BALANCING THE BREACH: DATA PRIVACY LAWS IN THE WAKE OF THE NSA REVELATIONS

Courtney Giles[*]

[*] Courtney Giles is a J.D. Candidate at the University of Houston Law Center. She received a Bachelor of Journalism in Strategic Communications from the University of Missouri. This comment received the James W. Skelton, Jr. Award for Outstanding Comment in Public International Law. The author would like to thank Professor Jacqueline Lipton for her guidance during the writing process, the editors of the *Houston Journal of International Law* for their hard work throughout the publication process, and her parents for their unwavering love and support.

I. INTRODUCTION

[I]f you want to keep a secret, you must also hide it from yourself.

– George Orwell[1]

In the famous novel *Nineteen Eighty-Four*, George Orwell painted a picture of a society that was constantly watched by Big Brother. Since the advent of computer databases, many different critics[2] and judges[3] have utilized the Big Brother metaphor to warn against the privacy concerns these computer databases pose.[4] In June 2013, the world found that this once fictional metaphor was in fact reality. Edward Snowden, a former National Security Agency ("NSA") contractor, leaked confidential documents and information. The information revealed that the United States had developed a top-secret program, called PRISM.[5] The PRISM program allowed the NSA to collect a variety of digital information from Internet and phone companies through a secret data-mining program to monitor worldwide Internet data, including information on foreign allies operating

1. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 231 (1949).

2. *E.g.*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394–96 (2001). Speaking against the Video Privacy Protection Act of 1988, Senator Patrick Leahy noted that information generated and "stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." He commented, "I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against." S. REP. NO. 100-599, at 7 (1988).

3. Solove, *supra* note 2; *see, e.g.*, Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 575–76 (1963) ("Where government is the Big Brother, privacy gives way to surveillance. But our commitment is otherwise. By the First Amendment we have staked our security on freedom to promote a multiplicity of ideas . . . and to defy governmental intrusion into these precincts."); *see, e.g.*, Planned Parenthood of S. Ariz. v. Lawall, 307 F.3d 783, 790–91 (9th Cir. 2002) (Ferguson, J., dissenting) (arguing an Arizona statute is an invasion of a woman's right to informational privacy, Judge Ferguson notes, "the Supreme Court has mandated that 'Big Brother' has no business snooping around this intensely private, constitutional right [to terminate a pregnancy]").

4. Solove argues that "the database problem cannot adequately be understood by way of the Big Brother metaphor," but rather "emerges from an older paradigm." Solove, *supra* note 2, at 1398.

5. *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents.

outside the United States.[6] The PRISM program was enacted for the sake of national security, but at the expense of individuals' and other countries' privacy.

How did other countries react to this unconsented international surveillance?[7] Many countries expressed concern over the substance of Snowden's revelations.[8] The leaked documents indicated that India was the fifth most tracked country by the NSA.[9] The NSA also targeted Brazil, and the Brazilian president's communications were intercepted.[10]

Even though both India and Brazil were targets of U.S. surveillance, the countries had differing initial reactions to the news. For example, Brazil expressed concern that the NSA had been secretly collecting data across the country without its government's knowledge. Brazil's president, Dilma Rousseff, emphasized the importance of the right to privacy, stating that "[t]he right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country."[11] President Rousseff emphasized the need for respect among nations in upholding international relations.[12]

---

6. *Id.* The slides posted by the *Washington Post* reveal that PRISM collected the data from nine companies, added from 2007 through 2012, including Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. *Id.* This data is collected from the cables where the information travels. Much of the world's information travels through the United States. Therefore, international communications could easily flow into and through the United States before arriving at its final destination. *Id.*

7. Former National Intelligence Director James Clapper defended the need to learn foreign intentions, stating, "this is the fundamental given in the intelligence business." *Looking Back at the Snowden Leaks that Sparked U.S. Surveillance Revelations*, PBS NEWSHOUR (Dec. 26, 2013), http://www.pbs.org/newshour/bb/government_programs/july-dec13/surveillance1_12-26.html.

8. Bruce Zagaris, *The Snowden Extradition Saga*, 29 INT'L ENFORCEMENT L. REP. 324 (2013).

9. *It Is Not Actually Snooping: Khurshid on US Surveillance*, HINDU (July 2, 2013), http://www.thehindu.com/news/national/it-is-not-actually-snooping-khurshid-on-us-surveillance/article4873351.ece.

10. Dilma Rousseff, President, Federative Republic of Braz., Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly 1 (Sept. 24, 2013) [hereinafter Statement of President Rousseff], *available at* http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

11. *Id.*

12. *Id.* at 2.

But, "[i]n the absence of the respect for sovereignty, there is no basis for the relationship among Nations."[13] President Rousseff further emphasized the importance of making new privacy laws when she stated, the "[t]ime is ripe to create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage, and attacks against systems and infrastructure of other countries."[14] The problem of protecting the interception and communication of online data affects the entire international community, not just the relationship among countries.[15] Finally, President Rousseff confirmed that Brazil has planned to establish its own secure, encrypted email service to "prevent possible espionage."[16]

In contrast, India reacted quite differently to the NSA leaks. India's Union Minister for External Affairs, Salman Khurshid, defended the United States' actions by noting, "[i]t is only computer analysis of patterns of calls and emails that are being sent . . . not actually snooping."[17]

Now, Brazil and India are collaborating to find a solution to the issue of data protection on the Internet. Khurshid reinforced that the mass surveillance by the NSA is an "area of concern for all democracies" and announced that India is collaborating with Brazil and other countries "in efforts to find platforms for global governance of the cyber space."[18]

This conundrum reveals three main objectives digital privacy seeks to reconcile: (1) the government's responsibility to ensure the security of its country; (2) the individual's right to privacy; and (3) the business's interest in providing services to its clients.[19]

---

13. *Id.*

14. *Id.*

15. *Id.*

16. *India Plans to Restrict Email Use After NSA Leaks*, BBC NEWS (Oct. 30, 2013), http://www.bbc.co.uk/news/technology-24744695.

17. *It Is Not Actually Snooping: Khurshid on US Surveillance*, *supra* note 9.

18. Shobhan Saxena, *India Working with Brazil on Cyber Security: Khurshid*, HINDU (Oct. 16, 2013), http://www.thehindu.com/news/international/world/india-working-with-brazil-on-cyber-security-khurshid/article5239710.ece.

19. *See* Dhruva Jaishankar, *Beyond Snowden: US Surveillance System a Useful Model for Democratic, Terror-Hit India*, ECON. TIMES (June 27, 2013), http://articles.economictimes.indiatimes.com/2013-06-27/news/40233413_1_surveillance-system-

This Comment will focus on the tension between an individual's privacy and a business's objectives in dealing with laws enacted by different governments. Part II will discuss the history of privacy laws in India and Brazil. It will then outline regulations that have been proposed in each country since the NSA revelations. Part III.A will compare the proposed regulations and the shortfalls of each regulation, including the inconsistency among data privacy laws. Part III.B will examine the possible effects of the laws on individuals and businesses. Part IV will propose a solution to the disjoined Internet privacy laws, arguing that co-regulation is the best option for cohesive Internet privacy laws on an international scale. Finally, the Conclusion will reinforce the need for unified data privacy protection to better ensure the objectives of different countries are met. This can be accomplished through already-established alliances among countries such as India and Brazil.

II. BACKGROUND

Our world is more connected than ever with the expansion of technology and the Internet. New technologies have decreased the cost and increased the speed of information storage and transfers, resulting in widespread information collection and exchange.[20] Businesses are taking advantage of these technologies to increase productivity, improve efficiency, and enhance competitiveness.[21] The low cost of data transfer has allowed businesses to locate operations and develop relationships throughout the world.[22] As a result, enormous amounts of data flow from country to country on a daily basis.[23] However, many privacy laws that govern the flow

---

government-surveillance-business-climate ("But rather than lambasting [PRISM] as Big Brother gone wild, [India] should look at it as a model—however imperfect—of how a modern, democratic society tries to reconcile its conflicting objectives and make necessary compromises between stakeholders on the issue of digital privacy.").

20. Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1091–92 (2002).

21. PRIVACY & COMPUTER CRIME COMM., AM. BAR ASS'N, INTERNATIONAL GUIDE TO PRIVACY 1 (Jody R. Westby ed., 2004) [hereinafter INTERNATIONAL GUIDE TO PRIVACY].

22. Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029, 1032 (2013).

23. INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21.

of this data are local or national.[24] Therefore, data is flowing across borders with varying degrees of legal protection.[25]

Despite this inconsistency in legal protection, countries continue to develop their own privacy laws without collaborating with other countries in the process. Part II.A will first discuss the specific evolution of privacy laws in India and Brazil. Then, Part II.B will walk through the relevant sections of the current proposed data privacy laws in both India and Brazil.

A. History of Privacy on the Internet

Privacy has been a major concern since computers transformed business processes and allowed people to share information in seconds.[26] The protection of this information is often referred to as "informational privacy."[27] It is a type of privacy that gives individuals a right to control their personal information.[28] Many countries have enacted omnibus laws that govern the collection, use, and dissemination of this personal data, and often have an oversight committee to ensure compliance with these laws.[29] However, today, international data privacy laws remain largely inconsistent and present challenges for businesses that operate on a global scale.[30]

1. India's Path to Data Privacy Protection

The Constitution of India ("Constitution") gives the government power to enact legislation.[31] Any laws enacted that

24. *Id.* at 1–2.

25. *Id.*

26. *Id.*; *see* Bartosz M. Marcinkowski, *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, 74 OHIO ST. L.J. 1167, 1170 (2013) (noting "privacy and personal data protection have become paramount issues in the world governed and driven by modern technologies").

27. Marcinkowski, *supra* note 26, at 1174; *see* ADAM D. MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 25 (2010) ("A right to privacy can be understood as right to maintain a certain level of control over the inner spheres of personal information.").

28. Marcinkowski, *supra* note 26, at 1174.

29. INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21, at xxi–xxii.

30. *Id.* at xxiii.

31. INDIA CONST. art. 246.

pertain to data protection or privacy must conform to the fundamental rights laid out in the Constitution.[32] There is no fundamental right to privacy laid out in the Constitution, but Article 21 recognizes the right to life and personal liberty.[33] The Supreme Court of India has held the right to privacy is included in the right to personal liberty set out in Article 21.[34] Although the highest court in India has acknowledged a constitutional right to privacy, it has not adequately enforced this constitutional right guaranteed to its citizens.[35]

Prompted by economic concerns, India finally gave protection for data privacy in 2000.[36] The large outsourcing industry in India brought vast amounts of data from foreign countries into India.[37] Outsourcing occurs when one company retains another to perform a non-core business process.[38] India is a favored destination for outsourcing, allowing business to operate more efficiently.[39] However, a critical concern for businesses that outsource is data privacy.[40] Companies export extensive amounts

32. *Id.*

33. *Id.*

34. *See* People's Union for Civil Liberties v. Union of India, A.I.R. 1997 S.C. 568 (India) (holding that improper wiretapping violates Article 21 of the Constitution because the right to personal liberty includes the right to privacy). Sajai Singh points to three themes that emerged from this judgment: (1) the individual's right to privacy exists, and any unlawful invasion of privacy would impose liability in accordance with law on the offender; (2) the right to privacy is accorded constitutional recognition, which protects personal privacy against unlawful governmental invasion; and (3) an individual's right to privacy is not an absolute right and may be lawfully restricted for the prevention of crime and disorder, the protection of health or morals, and the protection of rights and freedom of others. Sajai Singh, *The Security of Data Export to India*, 13 J. INTERNET L. 9, 10 (2009).

35. Caroline E. McKenna, *India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System*, 38 BROOK. J. INT'L L. 729, 732–33 (2013) (noting India's failure to enact and protect the fundamental rights provided by its constitution).

36. *Id.* at 739–40.

37. *Id.* at 739.

38. Todd B. Ruback & Sarah Mahony, *An Overview of Recent Statutory Changes to Privacy Law in India in Comparison to Similar U.S. and EU Privacy Rules*, 272 N.J. LAW. MAG. 38, 39 (2011).

39. *Id.*

40. Deborah Roach Gaut & Barbara Crutchfield George, *Offshore Outsourcing to*

of sensitive personal information about their customers, leading to increased privacy risks in outsourcing.[41] In India, these risks were heightened because the country lacked legislative and regulatory protection of data privacy.[42] To appease foreign businesses' reluctance to outsource to India, Parliament passed the Information Technology Act of 2000 ("IT Act").[43] The IT Act aimed to protect privacy in the business setting.[44] The legislation required businesses to use reasonable security practices for protecting sensitive data.[45]

However, for the most part, the IT Act did not actively ensure data was handled and stored safely,[46] and it did not specifically provide for protection of sensitive personal information.[47] As a result, foreign clients had to protect their data through data protection clauses in outsourcing contracts to ensure some sort of data security.[48] Many businesses were forced to self-regulate and voluntarily adopt stringent security measures to reduce the risks of misuse of personal data.[49] To attract foreign business and clients into India, stronger data protection laws were needed.[50]

India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing, U.C. DAVIS BUS. L.J. (May 1, 2006), http://blj.ucdavis.edu/archives/vol-6-no-2/Offshore-Outsourcing-to-India.html.

41. *Id.*

42. *Id.*

43. McKenna, *supra* note 35, at 739–40.

44. The Information Technology Act, No. 21 of 2000, INDIA CODE (2000); *see* McKenna, *supra* note 35, at 739–40 (stating the IT Act applies to corporate actors, not state actors).

45. The Information Technology Act, No. 21 of 2000, ch. 1 § 2(1) ¶ ze INDIA CODE (2000).

46. Singh, *supra* note 34, at 10.

47. Gaut & George, *supra* note 40.

48. Singh, *supra* note 34, at 10.

49. Gaut & George, *supra* note 40. This was especially a concern in India, where there were reports of employees selling personal information about customers to outside sources. *See id.* (noting one employee sold bank account details of 1,000 U.K. customers for $8,000 U.S. dollars).

50. Singh, *supra* note 34, at 10.

In 2008, Parliament passed an amendment to the IT Act.[51] The amendment added offenses such as cyber-terrorism and made more cyber-crimes punishable.[52] Section 43A makes every company responsible for implementing and maintaining "reasonable security practices" over sensitive personal data.[53] The transfer of any sensitive personal data out of India to another country is only allowed if that country maintains privacy laws that ensure the same level of data protection as India, or if the transfer is necessary to perform the function for which it was collected.[54] If the company is negligent in implementing and maintaining these practices, it is liable for damages.[55] Section 67C establishes the role of intermediaries.[56] Section 2(w) defines "intermediary" as a person who, on behalf of another person, receives, stores, or transmits an electronic record or provides any service with respect to that record.[57] All intermediaries must preserve and retain certain information in the particular manner prescribed by the government.[58]

In 2011, Parliament gave the IT Act some bite by defining necessary terms and explaining the role of intermediaries.[59] These intermediary guidelines made companies liable for criminal penalties if they fail to delete or take down content, which any individual flags as "offensive."[60]

---

51. The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

52. *Id.* at § 66F; Singh, *supra* note 34, at 10.

53. The Information Technology (Amendment) Act, 2008, No. 10, § 22, Acts of Parliament, 2009 (India).

54. Ruback & Mahony, *supra* note 38, at 40.

55. Singh, *supra* note 34, at 11.

56. *Id.* Examples include Internet service providers, search engines, and cyber-cafes. *Id.*

57. *Id.*

58. *Id.*

59. Information Technology (Electronic Service Delivery) Rules, 2011, Gen. S. R. & O. 316(E) (India); Information Technologies (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gen. S. R. & O. 313(E) (India).

60. Information Technologies (Intermediaries Guidelines) Rules, 2011, Gen. S. R. & O. 314(E) (India).

Although the IT Act was a step in the right direction, most information is still mainly protected via contract. This form of self-regulation allows companies in India to comply with other international standards by incorporating certain provisions into contracts. Companies also establish their own internal data protection policy and process to ensure compliance with data protection standards.[61] For example, under the European Commission's Directive on Data Protection, transfer of data to India must be in accordance with the standard contractual provisions approved by the Commission.[62] If a third country's privacy laws are inadequate, businesses can comply with European standards through contracts that cover gaps in the statutory provisions, and ensure a certain level of protection.[63] The combination of self-regulation and the IT Act ensure there are data protection standards in India.[64]

In 2009, India's Ministry of Communications & Information Technology proposed a program called, The Centralized Monitoring System ("CMS").[65] CMS gives India vast control over the privacy of both the government and individuals. CMS aims to strengthen "the security environment in the country."[66] CMS would be set up on mobile phones, landlines, and the Internet throughout India.[67] The program would intercept data, such as call data records, instantaneously from devices.[68] Call data records include the call details and location of the call.[69] Because

61. Singh, *supra* note 34, at 16.

62. *See* Council Directive 95/46, paras. 57, 58, 60, 1995 O.J. (L 281) 30(EC) (stating "the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited" unless provisions are made for exemptions in certain circumstances); Singh, *supra* note 34, at 16.

