PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill

*Furqan Mohammed**

On December 16, 2014, Taliban militants stormed an elementary school in Peshawar, Pakistan and murdered nearly 150 students and teachers.[1] This tragedy was a wake-up call for the Pakistani people—it shifted public opinion from one of indifference to a realization of the threat of harboring extremism.[2] Shortly after the attack, Pakistan created a "National Action Plan" consisting of 20 action items the country would implement to eradicate extremism.[3] Pakistani officials emphasized that the country must enact laws that granted an unfettered ability to monitor, locate, and prosecute alleged militants.[4]

* Associate, Perkins Coie LLP. The views and opinions expressed herein are those of the author and do not necessarily reflect the views of Perkins Coie, its affiliates, or its clients. I would like to first thank Furqaan Siddiqui, Aisha Sleiman, and the entire JINEL staff for editing multiple drafts of this article. I would also like to thank Farieha Aziz and Sana Saleem from Bolo Bhi (a non-profit in Pakistan) for their expert insight on cybercrime and for forwarding relevant articles for my review. Finally, I would be remiss if I did not recognize the efforts of Brian Davies, support staff at Perkins Coie, for his technical and editorial support.

1. Ashfaq Yusufzai, *Pupils Return to Pakistani School Where Taliban Killed 150*, The Telegraph, Jan. 12, 2015, *available at* http://www.telegraph.co.uk/news/worldnews/asia/pakistan/11339184/Pupils-return-to-Pakistani-school-where-Taliban-killed-150.html. The Taliban, which took responsibility for the attack, explained that particular school was chosen because it was attended primarily by children of Pakistani army members. Sara C. Nelson, *Peshawar Attack: Tragic List of Children Killed in School Massacre Emerges*, Huffington Post, (Dec. 16, 2014), http://www.huffingtonpost.co.uk/2014/12/16/peshawar-attack-tragic-list-children-killed-school-massacre-emerges_n_6333210.html.
2. Kamran Haider, *Shifting Attitudes put Pakistan's Islamic Extremists on Defense*, Hindustan Times − Mint (E-Paper), (Feb. 18, 2015), http://www.livemint.com/Politics/9R8ZZkKeSgiya9cwhRiygI/Shifting-attitudes-put-Pakistans-Islamic-extremists-on-defe.html ("An opinion poll conducted in January [2015] by Gallup Pakistan found that 52% of respondents saw the Taliban as a greater threat than neighbouring India. That contrasts with a Pew Research Center survey released last year in which respondents picked India as the nation's primary security threat by a margin of two to one over the Taliban.").
3. Anup Kaphle, *Pakistan Announces a National Plan to Fight Terrorism, Says Terrorists' Days are Numbered*, The Washington Post, (Dec. 24, 2014), https://www.washingtonpost.com/news/worldviews/wp/2014/12/24/pakistan-announces-a-national-plan-to-fight-terrorism-says-terrorists-days-are-numbered/. Among other things, Prime Minister Nawaz Sharif has said that he would set up a "rapid response force" in an effort to root terrorists out of the country. *Id*. One of the more notable action items was the creation of special terrorists courts designed to deal with militants. *See id*. Several reports have noted the problems with civilian courts' ability to dispense justice against militants: judges were openly threatened, and in many cases, fled in response to the death threats, and lawyers had been killed for prosecuting extremists. Shamil Shams, *Pakistan's Military Courts - a Solution or a Problem?*, Deutsche Welle (DW), (Aug. 7, 2015), http://www.dw.com/en/pakistans-military-courts-a-solution-or-a-problem/a-18633959.
4. *See, e.g*., Jamal Shahid, *'Flawed' Cybercrime Bill Approved*, Dawn News, (Apr. 17, 2015), http://www.dawn.com/news/1176440. For example, Tahir Iqbal, a leading political figure in the majority

While the intent to swiftly eradicate extremism is admirable, this desire for unfettered access has permeated beyond the National Action Plan to other laws under debate that directly affect Pakistan's general populace. The Prevention of Electronic Crimes Act of 2015 (hereinafter "PECA 2015" or "Bill") is one notable example. Broadly speaking, PECA 2015 would define the various types of cybercrimes and provide a means for prosecuting the same. The Bill started on the right track: it was negotiated over 18 months (starting in early 2013) and incorporated consultation from cybercrime experts, industry professionals and privacy groups.[5] The negotiations paid off; the proposed draft was 44 pages long and included privacy safeguards for citizens' rights.[6] This draft (hereinafter "Stakeholder Draft") was then presented to the National Assembly's Standing Committee on Information Technology ("Standing Committee") in late 2014.[7] If the Standing Committee approved, it could present it to the entire National Assembly for review and ratification.[8]

In the aftermath of the Peshawar attack—and consistent with the aforementioned desire for unfettered power to monitor alleged terrorists—the Standing Committee reduced the Stakeholder Draft from 44 pages to 13 pages by removing the privacy safeguards, and then added provisions that made the Bill overbroad and subject to misuse.[9] This version of the Bill (hereinafter "Draft") was then approved by the Standing Committee and is now awaiting decision by the entire National Assembly.[10]

Pakistan Muslim League-N, argued that "[t]he situation in the country demands immediate action to fight terrorism. Law enforcement agencies do not have time to get warrants and let terrorists win. This is the only way to save society." *Id*.

