websites or networks are to be taken down and prohibits censorship of content without a court order.”³¹ It is not clear how much support Santiago’s bill may attract, and passing a bill in the Philippines can take months or even years.

As of March 2013, there are eight other proposed bills in the Senate calling for regulation of online content pertaining to child pornography, gambling, and phishing, some of which would require ISPs, web hosting services and educational institutions to monitor users and disable access to banned content. The Anti-Child Pornography Act of 2009 also requires ISPs to install unspecified “available technology, program or software” to filter content prohibited by the act.³²

²⁴ OpenNet Initiative, “Internet Filtering in Asia,” 2009, <http://opennet.net/research/regions/asia>.

²⁵ Erwin A. Alampay and Regina Hechanova, “Monitoring Employee Use of Internet: Employers’ Perspective,” *Inquirer*, January 24, 2010, <http://business.inquirer.net/money/topstories/view/20100124-249272/Monitoring-employee-use-of-Internet-Employers-perspective>.

²⁶ “Republic Act 10175,” Official Gazette, September 12, 2012, <http://www.gov.ph/2012/09/12/republic-act-no-10175/>.

²⁷ “Author of Cybercrime Law to File Bill Amending It,” *Rappler*, October 3, 2012, <http://www.rappler.com/nation/13545-author-of-cybercrime-law-to-file-bill-amending-it>.

²⁸ Mark D. Merueñas, “SC Junks 16th Petition vs. Cybercrime Law,” January 24, 2013, <http://www.gmanetwork.com/news/story/291825/scitech/technology/sc-junks-16th-petition-vs-cybercrime-law>.

²⁹ Edu Punay, “SC Extends TRO on Cyber Law,” *Philippine Star*, February 6, 2013, <http://www.philstar.com/headlines/2013/02/06/905368/sc-extends-tro-cyber-law>.

³⁰ “Senate Bill No. 3327,” Senate of the Philippines, accessed July, 2013, <http://www.senate.gov.ph/lisdata/1446312119!.pdf>.

³¹ Norman Bordadora, “Santiago Proposes Magna Carta for Internet,” *Inquirer*, December 1, 2012, <http://technology.inquirer.net/20769/santiago-proposes-magna-carta-for-internet#ixzz2RJNaXMVZ>.

³² “Republic Act No. 9775,” November 17, 2009, The LawPhil Project, http://www.lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html.

There have been no reports of officials putting pressure on online journalists or bloggers to delete content when it is critical of the authorities. However, many news websites are online versions of traditional media which self-censor due to the level of violence against journalists in the Philippines. While it is fair to surmise that the same attitude is reflected in their online output, the degree is difficult to establish. Notably, however, one of the Senate's main proponents of the libel clause in the Anti-Cybercrime Act argued that it would instill self-censorship in internet users—the actual phrase was “think before you click,” according to local blogger Raïssa Robles.³³

More generally, the Philippine blogosphere is rich and thriving. Both state and non-state actors actively use the internet as a platform to discuss politics, especially during elections. Online protests against the Cybercrime Prevention Act were common for several months before and after the law was passed, with individuals blacking out their profile pictures on social networks. Many dubbed it Cyber Martial Law after the era of military rule in the 1970s when freedom of expression was seriously threatened.³⁴ While encouraging, these protests can only be called successful inasmuch as they spurred the filing of the 15 petitions with the Supreme Court, which are to be credited with ultimately suspending the law's implementation.

VIOLATIONS OF USER RIGHTS

The Cybercrime Prevention Act, which passed in 2012 after more than a decade of deliberations,³⁵ uncritically adopted archaic libel provisions from the penal code—long challenged by local and international human rights groups³⁶—and increased the minimum penalty for online violations from six months to a staggering six years in jail, apparently at the last minute and without public discussion.³⁷ Other provisions require service providers to cooperate with law enforcement in monitoring users suspected of cybercrime, and potentially allow police to monitor online traffic in real time. Despite the Supreme Court's restraining order on the law's implementation, it has already created a chilling effect among internet users. Violence against traditional journalists exerts a negative effect on freedom of expression in the Philippines, but as of 2013, had relatively little impact on online communication.³⁸

³³ Raïssa Robles, “Who Inserted that Libel Clause in the Cybercrime Law at the Last Minute?,” *RaïssaRobles*, September 18, 2012, <http://raissarobles.com/2012/09/18/who-inserted-that-libel-clause-in-the-cybercrime-law-at-the-last-minute/>.