63. Council Directive 95/46, para. 58, 1995 O.J. (L 281) 30(EC); Singh, *supra* note 34, at 16–17.

64. Singh, *supra* note 34, at 16.

65. Press Release, Shri Gurudas Kamat, Minister of State for Commc'ns & Info. Tech., Gov't of India, Centralised System to Monitor Communications (Nov. 26, 2009), *available at* http://pib.nic.in/newsite/erelease.aspx?relid=54679.

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

of this intrusiveness, CMS has been compared to the United States' PRISM program.[70] However, unlike PRISM, CMS surveillance actions do not have to be approved by courts.[71] At the time of the NSA surveillance leaks, the government was transitioning to the CMS system.[72]

2. Brazil's Path to Data Privacy Protection

Brazil is a federative republic composed by the Union.[73] Brazil has long recognized privacy as a fundamental right, through both international agreements and its Constitution. Brazil is a party to the International Covenant on Civil and Political Rights ("ICCPR"), which grants the right to privacy under Article 17.[74] Brazil is also a member to the American Convention on Human Rights ("ACHR"), which assures the right to privacy in Article 11.[75] In 2008, the Supreme Court held that

---

70. Danish Raza, *India's Central Monitoring System: Security Can't Come at Cost of Privacy*, FIRSTPOST (July 10, 2013), http://tech.firstpost.com/news-analysis/indias-central-monitoring-system-security-cant-come-at-cost-of-privacy-214436.html.

71. *Id.* PRISM was authorized by the Foreign Intelligence Service Act, which permitted the government to obtain an order from a specially created court that considered applications for blanket surveillance of foreigners abroad, without the need to obtain individualized warrants. Alan L. Zegas, *Social Media, the Police, and the Dystopian Vision of George Orwell*, 284 N.J. LAW. MAG. 54, 58 (2013).

72. *See* Maria Xynou, *India's 'Big Brother': The Central Monitoring System (CMS)*, CENTER FOR INTERNET & SOC'Y (Apr. 8, 2013), http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system (noting surveillance via the CMS system began in April 2013).

73. LUIZ COSTA, A BRIEF ANALYSIS OF DATA PROTECTION LAW IN BRAZIL 3 (2012), *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf.

74. International Covenant on Civil and Political Rights, art. 17, Dec. 19, 1966, 999 U.N.T.S. 171, 177 ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."). Brazil ratified the treaty on January 24, 1992. *Id.*

75. *See* American Convention on Human Rights Pact of San Jose, Costa Rica art. 11, ¶ 2, Nov. 22, 1969, O.A.S.T.S. No. 36 ("No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation."). Brazil ratified the agreement on July 9, 1992. *Multilateral Treaties*, ORG. AM. STATES, DEPARTMENT INT'L L., http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm (last visited Nov. 30, 2014).

national legislation must be in strict compliance with the ACHR.[76]

According to Brazil's Constitution, the Union has exclusive power to legislate on privacy protection.[77] Article 5 of Brazil's Constitution states, "the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured."[78] Article 5 further states habeas data shall be granted to ensure the access to the knowledge of information.[79] Habeas data gives people a right to see data on file about them in government databases, plus channels to correct them.[80] Although this provision grants the right to obtain information, it excludes access to people's information whose secrecy is vital to the security of the society and country.[81]

Privacy is further protected under the 2002 Civil Code, under the Personality Rights chapter. The Civil Code explicitly states: "Except as provided by law, personality rights are inalienable, can neither be renounced and nor undergo voluntary restraint."[82] Article 20 states the disclosure of requested information is prohibited, except as permitted or "necessary to the administration of justice or the maintenance of public order."[83] Article 21 of the code recognizes that " the private life of the natural person is inviolable, and the judge, attending the applicant's request, may take necessary measures to prevent or terminate action contrary to this standard."[84] Brazilian courts provide some protection of privacy and personal data according to these legal texts.[85]

---

76. COSTA, *supra* note 73, at 5.

77. *Id.* at 3.

78. CONSTITUIÇÃO FEDERAL [C.F.] [CONSTITUTION] art. 5, para. X (Braz.).

79. *Id.* para. XIV.

80. LUIZ FERNANDO MARTINS CASTRO ET AL., INTERNATIONAL ENCYCLOPEDIA OF LAWS: CYBER LAW pt. VI, ch. 1, § 3 (Jos Dumortier, et al. eds., 2010).

81. CONSTITUIÇÃO FEDERAL [C.F.] [CONSTITUTION] art. 5, para. XXXIII (Braz.).

82. Lei No. 10.406, de 10 de Janeiro de 2002, CÓDIGO CIVIL [C.C.] de 11.1.2002, art. 11 (Braz.).

83. *Id.* art. 20.

84. *Id.* art. 21.

85. COSTA, *supra* note 73, at 16.

In 2005, Brazil expressed its desire to internationalize control of the Internet.[86] Brazil and several other nations presented a proposal encouraging the World Intellectual Property Organization to consider the needs of developing nations in its policies and regulations regarding control over the Internet.[87] Brazil's proposal sought moderation in intellectual property to further development goals, but the United States, the overseer of Internet governance at the time, hardly considered this proposal.[88] The United States argued the Internet structure should "remain within the control of ICANN[89] and the United States so that the Internet remains stable and secure."[90] This divide over regulation of the Internet is a result of the struggle between control and information sharing.[91] In the country itself, there is no legal criterion to balance conflicts between the right to privacy and the right to information, which can lead to the absence of guidelines and ultimately to conflicts.[92]

B. The Proposed Regulations: India and Brazil

1. Taking Action: India's Proposed Law

Authorities in India are taking various actions to prevent breaches of online privacy.[93] India has banned its officials from

86. Kristin Delaney, *World Wide Web: Using Internet Governance Structures to Address Intellectual Property and International Development*, 32 BROOK. J. INT'L L. 603, 605–06 (2007).

87. *Id.* at 606.

88. *Id.* at 605–06.

89. ICANN is the Internet Corporation for Assigned Names and Numbers, which facilities the global operation of the Internet. *See Welcome to ICANN!*, INTERNET CORP. ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/about/welcome (last visited Nov. 30, 2014) (explaining that each computer is assigned a specific number so computers can communicate with each other to have a global Internet). ICANN also defines policies for how the Internet should run. *Id.*

90. Delaney, *supra* note 86, at 605–06. ICANN is an international non-profit organization that oversees the technical aspects of the Internet. *Id.* at 605 n.17.

91. *Id.* at 605–06.

92. COSTA, *supra* note 73, at 8.

93. *See* The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013 (India) (proposing a new law to protect privacy and personal data in India); Andrew North, *NSA Leaks Helping India Become 'Big Brother' State?*, BBC NEWS (Oct. 31, 2013), http://

using their personal email on government projects.[94] India also proposed plans to bring Internet traffic inside the country.[95] To do this, India would require telecom and Internet companies to route local data through a server located in India, called the National Internet Exchange of India ("NIXI").[96]

In stark contrast to CMS, India proposed The Privacy Protection Bill in 2013. This bill establishes an "effective regime to protect the privacy of all persons and their personal data from Governments, public authorities, private entities and others."[97] The bill sets out conditions for the surveillance and interception of personal data of individuals.[98] It recognizes the right to privacy as a fundamental human right essential to the maintenance of a democratic society, and sets forth a standard of necessity and proportionality when measuring intrusions into privacy.[99] Further, the right to privacy cannot override the right to information.[100] It also recognizes that some information is more sensitive and subject to a higher privacy standard than others.[101] A committee who oversees the regulations and implementation of the bill would implement this standard.[102]

---

www.bbc.co.uk/news/world-asia-india-24753696.