5. Talal Gondal, *the Final Frontier*, the Nation PK, (July 29, 2015), http://nation.com.pk/columns/29-Jul-2015/the-final-frontier ("In the case of the cybercrime bill, the process has gone in the opposite direction. The previous version of the Pakistan Electronic Cybercrimes bill was drafted in 2014 with the help of Barrister Zahid Jamil, who has expertise in drafting cybercrime laws—he has previously done so for the EU and the Commonwealth and the bill was prepared over an extensive period of negotiations between stakeholders, the IT ministry and security agencies. . . .").
6. *Id*. ("[the draft cybercrime bill was] a 44 page document [and] was described as a 'strong, well-thought-out and well-researched bill that rightfully protected citizens from the malicious use of the internet, while preserving their freedom of expression with certain limitations necessary for safeguarding national interests' by civil society members and rights groups.").
7. Gondal, *supra* note 5. Prior to being sent to the Standing Committee, it was also approved by a Cabinet Division on IT with minimal changes.
8. Asad Hashmi, *Surveilling and Censoring the Internet in Pakistan*, Al Jazeera English, (May 13, 2015), http://www.aljazeera.com/indepth/features/2015/05/pakistan-internet-censorship-150506124129138.html.
9. *See id*. (noting reduction in page length); *see also* Irfan Haider, *Terrorists Operating 3,000 Websites to Propagate Agenda in Pakistan*, Dawn News, (Aug. 14, 2015), http://www.dawn.com/news/1200276 (noting draft bill was reduced from 44 pages to 13 pages and that it omitted provisions aimed at safeguarding human rights). One of the most problematic additions to the draft bill was Section 34, which allowed the blocking of websites if it was "necessary in the interest of the glory of Islam" or on various other subjective bases. *See* Gondal, *supra* note 5 (noting concern with Section 34).
10. Shahid, *supra* note 4 (noting the draft bill had been approved by the Standing Committee on April 16, 2015); *see also* Jahanzib Haque, *Analysis: The Dangers of Fighting Terror with a Cybercrime Bill*, Dawn News, (Sept. 12, 2015), http://www.dawn.com/news/1206465 (Muhammad Aftab Alam, a lawyer and expert on media law in Pakistan, noted that "even if the [National Assembly] approves it, once the bill reaches Senate, it may be stopped by [minority] political parties. . . .").

Unless it is referred back to the Standing Committee, this Draft will become the new cybercrime law in Pakistan.[11]

This Article argues that the Draft should be rejected by the National Assembly. It is a step backwards for a country that has otherwise been applauded in recent years for democratic progress.[12] The primary concern with the Draft is that it is subject to misuse in the following ways: (1) there is no mandate to obtain a warrant, thereby granting the agency unchecked power to access or block content or make arrests; (2) it potentially criminalizes journalism; (3) it empowers the agency to remove content based on various subjective bases; and (4) it defines cyber terrorism broadly and therefore may be applied to non-terrorism cases to impose harsher punishments. The author recommends the Senate encourage the Standing Committee to utilize the Stakeholder Draft with one modification that would prevent overbroad application.

Part II provides a brief history of the cybercrime ordinances passed in Pakistan and the government's history of blocking content under those ordinances. Part II then describes the Peshawar school attacks and the National Action Plan. Part II finally discusses the legislative history of PECA 2015. Part III highlights the problematic sections in the Draft and why they should be removed. Part IV recommends that the National Assembly reject this Draft and encourage the Standing Committee to adopt the Stakeholder Draft with one modification. Part V concludes.

I. Background
The PECO Ordinances of 2007 and 2009

Pervez Musharraf was appointed Chief of Army Staff in 1998.[13] He led a bloodless coup in October 1999 and declared martial law thereafter.[14] In 2001, he appointed himself president, and in 2002, he held an emergency national referendum

11. Even if it passes into law, however, the bill can be challenged in the Supreme Court of Pakistan. *See id.* ("Babar Sattar, an Islamabad-based lawyer, noted '[c]onsensus will have to be developed in the senate in order for the bill to be passed...and even if it passes, the courts can take judicial review of laws to the extent that any provision can be struck down if it is in breach of the Constitution. If the law is overbroad and infringes on fundamental rights, any individual can provide evidence to begin the process of judicial review.'").
12. For example, Pakistan was applauded in recent years because, for the first time in Pakistan's nearly 70-year history, the country made a peaceful transition from one democratically elected government to another. *See* Tim Craig, *Nawaz Sharif is Formally Elected Prime Minister of Pakistan*, The Washington Post, (June 5, 2013), https://www.washingtonpost.com/world/asia_pacific/nawaz-sharif-formally-elected-prime-minister-of-pakistan/2013/06/05/2d1a1fee-cdd0-11e2-8f6b-67f40e176f03_story.html. In most other instances, Pakistan has endured hostile takeovers by military leaders who would subsequently impose martial law until another government could be elected. *See generally* Furqan Mohammed, *Exploring Power Politics and Constitutional Subversions in Pakistan: a Political and Constitutional Assessment of Instability in Pakistan*, 7 Loy. U. Chi. Int'l L. Rev. 229 (2010) (providing a brief history of the instability of leadership in Pakistan).
13. Sara Louise Kras, Major World Leaders: Pervez Musharraf 50 (Chelsea House Publishers 2004).
14. *See* Hamid Khan, Constitutional and Political History of Pakistan 486 (Oxford University Press 2001) (2005).

vote in which he was the sole candidate for president.[15] He was elected president for a period of five years.[16] Musharraf was reelected in 2007 for another five years.[17]

In December 2007, shortly after being elected to his second term, Musharraf introduced the Prevention of Electronic Crimes Ordinance ("PECO 2007").[18] By passing this law as an ordinance (as opposed to a law), Musharraf did not need parliamentary approval.[19] A president could pass any ordinance that would then be valid for 120 days.[20] At the end of the 120 days, a president could either seek parliamentary approval, or pass another ordinance to the same effect.[21]

PECO 2007 was a law the government could use to prosecute cybercrime.[22] Broadly speaking, PECO 2007 penalized criminal access, misuse of, or damage to electronic data and systems.[23] The government argued PECO 2007 was promulgated to increase security for the IT industry.[24] Critics, however, believed it was to silence Musharraf's opposition and halt satire about him on the internet.[25] There was also concern the law would be used to crack down on free expression because it prohibit-