³⁴ T.J.D., “Protests Versus Cybercrime Law Rage on Multiple Fronts,” October 2, 2012, *GMA News*, <http://www.gmanetwork.com/news/story/276448/scitech/technology/protests-vs-cybercrime-law-rage-on-multiple-fronts>.

³⁵ “The Road to the Cybercrime Prevention Act of 2012,” *Rappler*, October 9, 2012, <http://www.rappler.com/rich-media/13901-the-road-to-the-cybercrime-prevention-act-of-2012>.

³⁶ Human Rights Watch, “Philippines: New ‘Cybercrime’ Law Will Harm Free Speech,” September 28, 2012, <http://www.hrw.org/news/2012/09/28/philippines-new-cybercrime-law-will-harm-free-speech>.

³⁷ Jillian C. York, “Philippines' New Cybercrime Prevention Act Troubling for Free Expression,” Electronic Freedom Foundation, September 18, 2012, <https://www.eff.org/deeplinks/2012/09/philippines-new-cybercrime-prevention-act-troubling-free-expression>.

³⁸ Article 19, “Philippines: ARTICLE 19's Submission to the UN Universal Periodic Review,” November 29, 2011, <http://www.article19.org/resources.php/resource/2879/en/philippines:-article-19%27s-submission-to-the-un-universal-periodic-review>.

The Bill of Rights of the 1987 Constitution protects freedom of expression (Section 4) and privacy of communication (Section 1).³⁹ However, some laws undermine those protections. Libel is punishable by fines and imprisonment under the Revised Penal Code. This has historically been challenging to prove in online cases which lack a physical place of publication—one of the requirements for an offline prosecution—and in 2007, a Department of Justice resolution established that Articles 353 and 360 of the Revised Penal Code covering libel do not apply to statements posted on websites.⁴⁰ This may have discouraged, but did not stop, attempts to prosecute online libel. In 2011, a doctor filed a complaint over an allegedly defamatory statement about him posted in the comments section of their website. In January 2013, the prosecutor dismissed the complaint against the website staffers on the basis that they are not responsible for content they neither edited nor approved. However, charges are still pending against the third respondent who left the comment.⁴¹

The 2012 cybercrime law not only adopted the penal code's definition of libel, but further classified it as a cybercrime punishable by six to twelve years in prison or a fine determined by the Department of Justice. The identical offense perpetrated offline carries a lesser sentence of six months to four years and two months imprisonment under the Revised Penal Code.⁴² A government lawyer warned that liking or sharing a libelous post on Facebook or Twitter could result in imprisonment.⁴³ Others pointed out that the law could imprison the living for libeling the dead, and that the author of alleged libel could be sued for something written years before the law was passed if the content is still available online.⁴⁴ One lawyer reposted content that had sparked a libel suit against him in 2010 to his Facebook page in an attempt to create the kind of judicial controversy that would spur the Supreme Court to intervene over the law.⁴⁵

While the legal challenges to the law have left its future in doubt, a private citizen used it to sue a neighbor for uploading a video to YouTube under an allegedly libelous title in October 2012; the preliminary investigation into the complaint was suspended due to the restraining order issued by

³⁹ "1987 Philippine Constitution, Article III, Bill of Rights," via Asian Human Rights Commission, accessed July 2013, http://philippines.ahrchk.net/news/mainfile.php/leg_sel/15/.

⁴⁰ Department of Justice, Resolution No. 05-1-11895 on *Malayan Insurance vs. Philip Piccio, et al.*, June 20, 2007. Article 353 states that, "libel is committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means." The Department also stated that the accused are not culpable because they cannot be considered as authors, editors, or publishers as provided for in Article 360. Critics have further noted that the Revised Penal Code, which dates from 1932, long predates digital technology, and therefore shouldn't be applied to digital content.