94. *India Plans to Restrict Email Use After NSA Leaks*, *supra* note 16.

95. North, *supra* note 94.

96. Thomas K. Thomas, *Route Domestic Net Traffic via India Servers, NSA Tells Operators*, HINDU BUS. LINE (Aug. 14, 2013), http://www.thehindubusinessline.com/industry-and-economy/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article5022791.ece. Currently, only about ten percent of Internet traffic traveling within India actually goes through the NIXI. An email sent domestically within India may travel through a US server before reaching its destination. *Id.*

97. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013 (India).

98. *Id.*

99. *Id.* ch. I(3).

100. *Id.*

101. *See id.* ch. I(2) (defining "personal data" and "sensitive personal data" separately). Personal data is any data relating to a person, whether directly or indirectly connected with other data. Sensitive personal data is a type of personal data consisting of a person's biometric data or DNA. Sensitive personal data cannot be disclosed to anyone who is not the holder of the personal data. *Id.* ch. I(2), III(12).

102. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. VI(30) (India).

The Privacy Protection Bill establishes a Privacy Commission to enforce the bill.[103] The Commission would consist of a Chief Privacy Commissioner, appointed by the President, and not more than six other Privacy Commissioners.[104] The Chief Privacy Commissioner must have been a Judge of the Supreme Court.[105] One Privacy Commissioner must either be or have been a Judge of a High Court.[106] Finally, one Privacy Commissioner has to be a person of "ability, integrity and standing who has a special knowledge of, and professional experience not less than ten years in privacy law and policy."[107] These requirements ensure the Privacy Commission will properly carry out the duties set forth in the Privacy Protection Bill. In its judicial function, the Privacy Commission serves as a civil court, and all decisions and orders are binding.[108]

The duties of the Privacy Commission include: reviewing safeguards for the protection of privacy and recommending measures for their effective implementation, reviewing measures taken by organizations to ensure compliance with the bill and taking actions as it seems fit, promoting awareness and knowledge of privacy rights, publishing periodic reports related to the handling of personal data, and any other functions it deems necessary for the protection and promotion of privacy.[109]

The Privacy Protection Bill also sets out guidelines businesses must follow in order to collect data or surveillance on individuals.[110] Businesses cannot collect any personal data from individuals that is "not necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection."[111] When a business wants to collect personal data, it must obtain consent from the person whose

103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.* ch. VI(30).
107. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. VI (India).
108. *Id.* ch. VI(41–42).
109. *Id.* ch. VI(33).
110. *Id.* ch. III, ch. I(g).
111. *Id.* ch. III(6).

data it wants to collect.[112] The business has to disclose details about the personal data it is collecting prior to collecting the targeted data.[113] If the business receives consent from the person whose data it is seeking, the business may temporarily store the data, but not longer than necessary to achieve the purpose for which the data was collected or received.[114] Data can only be stored longer than necessary if the business receives consent from the person to whom the data relates, or it is required to be stored for "historical, statistical, or research purposes."[115]

Under the bill, businesses must protect the data they collect.[116] Businesses cannot collect, store, process, or handle personal data without implementing certain security measures to maintain the confidentiality, secrecy and safety of the data.[117] This includes protecting the data from loss or destruction.[118] If the security of the data is breached, the business must notify the person to whom the data pertains as soon as the business becomes aware of the breach.[119]

Businesses also have to follow certain guidelines when disclosing information to other sources. First, the business must obtain consent from the person to whom the data pertains.[120] The business must inform this person of the details of the disclosure.[121] However, a business does not have to obtain consent to disclose certain personal data if the data is necessary to "prevent a reasonable threat to national security, defence or public order" or to "prevent, investigate or prosecute a cognizable offence."[122]

112. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. III(6) (India).
113. *Id.*
114. *Id.* ch. III(7).
115. *Id.*
116. *Id.*
117. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. III (India).
118. *Id.* ch. III(9).
119. *Id.*
120. *Id.* ch. III(10).
121. *Id.*
122. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. III(10) (India).

If a business violates one of the provisions in the Privacy Protection Bill, the business as well as anyone who was responsible at the time the violation was committed, can be held liable.[123] If the business can prove the offense was committed without its knowledge, or that it exercised due diligence to prevent the offense, then it will not be liable.[124]

The Privacy Protection Bill requires interception, gathering and surveillance of personal data to be conducted in a systematic and transparent manner.[125] It not only establishes a system for collecting data, but it also enforces this system through the judiciary.[126] To the extent that this bill directly contradicts the CMS, which allowed for the interception of data without any judicial oversight or disclosure, the new Privacy Protection Bill will prevail.[127]

2. Taking Action: Brazil's Proposed Laws

Shortly after the NSA surveillance leaks, President Rousseff vowed to present proposals to establish a framework for the governance of the Internet.[128] This framework would "ensure the effective protection of data that travels through the web."[129] Since this statement, Brazil has passed two cybercrime bills and amended a document that essentially creates a constitution for the Internet.[130]

123. *Id.* ch. VII(47).

124. *Id.*

125. *Id.* pmbl.

126. *Id.* ch. VI(41–42).

127. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. VIII(55) (India) (stating that "the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law . . ."); Raza, *supra* note 70 (noting that court approval is not required for CMS surveillance).

128. Statement of President Rousseff, *supra* note 10, at 2.

129. *Id.*

130. *See* Carolina Rossini, *New Version of Marco Civil Threatens Freedom of Expression in Brazil*, ELECTRONIC FRONTIER FOUND. (Nov. 9, 2012), https://www.eff.org/deeplinks/2012/11/brazilian-internet-bill-threatens-freedom-expression (explaining two new Brazilian cybercrime bills as well as a new version of Marco Civil).

The Brazilian legislature recently passed two cybercrime bills, which are now awaiting the President's signature.[131] The first bill, called *Azeredo Law*, creates a police infrastructure to fight cybercrime.[132] The bill was originally proposed over ten years ago, and remained highly controversial until most of the controversial provisions were removed.[133] The second bill, called *Carolina Dieckmann Law* "criminalizes unauthorized access to emails and sensitive information online, punishable up to two years in prison."[134]

The largest law, *Marco Civil da Internet* ("Marco Civil"), establishes principles, guarantees, rights, and obligations related to the use of the Internet in Brazil.[135] Marco Civil started as an initiative of the Ministry of Justice to identify rights and responsibilities that must guide use on the Internet.[136] The main objectives of Marco Civil revolve around promoting access to information and cultural development.[137] The Internet regulation is grounded on five ideas: (1) the international nature of the Internet; (2) human rights; (3) values of diversity; (4) openness and collaboration; and (5) "free enterprise, free competition, and consumer protection."[138] Article 8 expressly provides that "the preservation of the right to privacy and freedom of expression in communications is a condition for the full exercise of the right to Internet access."[139]

---

131. *Id.*

132. *Id.*

133. *Id.*

134. *Id.*

135. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014 (Braz.).

136. Press Release, Article 19, Brazil: Original Marco Civil Internet Bill Should be Adopted (Sept. 20, 2013), *available at* http://www.article19.org/resources.php/resource/37253/en/brazil:-original-marco-civil-internet-bill-should-be-adopted [hereinafter Press Release]; *see* Kuek Yu-Chuang, *Yahoo! in Brazil: Support for the Marco Civil da Internet*, YAHOO! (Apr. 29, 2013), https://yodel.yahoo.com/blogs/general/yahoo-brazil-support-marco-civil-da-internet-165645803.html.

137. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, arts. 4,6 (Braz.).

138. *Id.* art. 2.

139. *Id.* art. 8.

The main principles include safeguarding freedom of speech, the protection of privacy, and the protection of personal data.[140] Article 7 acknowledges the Internet user's right to keep their communications secret, except under judicial order.[141] It further prohibits disclosure of information to third parties, except if the user's consent is obtained, or in other circumstances determined by law.[142]

Marco Civil establishes liability of agents in correspondence to their activities.[143] It also establishes the authority to require Internet service companies to install and use centers within Brazil for the collection and dissemination of data.[144] Requiring the data to be stored in Brazil makes these businesses subject to the jurisdiction of Brazilian courts.[145] Therefore, businesses would have to follow local privacy rules and other Brazilian laws.[146]

Internet service providers are not liable for the actions of third parties.[147] The Internet service providers can only be liable for damage arising from the content generated by third parties if they do not take action after receiving specific judicial orders to do so.[148] The judicial order must contain a "clear and specific identification of the infringing content."[149] For example, the proposed regulation provides that Internet users' data communications will only be "disclosed at the request of a court order and limited to instances of criminal investigations and

140. *Id.* art. 3.