15. *Id.* at 495.
16. *Id*.
17. Raja Asghar, *Musharraf Steals the Show, but Victory Hangs on Court*, Dawn News, (Oct. 7, 2007), http://www.dawn.com/news/270135/musharraf-steals-the-show-but-victory-hangs-on-court (noting that the Supreme Court of Pakistan had to decide whether challenges to Musharraf's candidacy for president were legitimate). Musharraf would only remain in office until 2008, when he resigned in the face of possible impeachment trials. *See generally* Note, *The Pakistani Lawyers' Movement and the Popular Currency of Judicial Power*, 123 Harv. L. Rev. 1705, 1710-1716 (2010) (providing history of Lawyers' Movement in Pakistan that ultimately led to Musharraf's resignation).
18. Osman Husain, *Is the New Cyber-Crime Bill Akin to Banning the Internet in Pakistan?*, The Express Trib. Blogs, (Apr. 20, 2015), http://blogs.tribune.com.pk/story/27245/is-the-new-cyber-crime-bill-akin-to-banning-the-internet-in-pakistan/. Musharraf had gained a reputation as someone who would keep a close watch on the media even before passing PECO 2007 because he wanted to ensure it would not challenge his power. For example, upon declaring a state of emergency in 2007 (before the elections), Musharraf amended the Pakistan Electronic Media Regulation Authority's (PEMRA) (the agency overseeing broadcast and media) charter to prohibit any programming that ridiculed the heads of state or members of the armed forces. *See* Open Net Initiative, *Pakistan 2010 Report*, https://opennet.net/sites/opennet.net/files/ONI_Pakistan_2010.pdf. Critics further argued that Musharraf had originally established PEMRA in 2002 to regulate private electronic media and that the regulatory framework it established was aimed at supporting Musharraf's "drive to control and restrict independent journalism." *Id*.
19. *See, e.g.*, Awab Alvi, *Pakistan: Funny SMS's may Land Pakistanis in for a Fourteen Year Prison Sentence*, Global Voice Advocates, (Aug. 2, 2009), https://advox.globalvoices.org/2009/08/02/pakistan-funny-smss-may-land-pakistanis-in-for-a-14-year-prison-sentence/.
20. *Id*.
21. *Id*.
22. *See* Syed Abbas Ahsan, *Current Situation and Issues of Illegal and Harmful Activities in the Field of Information and Communication Technology in Pakistan*, United Nations Asia and Far East Inst. (140th International Training Course Participants' Papers, 2009), http://www.unafei.or.jp/english/pdf/RS_No79/No79_11PA_Ahsan.pdf.
23. *Id*.
24. Irfan Khan, *New Cyber Law in Pakistan Restricts Free Speech*, OneWorld South Asia, (Jan. 24, 2008), http://southasia.oneworld.net/archive/Article/new-cyber-law-in-pakistan-restricts-free-speech#.VnSUJPkrLRZ.
25. Maham Javaid, *a World Without Law*, Herald Dawn, (Mar. 19, 2015), http://herald.dawn.com/news/1152775.

ed the use of internet and cell phones to criticize authorities or organize rallies.[26] The broad definition of cyber stalking—including taking pictures of any person without consent—was also seen as an attempt to illegalize journalism.[27] In sum, PECO 2007 was used to block several hundred anti-government blogs under the guise of "national security."[28]

PECO 2007 authorized the Federal Investigation Agency (FIA) to investigate alleged violations.[29] But the FIA has a reputation of silencing critics of high-level politicians.[30] For example, in October 2008, the FIA stated that it would hunt down the "antidemocratic" forces circulating YouTube videos and text messages aimed at discrediting the majority party's politicians.[31]

When PECO 2007 lapsed (after receiving three extensions)—and because it could never secure parliamentary approval—a new ordinance was promulgated in July 2009 by then-President Asif Ali Zardari.[32] This ordinance was known as the Pre-

26. Irfan Ahmed, *Media-Pakistan: Cybercrime Law Infringes on Rights*, Inter Press Service News Agency, (Jan. 23, 2008), http://www.ipsnews.net/2008/01/media-pakistan-cybercrime-law-infringes-on-rights-activists/. In a statement, the South Asian Free Media Association said that "against the backdrop of the use of internet and cell phones to criticize authorities to send calls for rallies, the ordinance is liable to be interpreted as a drastic measure aimed at putting curbs on civil rights." *Id*. In August 2008, the civil society organization Pakistan ICT Policy Monitors Network announced that six URLs were blocked upon the request of retired Admiral Afzal Tahir, accused in a number of YouTube videos of abusing his office in a personal land dispute. Open Net Initiative, *supra* note 18, at 492.
27. Open Net Initiative, *supra* note 18, at 492 ("Media rights advocates expressed concern that the prohibition against taking or distributing photographs of a person without consent made one of the major components of citizen journalism illegal.").
28. *Id*. at 495.
29. *Id*. at 492. The National Response Centre for Cyber Crime would also provide technical assistance, a reporting center, and spearhead awareness campaigns. *Id*.
30. *Id*. at 493.
31. *Id*.; *see also* Fatima Bhutto, *Online Crimes*, The Guardian, (Feb. 11, 2009), http://www.theguardian.com/commentisfree/2009/feb/10/pakistan-cyber-terrorism-law. A pro-government journalist argued that PECO 2007 was about security, not censorship, and that "Pakistan currently enjoys probably the freest and fiercely independent media in the world where every newspaper and TV channel is free to print and air what they want to." *See* Syeda Sultana Rizvi, *This is not Censorship. It's Security*, The Guardian, (Feb. 24. 2009), http://www.theguardian.com/commentisfree/2009/feb/24/pakistan-terrorism. Pakistan does not have the "freest and fiercely independent media in the world" by any objective measure. Although net neutrality statistics were not found for 2009, Freedom House, a non-profit reporting on net neutrality reported that Pakistan's "freedom on the net status" in 2011 was only "partly free." *See* Freedom House, *Pakistan 2011*, https://freedomhouse.org/report/freedom-net/2011/pakistan. (noting anti-military, blasphemous, or anti-state content was routinely blocked). Pakistan's net neutrality has since been downgraded to "not free." *See* also Freedom House, Pakistan 2011, https://freedomhouse.org/report/freedom-net/2015/pakistan. Pakistan has also been reported as one of the 10 worst countries in regards to internet freedom across the world. *See* Sajjad Haider & Yumna Rafi, *Pakistan Among 10 Worst Countries on Internet Freedom Index*, Dawn News, (Sept. 6, 2015), http://www.dawn.com/news/1148783; *see also* Ahsan Kureshi, *Bounded Freedom*, The Nation, (July 1, 2015), http://nation.com.pk/columns/01-Jul-2015/bounded-freedom (noting that Pakistan ranks 159 out of 180 countries in press freedom).
32. *Placing Lapsed Ordinance in Senate: Law Ministry Apologises to Committee*, Dawn News, (June 23, 2010), http://www.dawn.com/news/850187/placing-lapsed-ordinance-in-senate-law-ministry-apologises-to-committee. The ordinances were first passed in December 2007, and then re-promulgated in May 2008, February 2009 and July 2009. *See* Fazal Sher, *Prevention of Electronic Crimes Bill:*