⁴¹ Rene Acosta, "Prosecutor Drops Libel Complaint vs TV Network," January 6, 2013, *Business Mirror*, <http://www.businessmirror.com.ph/index.php/news/nation/7273-prosecutor-drops-libel-complaint-vs-tv-network>

⁴² Purple Romero, "DOJ Holds Dialogue on 'E-Martial Law'," October 9, 2012, Rappler, <http://www.rappler.com/nation/13837-it-s-not-e-martial-law>.

⁴³ "SolGen: Netizens Spreading 'Libelous' Posts Criminally Liable," January 29, 2013, *SunStar*, <http://www.sunstar.com.ph/breaking-news/2013/01/29/solgen-netizens-spreading-libelous-posts-criminally-liable-265420>.

⁴⁴ "Digital Martial Law: 10 Scary Things About the Cybercrime Prevention Act of 2012," *Spot*, October 2, 2012, <http://www.spot.ph/newsfeatures/52041/digital-martial-law-10-scary-things-about-the-cybercrime-prevention-act-of-2012/1#sthash.4vVhXXNS.dpuf>.

⁴⁵ Mark Merueñas, "Lawyer Wants Test Case on Cybercrime Law," *GMA News*, October 3, 2012, <http://www.gmanetwork.com/news/story/276548/news/nation/lawyer-wants-test-case-on-cybercrime-law>.

the Supreme Court against the cybercrime law.⁴⁶ Another prominent case did not involve a criminal prosecution. In 2012, a group of nurses said their hospital had fired them for ‘liking’ a Facebook post criticizing the management.⁴⁷ Though the state-run hospital denied Facebook was a factor in the termination, the case evoked the same fear—of authorities taking arbitrary action over ICT content—as the anti-cybercrime law itself.

The cybercrime act would also facilitate government surveillance of online communication, allowing the authorities to monitor online activities, and requiring service providers to assist the government in collecting and storing user data pertaining to acts classified as cybercrimes, including spam and file-sharing.⁴⁸ The extent to which they already conduct surveillance is not clear. The government acted on Section 10 of the law to create an anti-cybercrime group within the Philippine police force in March 2013.⁴⁹ It is not known whether the team has begun collecting real-time traffic data based on the law’s contested section 12.⁵⁰

A Data Privacy Act introduced into law on August 15, 2012 establishes parameters for the collection of personal information and an independent privacy regulator, but only pertaining to data voluntarily provided in private or official transactions, such as credit card information or social security details.⁵¹ While many clauses are ICT-specific, requiring those who control information online to take steps such as assessing reasonably foreseeable vulnerabilities in computer networks, it does not redress the provisions in the Cybercrime Prevention Act that would allow monitoring or collection of personal data in criminal cases with neither the user nor the court’s consent.⁵²

Other laws with privacy implications include the Anti-Child Pornography Act of 2009 which explicitly states that its section on ISPs may not be “construed to require an ISP to engage in the monitoring of any user,”⁵³ though it does require them to “obtain” and “preserve” evidence of violations, and threatens to revoke their license for non-compliance; section 12 of the law also authorizes local government units to monitor and regulate commercial establishments that provide internet services. Under the Human Security Act of 2007, law enforcement officials must obtain a

⁴⁶ Tricia Aquino, “Cebu Resident Subpoenaed Over ‘Cyber-Libelous’ YouTube Post”, October 27, 2012, *InterAksyon*, <http://www.interaksyon.com/article/46643/cebu-resident-subpoenaed-over-cyber-libelous-youtube-post>.

⁴⁷ Matika Santos, “Audio Recording Bares Nurses Fired Over Facebook ‘Like’ on Critical Status Update,” *Inquirer*, October 10, 2012, <http://technology.inquirer.net/18744/audio-recording-bares-nurses-fired-over-facebook-like-on-critical-status-update>.

⁴⁸ Paul Tassi, “The Philippines Passes a Cybercrime Prevention Act that Makes SOPA Look Reasonable,” *Forbes*, October 2, 2012, <http://www.forbes.com/sites/insertcoin/2012/10/02/the-philippines-passes-the-cybercrime-prevention-act-that-makes-sopa-look-reasonable/>.