141. *Id.* art. 7.

142. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, art. 7 (Braz.).

143. *Id.* art. 3.

144. Esteban Israel & Anthony Boadle, *Brazil to Insist on Local Internet Data Storage After U.S. Spying*, REUTERS, Oct. 28, 2013, http://www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028.

145. *Id.*

146. *Id.*

147. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, art. 18 (Braz.).

148. *Id.* art. 19.

149. *Id.*

prosecutions."[150] Further, Internet service companies cannot monitor, filter, or supervise data content, except in the circumstances allowed by law.[151]

III. A CLOSER LOOK INTO THE PROPOSED DATA PRIVACY LAWS

Part III.A will analyze the strengths and weakness of India and Brazil's proposed data privacy laws, highlighting the inconsistencies in the laws. Then, Part III.B will discuss the effect that these laws will have on India, Brazil, and international businesses operations in these countries.

A. Strengths and Weaknesses of the Proposed Laws

1. India's Governmental Operation

The Privacy Protection Bill emphasizes that the right to privacy is essential and makes a distinction between "personal data" and "sensitive personal data."[152] India gives a higher standard to sensitive personal data, further protecting personal data for its citizens.[153]Although India's proposed bill acknowledges the importance of data privacy protection, it is ambiguous in two major aspects in relation to businesses: first, the type of data businesses can collect, and second, when business do not have to obtain consent to collect this data.

The Privacy Protection Bill establishes a standard for when a company can intrude on a person's privacy.[154] Though this standard establishes some guidelines for businesses and the Privacy Commission to follow, the code still leaves much up to the Commission's interpretation.

First, a business can collect any data "necessary for the achievement of a purpose that is connected to a stated function

150. Press Release, *supra* note 136.

151. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, art. 9 (Braz.).

152. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. I (India).

153. *See id.* ch. III(12) (providing special, more stringent rules for sensitive data).

154. *See id.* ch. I(3) (establishing that intrusions into privacy are always measured by "necessity and tempered by proportionality").

of the person seeking its collection."[155] Virtually any type of data could be "necessary" or have a "connection" to a certain function.[156] These terms give businesses vast leeway in the type of data they collect.[157] If the terms are interpreted loosely, they could potentially serve no use in protecting secret or personal data.[158]

Second, businesses do not have to receive consent to collect this data if the data is necessary to "prevent a reasonable threat to national security, defence or public order" or to "prevent, investigate or prosecute a cognisable offence."[159] Since business information is such a valuable asset, any offense a competing business or other citizen claims against another business could be considered a cognizable offense.[160] If businesses are allowed to obtain private information from other businesses without consent, important assets could be at risk.[161]

Further, with the increased sensitivity to national security issues, an increased variety of information could be considered "necessary to prevent a reasonable threat to national security."[162]

---

155. *Id.* ch. III.

156. BLACK'S LAW DICTIONARY 1030 (9th ed. 2009) (defining "necessary and proper" as being appropriate and well adapted to fulfilling an objective).

157. In general, Indian companies already operate without specific legal requirements related to personal information privacy protection, other than those imposed by contract. Jane Hils Shea, *Attitudes Toward Privacy: A Comparison of India and the United States*, FROST BROWN TODD, http://www.frostbrowntodd.com/pp/publication-214.pdf (last visited Nov. 30, 2014) ("Depending on the specificity of the [contract] . . . the degree of protections will vary considerably from company to company.").

158. *See* Evans v. Commonwealth, 308 S.E.2d 126, 128–29 (Va. 1983) (arguing that "in connection with" in the data collection statute is overly broad and invites arbitrary enforcement).

159. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. III(13) (India).

160. Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 RICH. J.L. & TECH. 12, 28 (2013).

161. *See id.* at 3–4 (noting that information kept passed its useful life poses an increased risk because it is subject to future requests in litigation or governmental investigations).

162. *See* Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 927 (D.C. Cir. 2003) (giving strong deference to agencies that have the authority to disclose confidential information given the "magnitude of the national security interests and potential risks at stake"); Shiri Krebs, Comment, *Lifting the Veil of Secrecy: Judicial Review of Administrative Detentions in the Israeli Supreme Court*, 45 VAND. J. TRANSNAT'L

Businesses and the government would be given free reign to access emails and phone calls, much like the NSA did, without the consent of the parties they were taking the information from.[163] After taking action, establishing in each case that the information was collected in the interests of sovereignty, security in India could not only be practically difficult, but could also lead to increased litigation.[164]

Though the Privacy Protection Bill would establish the first comprehensive privacy regime in India, the bill still needs further clarity and guidance on the investigative board and stricter standards for the type of data gathered and the conditions on when consent must be obtained.

2. Brazil's Transparent Operation

Similar to the Privacy Protection Bill, Marco Civil acknowledges a right to privacy on the Internet, and establishes guidelines for gathering information. However, Brazil's proposed law focuses on sharing data and the transparency of gathering information rather than the process in gathering it.[165] The transparency Brazil promotes supports the public interest and allows those in power to be held accountable for their actions.[166]

Marco Civil establishes that the right to Internet access includes the right to privacy.[167] Although this does not establish

---

L. 639, 645 (2012) (noting since the emergence of the global war or terror, many countries have employed various regimes to confront threats to national security). The Court's judicial review is challenging in cases where the government has relied on privileged intelligence information provided by undisclosed sources, and collected secretly by agencies. *Id.* at 652.

163. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 5.

164. Gulveen Aulakh, *India Proposes the Penalise Invasion of Privacy Offences in Draft Bill*, ECON. TIMES (Feb. 18, 2014), http://articles.economictimes.indiatimes.com/2014-02-18/news/47451233_1_personal-data-privacy-bill-draft-bill.

165. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, art. 4 (Braz.).

166. *Cf.* MOORE, *supra* note 27, at 214 (noting "transparency is an essential component of good government in the sense that those in power can be held accountable for their actions").

167. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, art. 8 (Braz.).

it as a fundamental right, it does make it a condition for access to the Internet.[168]

While the Privacy Protection Bill allows a company to collect data in instances of suit or threats to national security, Marco Civil only allows parties to request information for evidence in a civil or criminal proceeding.[169] Marco Civil only refers to judicial orders for parties responsible for storing Internet service access logs or connection logs.[170] Marco Civil does not address other types of business or government action. Compared to India, these provisions arguably give individuals more privacy and governments a decreased ability to intrude for security purposes.

Rather than establish a separate court to oversee that Internet users' privacy is upheld, Marco Civil gives authority to many different public authorities and sectors of society to establish a transparent, collaborative, and democratic method of oversight.[171] However, Marco Civil does rely on judges to make decisions with respect to the disclosure of certain types of information.[172] It relies on judges to declare whether information is secret, and guarantee the secrecy of the information received.[173] This system is arguably more transparent than India's system because the judges' decisions are not made through a separate, secret court, but through the public judicial system.[174] Having this judicial check ensures that personal data will remain a secret, but also allows the government to get information

168. *Id.*

169. *Id.* art. 22.

170. *Id.*

171. *Compare id.* art. 24 (noting the role of public authorities in promoting transparency, accessibility and social participation in public policy), *with* The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. VI (India) (establishing a separate Privacy Commission to act as a civil court with binding authority over all decisions).

172. Lei No. 12.965, de 23 Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014, art. 23 (Braz.) ("It is the obligation of judges to take the measures necessary to guarantee the secrecy of the information received, and the preservation of the intimacy, private life, honor and image of Internet users.").

173. *Id.*

174. *Cf.* MOORE, *supra* note 27, at 191 (noting the Foreign Intelligence Service Court in the United States, which exercises oversight on U.S. surveillance and rules on surveillance issues and requests, meets in secret and the findings are almost never published).

necessary for the maintenance of the nation.[175] Overall, Brazil's Marco Civil favors the individual's autonomy and protection, while India's Privacy Protection Bill favors the government's interests in national security.