vention of Electronic Crimes Ordinance of 2009 ("PECO 2009").[33] PECO 2009 was identical to PECO 2007 and thus raised the same concerns.[34] It lapsed in November 2009 for failure to secure parliamentary approval.[35] Pakistan thereafter had no law to effectively prosecute cybercrimes.[36]

NA Body Seeks Recommendations, Business Recorder, (June 30, 2012), http://www.brecorder.com/top-news/108/64900-prevention-of-electronic-crimes-bill-na-body-seeks-recommendations-.html.

33. Alvi, *supra* note 19.
34. *Id*. PECO 2009 also resulted in much criticism. For example, bloggers stressed that the vague definitions of the crimes listed, including "spoofing" and "spamming," were inherently vague acts and this lack of certainty would result in the government using those terms to prevent publications critical of the state. *See* Carrie Tian and Zachary Popp, *Cyberspace in Court: Around the World: Pakistan*, Harvard Law School Blog, (Dec. 10, 2011), http://blogs.law.harvard.edu/aroundtheworld/#_ftn7; *see also* Bhutto, *supra* note 31 (noting that the definitions of "spoofing," "spamming," or the "character assassination" of any member of state could result in prison sentences. Furthermore, writing articles critical of Pakistan's role in the war on terror or questioning the corruption of the state could constitute "spoofing.").
35. Alvi, *supra* note 19. It is unclear why Zardari and his predecessor did not re-promulgate PECO 2009 as an ordinance in November 2009 when it lapsed.
36. Azam Khan, *NA Session on Cybercrime Bill 2015 Postponed Till Next Week*, The Express Tribune, (Apr. 24, 2015), http://tribune.com.pk/story/875246/na-session-on-cybercrime-bill-2015-postponed-till-next-week/ (noting that both PECO 2007 and PECO 2009 had failed to secure parliamentary approval). After the lapse, the government went back to utilizing the Electronic Transactions Ordinance of 2002 ("ETO 2002") to prosecute crimes. *See* Jahanzaib Haque, *Open Democratic Initiative: Developing a Progressive Internet Policy for Pakistan*, Jinnah Inst. Policy Brief, (Jan. 30, 2015), http://jinnah-institute.org/wp-content/uploads/2015/01/Internet-Policy-Brief.pdf. The ETO 2002 was the first IT-relevant legislation passed by Pakistan. *See* Omair Zeeshan, *Investigators Suffering from Absence of Law*, The Express Tribune, (Mar. 24, 2011), http://tribune.com.pk/story/136794/investigators-suffering-from-absence-of-law/. Sections 36 and 37 were the most relevant to cybercrime. *Id*. Section 36 of the ETO 2002, titled "violation of privacy information," prohibited a person who "gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature of contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance. . . ." Electronic Transactions Ordinance, § 36 (2002), *available at* http://www.pakistanlaw.com/eto.pdf. Section 37, titled "Damage to information system," prohibited any person who (1) "does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorised to do any of the foregoing, shall be guilty. . ." or (2) "does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty. . . ." *Id*. § 37. The government likely had difficulty fitting cybercrimes into one of these sections and therefore wished to pass a new cybercrime bill. *See* Zeeshan, *supra* note 36 (an official from the FIA noted that "we had been dealing with corporate sector crimes, financial fraud, email phishing and other similar attacks through electronic medium, but these are now up for grabs and we are unable to do anything," and further noting that "[t]his is similar to cutting off our right hand and leaving us to deal with cybercrime in a paralysed state."). The ETO was also problematic because it was not significant for courts; offenses brought under the ETO were therefore given low priority due to the overburdened judicial system. *Id*.

The Peshawar School Terrorist Attacks and the Implementation of the National Action Plan

The event that swayed politicians to consider an overbroad cybercrime bill was the Peshawar school terrorist attack. On December 16, 2014, six Pakistani Taliban members stormed a school in Peshawar and opened fire at school children and teachers in retaliation for the Pakistan army's ongoing operative against the Taliban.[37] By the time the attack was quelled, nearly 150 children and teachers had been killed, and over 100 had been injured.[38] This was the worst attack in Pakistan's history and was labeled barbaric across political lines.[39]

In response to that attack, the Pakistani government passed the National Action Plan ("Plan") in January 2015.[40] The Plan was seen as a necessary step to eradicate extremism.[41] The Plan consisted of 20 action items to eradicate extremism, including the creation of military courts to try terror suspects, a new counter-terrorism unit in the army, and other measures to halt the operations of extremist organizations.[42]