⁴⁹ Official Homepage of the Philippine National Police, “PNP Activates Anti-Cybercrime Group,” press release, March 21, 2013, <http://pnp.gov.ph/portal/press-news-releases/latest-news/969-pnp-activates-anti-cybercrime-group>.

⁵⁰ Tetch Torres, “Gov’t Admits Cyberlaw Barely Constitutional,” January 29, 2013, *Inquirer*, <http://newsinfo.inquirer.net/349173/govt-admits-cyber-law-barely-constitutional>.

⁵¹ “Republic Act No. 10173,” Official Gazette, August 15, 2012, <http://www.gov.ph/2012/08/15/republic-act-no-10173/>; Janette Toral, “Salient features of Data Privacy Act of 2012 – Republic Act 10173,” *Digital Filipino*, December 17, 2012, <http://digitalfilipino.com/salient-features-of-data-privacy-act-of-2012-republic-act-10173/>.

⁵² Alec Christie and Arthur Cheuk, “Australia: New Tough Privacy Regime in the Philippines Data Privacy Act Signed Into Law,” DLA Piper Australia via *Mondaq*, October 27, 2012, <http://www.mondaq.com/australia/x/203136/Data+Protection+Privacy/privacy+law+Philippines>.

⁵³ “Implementing Rules and Regulations of the Anti-Child Pornography Act of 2009,” via University of Minnesota Human Rights Library, accessed July 2013, <http://www1.umn.edu/humanrts/research/Philippines/IRR%20of%20the%20Anti%20Child%20Pornography%20Act.pdf>.

court order to intercept communications or conduct surveillance activities against individuals or organizations suspected of terrorist activity.⁵⁴ To date, no abuse of this law has been reported. Other bills pending in Congress as of March 2013 would potentially add to privacy concerns by requiring ISPs, web-hosts, and educational institutions to monitor users trying to access child pornography, gambling sites, or performing illegal hacking.⁵⁵

Violence against journalists is a significant problem in the Philippines. As of April 30, 2013, the Committee to Protect Journalists reported at least 73 Philippine journalists had been killed in relation to their work—most covering political beats—since the organization started compiling records in 1992.⁵⁶ Not one of these murders has been fully prosecuted—meaning that everyone responsible for both ordering and executing the killing have been tried and convicted—creating an entrenched culture of impunity that sends the message that individuals exercising free speech can be attacked at will. This trend has yet to make itself felt among internet users: There have been no prominent cases reported of attacks on bloggers for online expression, though some fear that may change as internet penetration grows and more people turn to web-based news sources.

There are no restrictions on anonymous communication in the Philippines. The government does not require the registration of user information prior to logging online or subscribing to internet and mobile phone services, especially since prepaid services are widely available, even in small neighborhood stores.

There have been no reports of politically-motivated incidents of technical violence or cyberattacks perpetrated by the government towards private individuals. However, in October 2012, the Philippine chapter of the group Anonymous perpetrated a series of cyberattacks against government- and privately-owned websites.⁵⁷

⁵⁴ “Republic Act 9372 – Human Security Act of 2011 (full text),” Philippine e-Legal Forum, July 10, 2007, <http://jlp-law.com/blog/ra-9327-human-security-act-of-2007-full-text/>

⁵⁵ For example, “SBN-1710: Safer Net Act,” Senate of the Philippines, accessed July, 2013, http://www.senate.gov.ph/lis/bill_res.aspx?congress=15&q=SBN-1710.

⁵⁶ The organization documented an additional 37 journalist murders in which the motive was not confirmed. Committee to Protect Journalists, “73 Journalists Murdered in Philippines since 1992,” accessed May 2013, <http://cpj.org/killed/asia/philippines/>.

⁵⁷ Camille Diola, “‘Anonymous Philippines’ Hacks Gov’t Websites Anew,” *Philippine Star*, January 15, 2013, <http://www.philstar.com/cybercrime-law/2013/1/15/897221/anonymous-philippines-hacks-gov-t-websites-anew>.