3. The Bigger Problem of Consistency

The differences in the proposed laws highlight the main problem for international businesses today: consistency.[176] International companies, such as Google, must comply with the individual laws in each country, or face consequences.[177] Vast amounts of resources are needed to make sure the company is complying with these laws.[178] This deters smaller companies from establishing markets internationally because the risks of a security breach are too high.[179] Every company has private information that needs to be kept secret.[180] If this information is released, even through litigation or government request, the company can lose value or a handle on its competition.[181] Because information is a valuable asset, companies cannot risk a security breach, and should follow the laws established in the countries where they operate. These laws determine what a company can and cannot do with its data, without incurring legal liability or unwanted risk.[182] But unfortunately, countries differ in the execution and enforcement of their privacy laws.[183]

---

175. *Cf. id.* at 190–201 (arguing that we should insist on judicial oversight and accountability when allowing the government to gather information).

176. *See* Hirsch, *supra* note 22, at 1036 ("The lack of consistency among national laws also creates significant problems for businesses that engage in cross-border transfers of personal data and desire to comply with legal requirements.").

177. *See* Cynthia Miley, *France Data Authorities Fine Google for Non-Compliance with Privacy Policy*, JURIST (Jan. 9, 2014), http://jurist.org/paperchase/2014/01/france-data-authorities-fine-google-for-non-compliance-with-privacy-policy.php (reporting that Google has faced monetary fines from France, the Netherlands, and Germany for violating the countries' data privacy laws).

178. *See* Hirsch, *supra* note 22, at 1037–43 (noting resources include not only on meeting privacy requirements, but also tracking them down and learning about them).

179. *Id.* at 1051.

180. INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21, at xxiii.

181. *Id.* at xxiii.

182. *Id.* at xxi–xxii.

183. *See* Hirsch, *supra* note 22, at 1035 (noting privacy law "differences are

These inconsistent laws can leave businesses, specifically Internet service providers, stuck in the middle between protecting their clients and disclosing requested information.[184] For example, in 2006, Brazil requested data from Google regarding child pornographers and others who commit hate crimes using a social networking site called Orkut.[185] The police wanted this information to track down those responsible for the cyber crimes.[186] When Google initially refused to hand over the information, human rights groups criticized the company for not taking a more active role in going after these criminals.[187] Brazilian prosecutors even threatened to incarcerate Google's sales manager in Brazil if the company did not hand over customer information related to the questioned Orkut accounts.[188] The decision certainly put Google in a tight spot.

Google handed over the data and expressed its intent to cooperate in investigations "while being careful to balance the interests of [its] users and the request[s] from the authorities."[189] It is important to remember that Internet service providers such as Google are not in the business of electronic surveillance.[190] However, they are often targets of law enforcement and courts to turn over private information needed for investigations.[191] Google reports that the number of data requests from governments worldwide has more than doubled in the past three years.[192] In

---

particularly salient on the Internet where personal data are more likely to travel among a variety of legal jurisdictions"); Ragan, *supra* note 160, at 15 (noting "enforcement of privacy regulations varies widely from one jurisdiction to another").

184. Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 555 (2007).

185. *Id.*

186. *Id.*; Andrew Downie, *Google's Brazil Headache*, BLOOMBERG BUSINESS (Aug. 31, 2006), http://www.bloomberg.com/bw/stories/2006-08-31/googles-brazil-headache.

187. Downie, *supra* note 186.

188. Gidari, *supra* note 184.

189. Ellen Nakashima, *Google to Give Data to Brazilian Court: Request Differs from U.S.'s, It Says*, WASH. POST (Sept. 2, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090100608_pf.html.

190. Gidari, *supra* note 184, at 535.

191. *Id.*

192. Jon Fingas, *Google Transparency Report Now Breaks Out US Court Orders*, ENGADGET (Nov. 14, 2013), http://www.engadget.com/2013/11/14/google-transparency-

2012, Brazil issued 783 court ordered requests for information from Google, and India issued 58 orders.[193] From January to June 2013 alone, Brazil made 237 court ordered requests for information, second only to the United States.[194] Google complied with 46 percent of these requests.[195] In August 2013, Facebook released a similar report.[196] From January to June 2013, India ranked second in number of total requests with 3,245 requests.[197] Facebook produced data in 50 percent of the cases.[198]

Google and other Internet service providers face a choice: violate the law or violate the policy of protecting their customers' privacy. Many officials who violate the law justify their actions by alleging there is some socially desirable result for violating the rule.[199] To shield these accusations from criticism, some claim their actions are motivated by moral concerns, national security concerns, or are otherwise necessary, whether the action was legal or not.[200] In a study conducted to test the public's perception of those who violated rules, the violations were deemed more appropriate when the rule was broken in an effort to achieve a socially desirable goal than when it was broken for

report-now-breaks-out-us-court-orders.

193. *Transparency Report*, *January to June 2012*, GOOGLE, http://www.google.com/transparencyreport/removals/government/countries/?p=2012-06 (last visited Nov. 30, 2014); *Transparency Report, July to December 2012*, GOOGLE, http://www.google.com/transparencyreport/removals/government/countries/?p=2012-12 (last visited Nov. 30, 2014).

194. *Transparency Report*, *January to June 2013*, GOOGLE, http://www.google.com/transparencyreport/removals/government/countries/?p=2013-06 (last visited Nov. 30, 2014).

195. *Id.* India made 16 court ordered requests during this time period, and Google complied with 38 percent of the orders. *Id.*

196. MELODY PATRY, INDIA: DIGITAL FREEDOM UNDER THREAT? 16 (Mike Harris & Kirsty Hughes eds., 2013), *available at* http://www.indexoncensorship.org/wp-content/uploads/2013/11/india_digital-freedom-under-threat.pdf.

197. *Id.*

198. *Id.*

199. N.J. Schweitzer et al., *Rule Violations and the Rule of Law: A Factorial Survey of Public Attitudes*, 56 DEPAUL L. REV. 615, 618 n.7 (2007).

200. *Id.* at 618. For example, when President George W. Bush ordered electronic eavesdropping of communications into and out of the United States, supporters of this order pointed to the socially desirable outcome of national security, while critics noted that it violated the Fourth Amendment. *Id.* at 618 n.7.

less virtuous purposes.[201] Here, Internet service providers have a strong case for protecting customer's privacy rights because this socially desirable result is more important than paying a fine to retain customer information.

To complicate matters further, laws surrounding the issue of content removal vary by country and jurisdiction. Since Google has control to post and take down information, it arguably has more power over our privacy than the courts.[202] The question still remains as to how Internet service providers should handle different countries' judgments.[203] Some even believe Google could be a better gatekeeper for privacy than the available alternatives, such as allowing judges to decide.[204]

B. Effects of the Proposed Laws

1. India's Big Brother Approach

Although the IT Act expanded the ability to conduct electronic surveillance, the CMS project still lacks legal backing.[205] Currently, India lacks privacy laws that can protect its citizens from privacy intrusions.[206] Through the CMS, all citizens can be targeted and watched, regardless of whether they have been involved in illegal activity.[207] For example, social

---

201. *Id.* at 633.

202. *See* Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1529 (2012) (arguing that Google executives, who order videos to be taken up and down, exercise more power over free speech than the Supreme Court).

203. *See* Gidari, note 184 (posing questions related to the Internet service provider's choice to challenge the government and go to court, or let large companies take responsibility). For example, Peter Fleisher, the Global Privacy Counsel at Google, noted: "[I]f a German court decides that German murderers should be able to delete evidence of their conviction after a specified time has passed, should that deletion apply only in Germany or across the globe, and who should enforce it?" Rosen, *supra* note 202, at 1534 (citing Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY . . . ? (Mar. 9, 2011, 8:59 AM), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html).

204. *Id.* at 1537.

205. Xynou, *supra* note 72.

206. *Id.*

207. *Id.*

network analysis can be conducted to uncover networks and relationships through social media in attempts to reveal connections to terrorist organizations.[208] These operations enable law enforcement officers to tackle crime and terrorism at the expense of individual privacy.[209]

Cyber security experts in India argue that there is no harm in the CMS, especially since other countries, such as the United States, are conducting similar surveillance.[210] The experts seem to justify the validity of the program as long as it is in the name of security.[211] Opponents of the CMS worry the government will abuse the CMS to monitor or arrest political critics rather than to enhance national security, as intended.[212] Therefore, like in a Big Brother society, the government interest in India prevails.