37. *See, e.g.*, Omar Waraich, *Peshawar School Attack: Will the Most Horrific Attack in Pakistan's Recent History Finally Unite Its Squabbling Politicians?*, The Independent, (Dec. 16, 2014), http://www.independent.co.uk/voices/comment/peshawar-school-attack-will-the-most-horrific-attack-in-pakistans-recent-history-finally-unite-its-9929383.html.
38. BBC News, *Pakistan Taliban: Peshawar School Attack Leaves 141 Dead*, (Dec. 16, 2014), http://www.bbc.com/news/world-asia-30491435. *See generally supra* note 1.
39. BBC News, *supra* note 38. *See generally supra* note 1.
40. Kaphle, *supra* note 3. *See generally supra* note 3.
41. Abdul Manan, *Fight Against Terrorism: Defining Moment*, The Express Tribune, (Dec. 25, 2014), http://tribune.com.pk/story/811947/fight-against-terrorism-defining-moment/. This shift in thinking was likely the result of the Peshawar school attacks. *See* Haque, *supra* note 10; *see also* Azam Khan, *supra* note 36 (noting that the cybercrime bill has a "direct link" with the National Action Plan, which was devised after the Peshawar attack); *see also* Tahir Amin, *National Assembly Body to Restructure Prevention of Electronic Crimes Bill*, Business Recorder, (Feb. 5, 2015), http://bolobhi.org/resources/timelines/tracking-cyber-crime-legislation/ ("The Standing Committee, after review of the Stakeholder Draft, unanimously agreed to modify it because the present scenario is quite different especially after the National Action Plan as certain amendments are required according to the situation.").
42. *See* Manan, *supra* note 41 (identifying 20-point National Action Plan). For example, consistent with Point 1 ("execution of convicted terrorists will continue"), Pakistan lifted its moratorium on executions, which had been in place since 2008. *See* AFP, *Death Penalty Moratorium Lifted Completely in Pakistan: Officials*, Dawn News, (Mar. 10, 2015), http://www.dawn.com/news/1168652. Supporters of the death penalty in Pakistan argued that fast-track executions were necessary to rein in militant attacks. *Pakistan Ends Death Penalty Suspension After Seven Years*, BBC News, (Mar. 10, 2015), http://www.bbc.com/news/world-asia-31812177. However, human rights activists noted Pakistan's poor track record of categorizing who should be on death row, and for reasons uncertain, Pakistan lifted the moratorium as to all persons on death row—even those on death row not tied to terrorism. In June 2015, for example, Pakistan hung Aftab Bahadur, a man convicted of a double murder when he was 15 years old primarily on the testimony of two eyewitnesses, both of whom, later retracted their statements claiming they were made under torture. *See Pakistan Executes Man Who was Minor When Convicted*, BBC News, (June 10, 2015), http://www.bbc.com/news/world-asia-33074769. It was further reported that the court even refused to grant his volunteer lawyers the few days needed to present evidence that may have proved his innocence. *Id*. In yet another example, in August 2015, Pakistan executed Shafqat Hussain, who was a minor at the time of the murder but his age had been incorrectly recorded as 23. *See* Qasim Nauman, *Pakistan Executes Shafqat Hussain Despite Appeals*, The Wall Street Journal, (Aug. 4, 2015), http://www.wsj.com/

In the aftermath of the attack, government officials argued that they needed the unfettered ability to monitor, locate, and prosecute alleged militants.[43] This desire for unfettered power then permeated to other laws that were under debate at the time.

The PECA 2015 is Passed by the Standing Committee

A cybercrime bill that would finally replace PECO 2009 was one of the laws being debated at the time of the Peshawar attack. The drafting of this bill had started in early 2013 and was being overseen by a cybercrime expert.[44] The draft was prepared over the course of over 18 months and included input from industry experts and privacy groups.[45] The end product, a 44-page draft (hereinafter "Stakeholder Draft"), was hailed as a success because it promoted the country's desire to effectively prosecute cybercrime while preserving freedom of expression.[46] It was presented to the Standing Committee for consideration and vote.[47]

In the aftermath of the Peshawar attack, however, the Standing Committee made several alterations to the Stakeholder Draft. The 44-page document was reduced to 13 pages by omitting privacy safeguards.[48] The Standing Committee also inserted several overbroad sections without input, such as a provision to remove content if necessary "in the glory of Islam."[49] When questioned about its changes, the majority party members argued that the only things deleted from the draft were

articles/pakistan-executes-shafqat-hussain-despite-appeals-1438690634. Minors could not be executed under Pakistan law. *Id*. The Wall Street Journal further reported that Mr. Hussain was forced to confess under torture. *See id*. In what seemed to be inevitably another unjust execution, Pakistan had sentenced Aasia Noreen, more commonly known as Asia Bibi, a Christian woman, to death for alleged blasphemy. *See* Rishi Iyengar, *Pakistan Stays Death Sentence of Christian Woman Convicted of Blasphemy*, Time World, July 22, 2015, *available at* http://time.com/3969035/asia-bibi-death-sentence-stayed-appeal-pakistan/. Ms. Bibi was sentenced to death in 2010 after an argument with a group of women who refused to drink the water she offered them because her status as a Christian made it "unclean." *Id*. Ms. Bibi argues that she was implicated because of a personal vendetta that the group of women had against her. *Id*. The Pakistan Supreme Court has stayed that execution, stating it would hear an appeal from Ms. Bibi. *Id*.

43. Shahid, *supra* note 4. For example, Tahir Iqbal, a leading political figure in the majority Pakistan Muslim League-N, argued that "[t]he situation in the country demands immediate action to fight terrorism. Law enforcement agencies do not have time to get warrants and let terrorists win. This is the only way to save society." *Id*.
44. Gondal, *supra* note 5 ("The previous version of the Pakistan Electronic Cybercrimes bill was drafted in 2014 with the help of Barrister Zahid Jamil, who has expertise in drafting cybercrime laws—he has previously done so for the EU and the Commonwealth. . . .").
45. *Id*. ("The previous version of the Pakistan Electronic Cybercrimes bill was . . . prepared over an extensive period of negotiations between stakeholders, the IT ministry and security agencies. . . .").
46. *Id*.
47. Zahid Gishkori, *Parliamentary Panel Passes Cybercrime Bill*, The Express Tribune, (Sept. 18, 2015), http://tribune.com.pk/story/958826/tackling-crime-or-curbing-speech-parliamentary-panel-passes-cybercrime-bill/.
48. Irfan Haider, *Terrorists Operating 3,000 Websites to Propagate Agenda in Pakistan*, Dawn News, (Aug. 14, 2015), http://www.dawn.com/news/1200276 (noting draft bill was reduced from 44 pages to 13 pages and that it omitted provisions aimed at safeguarding human rights).
49. *Id*.

irrelevant or repetitious provisions. *Id*. They coined this a "perfect legislation" and argued that the country should just trust the government to not misuse the law.[50]

As these changes were being made, persons who would likely oppose them were "frozen out" of further discussions.[51] Meetings were called with little or indirect notice with the hope that opposition members would not attend.[52] These members did not even receive a final draft of the bill before the Standing Committee's vote.[53] To pacify these members, the Standing Committee's chairman, Mohammed Safdar, stated that *he* had seen the draft (hereinafter "Draft") and that this was "sufficient" for the vote.[54]

The Draft passed the Standing Committee by a vote of 14 to 1.[55] All 14 members from the majority party voted in favor.[56] From six opposition members, one voted in opposition and five were not present.[57] The Draft is now awaiting vote before the National Assembly.[58]

50. Azam Khan, *NA Committee Approves Controversial Cyber Crime Bill*, The Express Tribune, (Apr. 16, 2015), http://tribune.com.pk/story/870919/na-committee-approves-controversial-cyber-crime-bill/ ("[Member of the majority party] Talal Chaudhry said we should trust that our institutions will not misuse this new legislation, while Major (retd) Tahir Iqbal termed the bill a perfect legislation, saying only one out 100 officers may misuse the law.").
51. Asad Hashmi, *Surveilling and Censoring the Internet in Pakistan*, Al Jazeera English, (May 13, 2015), http://www.aljazeera.com/indepth/features/2015/05/pakistan-internet-censorship-150506124129138.html (noting that "industry leaders from bodies such as ISPAK [Internet Service Providers Association of Pakistan], P@SHA [Pakistan Software Houses Association for IT] and others say they were frozen out of the drafting of the final bill, after more than a year of consultations on what should be included.").
52. Azam Khan, *Cybercrime Bill Consultation Leaves Out Stakeholders*, The Express Tribune, (Aug. 22, 2015), http://tribune.com.pk/story/942627/senate-approached-cybercrime-bill-consultation-leaves-out-stakeholders/ ("On August 5 it was through a television show that we learned a meeting of the NA's standing committee on IT had been called the next day to finalize the bill. Similarly members of opposition on the committee hardly received a day's notice for the meeting and recorded their protest at the meeting held on August 6. . . ."). Another meeting was held "at a day's notice" for August 13 to discuss the bill. *Id*.
53. Shahid, *supra* note 4 ("'I just received a copy. It's obvious the bill has been approved in haste. Nobody is willing to listen,' Mr Abidi [member of opposition party and member of Standing Committee] said, explaining how the members did not have adequate knowledge about the Internet, its technicalities and how best to address them."). Other opposition members on the Standing Committee also had complained that they had not been provided copies of the bill to review before the meeting. *Id*.
54. Jamal Shahid, *Draft Cybercrime Bill Bulldozed Through NA Body*, Dawn News (Sept. 18, 2015), http://www.dawn.com/news/1207737. Others reported that Safdar was interested in wrapping up the meeting. *Id*. He argued that "[a]bout 70 to 80 per cent recommendations have been accommodated in the bill" and that "[q]uestions can be raised later in the National Assembly." *Id*.
55. Shahid, *supra* note 4.
56. *Id*.
57. *Id*.
58. Asad Hashmi, *Surveilling and Censoring the Internet in Pakistan*, Al Jazeera News, (May 13, 2015), http://www.aljazeera.com/indepth/features/2015/05/pakistan-internet-censorship-150506124129138.html.

II. DISCUSSION

The Draft is problematic in several respects. Subpart A argues the permissive nature of search and arrest warrants in the Draft subject the Bill to misuse. Subpart B argues that the Draft potentially criminalizes journalism. Subpart C argues Section 34 of the Draft, a clause that allows for removal of content, is subjective and likely to be applied to silence political opposition. Subpart D argues the definition of cyber terrorism is overbroad and likely to be invoked in non-terrorism cases to impose longer prison sentences.

The Draft Does not Require an Officer to Obtain a Warrant

The Draft does not mandate warrants.[59] All of the sections referencing warrants contain only *permissive* language. Section 30, titled "Warrant for search or seizure," provides that a court "may" issue a warrant upon application of an officer to search a premises.[60] Section 31, titled "Warrant for disclosure of data," provides that a court "may" order a person to turn over data.[61] Section 36, titled "Real-time collection and recording of intelligence," provides that a court "may" order the collection of real-time data.[62] This language making warrants permissive is consistent with Sections 32 and 34, which outline the broad powers of the FIA to inspect, copy or seize data, and to block content in its discretion.[63] There also does not appear to be any restriction on an agent's authority to make arrests.[64] An agent may therefore choose to obtain a warrant prior to taking action, but he or she is not required to do so.[65] In light of the abuse of PECO 2007 and PECO 2009, however, a provision necessitating a warrant should be inserted to prevent abuse of PECA 2015.[66]