The Privacy Protection Bill explicitly states, "[t]he provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force."[213] Therefore, the Privacy Protection Bill will control over the CMS system. The Privacy Protection Bill allows businesses and the government to gather any information necessary to "prevent a reasonable threat to national security, defence or public order" or to "prevent, investigate or prosecute a cognisable offence."[214] Even if the CMS is not abused, and data is gathered only for these purposes, it still creates problems because the law in itself is too vague and broad, which could result in disproportionate arrests and prosecutions merely for expressing views on a blog, Facebook, or through email. Without stronger safeguards and checks on the government's actions, the collection of personal data could have a chilling effect on the Indian population because Indian citizens will be deterred from putting

208. *Id.*
209. *Id.*
210. Xynou, *supra* note 72.
211. *Id.*
212. PATRY, *supra* note 196, at 15.
213. The Privacy (Protection) Bill, 2013, Acts of Parliament, 2013, ch. VIII (India).
214. *Id.* ch. III.

personal information on the Internet, obstructing the free flow of information.[215]

2. Brazil's Inadvertent Enclosure

Businesses argue Marco Civil will also hamper the free flow of data.[216] Many business groups fighting hard against the proposed law argue that "[i]n-country data storage requirements would detrimentally impact all economic activity that depends on data flows."[217] However, President Rousseff ensures this proposed law does not intercept the free flow of data.[218]

The proposed law in Brazil would put a great burden on Internet service companies in establishing infrastructure within the country.[219] Even global companies such as Google are pushing back, stating the "data-center requirement would hinder expansion in Brazil, the world's sixth-largest market for Internet users, because the infrastructure would be complicated to develop."[220] If Google violates these laws, it would cost Google ten percent of its total sales in Brazil.[221] Google and other businesses would not be the only ones affected by the laws.[222] According to the public policy director of Google in Brazil, the citizens of Brazil would ultimately suffer because they could not access new services and new tools because companies might not implement these required services until much later, if at all.[223]

The largest complaint of Marco Civil relates to the security problems with establishing local data centers.[224] In a letter to

215. PATRY, *supra* note 196, at 16.

216. Adam Behsudi, *Brazil to Take Up Internet Privacy Bill*, POLITICO (Oct. 29, 2013), http://www.politico.com/story/2013/10/brazil-to-take-up-internet-privacy-bill-98987.html.

217. Israel & Boadle, *supra* note 144.

218. *Id.*

219. Anna Edgerton, *NSA Spying Allegations Put Google on Hot Seat in Brazil*, BLOOMBERG BUSINESS (Oct. 29, 2013), http://www.bloomberg.com/news/articles/2013-10-29/nsa-spying-allegations-put-google-on-hot-seat-in-brazil.

220. *Id.*

221. *Id.*

222. *Id.*

223. *Id.*

224. Esteban Israel & Alonso Soto, *Brazil's Anti-Spying Internet Push Could Backfire, Industry Says*, REUTERS, Oct. 2, 2013, http://www.reuters.com/article/2013/10/

the Brazilian Congress, both Internet trade associations and the International Chamber of Commerce said that the data-center proposal would hurt Brazil's "competitiveness, increase the cost of doing business, lead to slower growth and make Brazilian Internet users more vulnerable to hacking."[225] The International Chamber of Commerce points out that localizing data would make it more susceptible, not less susceptible, to data breaches.[226] This could put international businesses at an increased risk that their most valuable assets could be compromised through a security breach.[227] Because the privacy risks are increased, localizing data inadvertently hinders business objectives to expand internationally while increasing efficiency.

For example, Google normally implements a security strategy that chunks and replicates data over multiple systems to protect user data from cyber attacks.[228] In response, Alessandro Molon, Marco Civil's sponsor, reasoned the "priority of the data-center measure is to make Internet companies subject to Brazilian law, which safeguards citizens against monitoring[;] storing data locally gives Brazil legal control of user information."[229] Even if Marco Civil does protect local communications, the bill does not prevent against the possibility of intrusive surveillance occurring outside of Brazil.[230]

IV. A PRACTICAL SOLUTION TO THE INCONSISTENCY

Surveillance technology is growing rapidly, and governments are adopting these new technologies just as quickly.[231] However, many countries have outdated laws that simply cannot keep up

---

02/us-brazil-internet-idUSBRE9910F120131002.

225. Edgerton, *supra* note 219.

226. *Id.*

227. *See* INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21, at xxi–xxii; Israel & Soto, *supra* note 224.

228. Edgerton, *supra* note 219.

229. *Id.*

230. Press Release, *supra* note 136.

231. Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 76 OHIO ST. L.J. 1071, 1071 (2013).

with the pace that technology is advancing[232] or the ways the government is using these technologies.[233] As a result, direct regulation can be difficult.[234] Part IV recognizes the need for unified laws in the data privacy arena and proposes a practical solution to establish consistency in the laws on an international scale.

Co-regulation within the boundaries of already existing privacy laws may be the best solution to establishing consistency in privacy laws worldwide.[235] Co-regulation combines government and industry initiatives to draft, monitor and enforce privacy standards.[236] This way, the government gets involved in passing laws that keep the public's interests in mind, while the industry provides expertise that makes them more likely to buy into the rules that are established.[237] For example, the Asia-Pacific Economic Cooperation forum ("APEC") and the European Union already employ co-regulation systems that allow for approval of individual codes.[238] Specifically, APEC's Cross Border Privacy Rules relies on co-regulatory codes of conduct that all APEC member states have endorsed.[239] A participating business prepares its own code of conduct that explains how APEC

232. Ragan, *supra* note 160, at 11–12, 16–17 (noting the challenge of regulating information because technologies that generate and deliver information are constantly changing); *see* MOORE, *supra* note 27, at 212–13 (noting that the advancement of information technologies has dramatically changed the ability to control personal information); *see also* INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21, at xxii (stating that many countries have chosen not to address privacy legislation at all).

233. *See* Hosein & Palow, *supra* note 231, at 1076 & n.27 (noting that the United States amended its laws to accommodate this new technique that allowed surveillance of entire populations).

234. *See* Hirsch, *supra* note 22, at 1046 (explaining why co-regulation would be effective for privacy laws).

235. *See id*. (noting co-regulation is an attractive option in areas such as privacy law, where "technologies and business models change too quickly for direct regulation, but where the stakes are too high to rely on industry self-regulation").

236. *Id*. at 1045.

237. *Id*. at 1045–46. Co-regulation is not without its faults, however. It can be slower than self-regulation because you must get government approval. Also, public interest can counter the industry influence for less strict rules. *Id*.

238. Hirsch, *supra* note 22, at 1065.

239. *Id*. at 1048.

principles apply to its operation.[240] Then, if the code properly fulfills APEC's privacy principles, it will be approved.[241] In the European Union, if an outside country has laws that afford an adequate level of protection, the European Commission will approve the cross-border flow of personal data.[242]

India and Brazil should take advantage of alliances similar to APEC and the European Union and use them to act as a springboard to approve privacy regulations across multiple countries.[243] BRICS would be a valid alliance to collaborate and create these laws. BRICS is an alliance between Brazil, Russia, India, China, and South Africa.[244] Like APEC, BRICS began as an informal meeting of government trade officials.[245] APEC's activities are strictly limited to the facilitation of economic development.[246] BRICS countries meet each year to discuss a wide range of global governance issues such as development, security, and social issues.[247] Since its inception, BRICS countries have become major players on an international scale.[248] There is

240. *Id.*

241. *Id.*

242. Council Directive 95/46, para. 5, 1995 O.J. (L 281) 30(EC); INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21, at xxii.

243. *See* Carla Bulford, Comment, *Between East and West: The APEC Privacy Framework and the Balance of International Data Flows*, 3 ISJLP 705, 705 (2008) (discussing APEC's policy framework that can be used by both member economies to adopt comprehensive legislation and by industry groups or companies to implement self-regulatory standards). Although the framework does not bind member countries, it serves as a unifying baseline for their privacy policies. *Id.* at 706.