59. Staff Report, *PPP Demands Toothcomb Review of 'Inhumane' Cybercrime Bill*, Pakistan Daily Times, (Oct. 7, 2015), http://www.dailytimes.com.pk/national/07-Oct-2015/ppp-demands-toothcomb-review-of-inhumane-cybercrime-bill.
60. Prevention of Electronic Crimes Draft Bill, § 9 http://bolobhi.org/wp-content/uploads/2015/04/NA-Standing-Committee-Version.pdf (draft bill that was leaked by Bolo Bhi (meaning 'Speak up'), a nonprofit working in the area of gender rights, government transparency, internet access, digital security and privacy. *See* Bolo Bhi Website, About Us, http://bolobhi.org/about-us/ (last visited Dec. 19, 2015).
61. Prevention of Electronic Crimes Draft Bill, § 31, https://content.bytesforall.pk/sites/default/files/PECA2015.pdf.
62. *Id*. at § 36.
63. *Id*. at § 32.
64. *See generally* Prevention of Electronic Crimes Draft Bill.
65. Non-profit agencies and news outlets have noted this same concern in their review of the Draft. *See, e.g.*, *Pakistan: Cybercrime Bill Threatens Rights,* Human Rights Watch, (Apr. 20, 2015), https://www.hrw.org/news/2015/04/20/pakistan-cybercrime-bill-threatens-rights (the bill is abusive because it "permits government authorities access to the data of internet users without any form of judicial review process to justify that access"); Madiha Latif, *Why Pakistan's Cybercrime Bill is a Dangerous Farce*, Dawn News, (Apr. 17, 2015), http://www.dawn.com/news/1176538 (noting that warrant may exist as a formality but it need not prior to arrest or blocking of content); Staff Report, *PPP Demands Toothcomb Review of 'Inhumane' Cybercrime Bill*, Pakistan Daily Times, (Oct. 7, 2015), http://www.dailytimes.com.pk/national/07-Oct-2015/ppp-demands-toothcomb-review-of-inhumane-cybercrime-bill (noting the same).
66. *See supra* Section II.B.

The Draft Criminalizes Otherwise Proper Journalism

Sections 18 and 21 of the Draft are also problematic because they criminalize proper journalism. Section 18 criminalizes the intentional transmission of any "false intelligence, which is likely to harm or intimidate the reputation or privacy of a natural person."[67] Section 21 titled "cyber stalking," criminalizes various acts, including taking a picture and displaying it without a person's consent.[68] Both PECO 2007 and PECO 2009 were similarly criticized for their overbroad definition of cyber stalking and for their attempt to curtail journalism.[69] These provisions should be removed from PECA 2015.

Section 34 is Subject to Misuse Against Political Opposition

Section 34 is problematic because it permits blocking of content for subjective reasons. Section 34 provides that content can be blocked if the FIA considers it "necessary in the interest of the glory of Islam or the integrity, security or defen[se] of Pakistan or . . . friendly relations with foreign states, public order, decency or morality. . . ."[70] There are no definitions of what constitutes "necessity," what can be deemed against the "glory of Islam," against the "integrity, security or defen[se] of Pakistan," or against "public order, decency [and] morality."[71] No exceptions or exclusions are identified in this Section nor is there an appeals process.[72]

Section 34 is subject to misuse against political opposition and critics of the government because there are no guidelines for these bases of removal.[73] Without insight as to what can fall under the "against the glory of Islam" or other bases for removal, the Bill will be subject to misuse like PECO 2007 and PECO 2009.[74] A related concern is that it restricts content critical of the government's foreign policy under the "friendly relations" factor.[75] Criticisms of Pakistan's relationship with the United States or Saudi Arabia—two of the most commonly criticized foreign relationships

67. Prevention of Electronic Crimes Draft Bill, § 18. This Section essentially criminalizes defamation. It is unclear how one can "intimidate" the reputation or privacy of a natural person.
68. *Id*. § 21.
69. *See supra* note 27 and accompanying text.
70. Prevention of Electronic Crimes Draft Bill, § 34.
71. *See id.*
72. *See id.*
73. *See id.* The "glory of Islam" basis is further problematic because it could be used to target religious minorities (*i.e*., Christians and Ahmadi and Shia Muslims) practicing their religion. Such an outcome would not be surprising because Pakistan officials already severely misuse the country's blasphemy laws against minorities. *See* Raza Rumi, *Sabeen Mahmud, Martyr for Free Speech*, N.Y. Times, (Apr. 29, 2015), http://www.nytimes.com/2015/04/30/opinion/sabeen-mahmud-martyr-for-free-speech.html?smid=nytcore-ipad-share&smprod=nytcore-ipad&_r=0. The blasphemy laws prohibit derogatory remarks about Islam or the Prophet Muhammad (peace be upon him). *See Pakistan Blasphemy Laws: Ending the Abuse of the Blasphemy Laws*, *available at* http://www.pakistanblasphemylaw.com/?page_id=15.
74. *See supra* Section II.B.
75. *Id*.

of Pakistan—could therefore be blocked.[76] In light of PECO 2007 and PECO 2009's misuse to silence political opposition, Section 34 should be deleted.[77]

The Definition of Cyberterrorism is Overbroad and may be Invoked in Non-Terrorism Cases

The Draft's definition of cyber terrorism is also overbroad and subject to misapplication. Section 10(a) defines "cyber terrorism" as the commission of any crime that falls under Sections 6 through 9[78] with the intent to (a) "coerce, intimidate, overawe or create a sense of fear, panic or insecurity . . . in the public."[79] Violations of Section 10 result in harsher penalties than a crime committed under Sections 6 through 9 alone.[80]

Pakistan has a history of misapplying its terrorism laws. The Reprieve and Justice Project Pakistan ("Justice Project"), a non-profit that analyzes Pakistan's prison system, reviewed over 800 prisoners on death row in Pakistan who were charged as terrorists under the Anti-Terrorism Act, a law enacted in 1997 to prosecute alleged terrorists.[81] It concluded that there was no link to anything that could reasonably be defined as terrorism in over ***85 percent*** of those cases.[82]

The case of Zafer Iqbal sheds light on this misapplication. In 2003, Iqbal was arrested for fatally shooting his father over a dispute about Iqbal's inheritance.[83] The judge held that the ATA would apply because "[t]he cold-blooded murder of a father by his son is itself sufficient to create the sense of insecurity and terror in the people of the locality" to fall under the ATA's definition of terrorism.[84] Iqbal was sentenced

76. Madiha Latif, *Why Pakistan's Cybercrime Bill is a Dangerous Farce*, Dawn News, (April 17, 2015), http://www.dawn.com/news/1176538 see also http://tribune.com.pk/story/841910/pakistan-terror-wave-sparks-rare-criticism-of-saudi-arabia/ (noting that criticism of Saudi Arabia or the United States could be blocked under Section 34).
77. *See supra* Section II.B.
78. Section 6 prohibits unauthorized access to a critical infrastructure information system or data. Section 7 criminalizes unauthorized copying or transmission of critical infrastructure data. Section 8 criminalizes interference with a critical infrastructure information system or data. *See* Prevention of Electronic Crimes Draft Bill, §§ 6-9.
79. *Id*. at § 10(a).
80. *See id.* (the maximum penalty under Section 10 is 14 years imprisonment and/or a fine of up to 50 million rupees. Sections 6, 7,8 and 9 authorize prison sentences of 3, 5, 7 and 5 years, respectively and fines of 1, 5, 10 and 10 million rupees, respectively).
81. *See* Justice Project Pakistan and Reprieve, *Terror on Death Row*, at 3, Dec. 2015, http://www.jpp.org.pk/upload/Terror%20on%20Death%20Row/2014_12_15_PUB%20WEP%20Terrorism%20Report.pdf (hereinafter "Justice Project Pakistan").
82. *Id*. The problem with trying person under the ATA, beyond the harsher sentences, is that those suspects have certain fundamental rights suspended, including a reversal of the burden of proving innocence to receive bail. *See* Amnesty International PAKISTAN, *Legalizing the Impermissible: the New Anti-Terrorism Law*, (Oct. 1997), https://www.amnesty.org/en/documents/document/?indexNumber=ASA33%2F034%2F1997&language=en (click on "Download PDF") (noting the myriad fundamental rights curtailed when a person is charged under the ATA).
83. Justice Project Pakistan, *supra* note 81, at 9.
84. *Id*. The ATA defines terrorism similar to the Draft. *See* Anti-Terrorism Act, 1997, § 6(1)(b) http://www.ppra.org.pk/doc/anti-t-act.pdf (defining terrorism as "the use or threat of action where . . .(b) the use or threat is designed to coerce and intimidate or overawe the Government or the public . . .

to death as a terrorist.[85] Any cybercrime bill passed by the National Assembly should therefore remove Section 10(a).

III. Analysis

The National Assembly should reject the Draft and encourage the Standing Committee to adopt the Stakeholder Draft, albeit with one modification.[86] First, the Stakeholder Draft already imposes oversight upon the FIA by requiring search warrants prior to searches, seizures and arrests (discussed in Section III.A). In addition, the Stakeholder Draft omits Sections 18, 21 and 34—the sections that potentially criminalize journalism and permit blocking content on subjective bases, respectively (discussed in Sections III.B and III.C).[87] However, the Stakeholder Draft's definition of cyber terrorism, Section 10, should remove subsection (a) because it is commonly misapplied by the judiciary (discussed in Section III.D).[88] Overall, the Stakeholder Draft, especially with the removal of Section 10(a), will promote Pakistan's desire to combat cybercrime without infringing on freedom of expression.[89]

IV. Conclusion

Pakistan's resolve to fight terrorism is admirable, but enacting a vague and overbroad cybercrime law under that guise is not the solution. Both PECO 2007 and PECO 2009 were used to promote political agendas and curtail human rights. Unless the course is changed with PECA 2015, that history will repeat itself.

This author recommends the National Assembly reject the Draft and encourage the Standing Committee to adopt the Stakeholder Draft, albeit with one

---

or create a sense of fear or insecurity in society . . . .").

85. The judge noted that there were various flaws in the case, but it nonetheless sentenced him to death. Justice Project Pakistan, *supra* note 81, at 9.
86. The Stakeholder Draft, as approved by the Cabinet Division, can be found on the Bolo Bhi website. *See* Bolo Bhi Resources on Cybercrime, http://bolobhi.org/resources/timelines/bolo-bhi-resources-on-cybercrime/ (to find version of Stakeholder Draft, click through timeline to February 2, 2015 entry titled "Prevention of Electronic Crimes Bill 2015 as Approved by Cabinet Division." Under the document preview, there is a hyperlink to the Stakeholder Draft under the title "Read the Feb 2015 Bill here.").
87. *See id*. For example, Section 21 notes that an agent's powers are "subject to obtaining a search warrant." *Id*. § 21. Sections 18, 21 and 34 are omitted and there are no sections comparable to those sections in the Draft.
88. *See id.* § 7 (defining cyber terrorism in the same manner as the Draft).
89. Although beyond the scope of this paper, one section that will likely need to be modified in the Stakeholder Draft is Section 13. Section 13, as well-intentioned as it may be, confers special protection to women against certain conduct on the internet, including the intentional transmission of communications that harm their reputation, threaten any sexual acts against them, superimpose a photograph of their face over sexually explicit images, or transmit a sexually explicit photograph or video of them. *See id.* § 13. This Section thus provides extra protections to women that are not available to men. Clause 25 of the Constitution of Pakistan prohibits discrimination on the basis of sex. It states that "[a]ll citizens are equal before law and are entitled to equal protection of law and that "[t]here shall be no discrimination on the basis of sex." *See* Pak. Const. Art. 25.

modification, because it provides oversight of the FIA, and omits the sections most likely to be abused. This step is critical for Pakistan to continue its progress as a democratic institution and to preserve freedom of expression, a right too often sacrificed by Pakistan's leaders.