244. Lauren Verbiscus, *Economic Globalization and the Need for Legal Innovation*, 21 MICH. ST. INT'L L. REV. 779, 781 n.3 (2013). These countries were first grouped together in a 2001 economic report because they had similar emerging market economies. *See* JIM O'NEILL, BUILDING BETTER GLOBAL ECONOMIC BRICS, at S.04–.05 (2001), *available at* http://www.goldmansachs.com/our-thinking/archive/archive-pdfs/build-better-brics.pdf (proposing that the emerging economies of these four countries highlights the need for international cooperation on a "truly global basis"); *About the BRICS*, BRICS INFO. CENTRE, http://www.brics.utoronto.ca/about.html (last updated Jan. 6, 2013) (stating that South Africa was added to the BRIC in 2011).

245. Bulford, *supra* note 243, at 707.

246. *Id.*

247. *About the BRICS*, *supra* note 244.

248. Thomas Osang, *World Trade and Investment: Where Do the BRICS Stand?*, 18 L. & BUS. REV. AM. 515, 516 (2012). Part of this economic growth resulted from the

strong evidence that the BRICS countries are no longer just an acronym to describe similar economies.[249] BRICS countries have worked together to advance their joint interests and coordinate responses to key global challenges.[250]

As a result of the BRICS countries' growing economies and development, the countries have become an attractive destination for businesses to establish their operations.[251] The expanding economies and increased trade in BRICS countries promotes the need for Internet privacy laws.[252] BRICS countries have already instituted a multitude of cooperation mechanisms, spanning a range of sectors, from meeting of government ministers of foreign affairs to business leaders and research institutes.[253] This collaboration gives hope to the idea that BRICS can implement some sort of co-regulation standard for the Internet sector.[254] Co-regulation would be the best method because it will combine the governments of each country with the businesses that have a stake in Internet privacy laws. This standard would establish baseline privacy protections for individuals and businesses on the Internet, improving interoperability with other countries' privacy laws around the world.[255] If a BRICS country has stricter

---

technology and dot com investment boom during the 1990s. *Id.* at 522. Another major factor in economic growth was the technological developments that allowed the rapid spread of information across borders, reducing transaction costs and increasing business. Verbiscus, *supra* note 244.

249. David B. Wilkins & Mihaela Papa, *The Rise of the Corporate Legal Elite in the BRICS: Implications for Global Governance*, 36 B.C. INT'L & COMP. L. REV. 1149, 1150 (2013).

250. *Id.*

251. Osang, *supra* note 248, at 521; *see* Verbiscus, *supra* note 244 (noting countries are shifting business operations to BRICS markets, which offer vast growth opportunities).

252. *See* Wilkins & Papa, *supra* note 249, at 1150 ("[T]he BRICS markets and their increasing influence on the world stage has fueled a growing demand within each country for new laws, regulations, and administrative apparatus to govern this new economic activity and to interface with the broader economic and political environment."); Osang, *supra* note 248, at 520–21 (noting the emergence of BRICS as a major player in the global market due to the vast increase in total trade over the last several years).

253. Wilkins & Papa, *supra* note 249, at 1160.

254. *See id*. (noting BRICS countries continue to collaborate and implement networked cooperation mechanisms).

255. *Cf.* DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 53 (2010) ("The U.S. government

laws, then those would govern.[256] However, if a country did not have a privacy law addressing the specific privacy area, then the BRICS agreement would govern.[257]

For example, the OECD[258] released a recommendation in 2013 recognizing that member countries have a common interest in promoting and protecting the fundamental right to privacy and that the increasing flow of personal data across borders increases the need for improved interoperability among privacy frameworks, as well as strengthened cooperation among privacy enforcement authorities in different countries.[259] The OECD recommends that member countries implement the proposed guidelines.[260] In the proposed guidelines, the OECD notes the guidelines should be regarded as a minimum standard and can be supplemented by additional measures for the protection of privacy, which may impact the flow of personal data across borders.[261] Finally, the recommendation discourages the restriction of the flow of personal data across borders and encourages the development of internal arrangements that promote interoperability between privacy frameworks.[262] APEC modeled its Privacy Framework off of similar OECD guidelines released in September 1980.[263]

---

should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' commercial data privacy frameworks.").

256. *Cf.* Hirsch, *supra* note 22, at 1048–49 (stating that companies that follow APEC-approved codes of conduct are still subject to the privacy laws of individual APEC nations).

257. *Cf.* Marcinkowski, *supra* note 26, at 1193 (noting that if civil law measures were not available, international standards would apply to ensure enforcement).

258. The Organisation for Economic Co-operation and Development (OECD) aims to promote policies that will improve the economic and social well being of people around the world. The OECD works with governments, and provides a forum for governments to work together to seek solutions to common issues, including the protection of privacy and personal data worldwide. *About the OECD: Our Mission*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/about (last visited Nov. 30, 2014).

259. ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 11 (2013), *available at* http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

260. *Id.* at 12.

261. *Id.* Annex para. 6.

262. *Id.* Annex paras. 17, 21.

263. Bulford, *supra* note 243, at 709.

These guidelines addressed collection limitations, data quality, purpose specifications, use limitations, security safeguards, openness, individual participation, and accountability.[264]

If BRICS countries can agree on a set of privacy standards to enforce throughout the countries, international trade would become easier and more efficient.[265] The extraterritorial application of privacy laws and the differing standards for safety as data moves from country to country highlights the need for increased international agreement regarding data privacy and movement across borders.[266] The economic, political, and cultural relations in different countries should teach away from the view that the Internet is "some omnipotent force inevitably destined to emancipate humanity."[267] Rather, the Internet is ever-changing and locally-specific.[268] The difference in the proposed laws between Brazil and India underscore this disunited system and further highlight the need for a unified standards and co-regulation that can respond faster to the ever-changing technology of the Internet.

V. CONCLUSION

Although the NSA surveillance leaks reinforce the view that the Internet can lead to a Big Brother society, we should look at the Internet in different terms. Countries should collaborate to foster activity on the Internet, rather than chill Internet usage. In spite of the initial differing responses to the NSA surveillance leaks, both Brazil and India took immediate action to address the privacy rights of their citizens on the Internet. Both the Privacy Protection Bill and Marco Civil have strong implications

---

264. *Id.* at 709 n.16.

265. *But see* Gaut & George, *supra* note 40 (noting that despite the growing convergence of international data privacy protection, "privacy" still has different meanings for different cultures). Just because privacy directives differ, or a country does not explicitly define privacy as a fundamental right, it does not mean, however, that one country values privacy less than another. Alessandra Suuberg, *The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law*, 16 TUL. J. TECH. & INTELL. PROP. 267, 271–72 (2013).

266. INTERNATIONAL GUIDE TO PRIVACY, *supra* note 21, at xxi–xxii.

267. BARNEY WARF, GLOBAL GEOGRAPHIES OF THE INTERNET 40 (2013).

268. *Id.*

on Internet service providers and international businesses that must comply with these laws.

The possible effects of these laws reveals the tension between objectives of the government in ensuring national security, the individual's right to privacy, and the business interest in providing services to customers on the Internet. Big Brother imposed total government surveillance at the expense of individual privacy. This type of society does not balances these objectives at all. While India's law favors the government's interest in security, it still recognizes the fundamental right to privacy. Brazil's law tries to increase individual autonomy and the free flow of data, in exchange for more government transparency and implementation through public courts.

Though these objectives weigh differently among different countries, countries should still work together to establish more cohesive data privacy laws. This would make the operation of international businesses more efficient in both the daily operations and interactions with governments. Similar laws would allow businesses to operate similarly in each country and handle requests for information and court judgments in similar ways, thus saving time and money.

Brazil and India should use the BRICS alliance as a tool to establish a blanket privacy law among these developing nations. This agreement could function similarly to APEC's privacy rules, and make it easier for businesses to comply with privacy laws, as well as promote steps toward a unified privacy system on the Internet. A co-regulation system would allow countries and businesses to work together to amend or implement laws necessary to keep up with technology growth. Until countries reach such an agreement, businesses should mitigate risks by enacting their own set of privacy practices through self-regulation to comply with privacy policies and keep breaches from occurring in the first place.[269]

Ultimately, countries should work together to safeguard data privacy on the Internet so that the fundamental right to privacy is protected and the international flow of data is secure, keeping

269. Ruback & Mahony, *supra* note 38, at 41.

in mind the balance between the government's responsibility to ensure national security, the individual's right to privacy, and the role of businesses in balancing these two objectives.