www.jusletter-it.eu

Gertjan Boulet / Elonnai Hickok

Post-Snowden reactions in India and Belgium: A snapshot

This article explores and analyzes reactions, policies, and projects that have emerged post-Snowden in India and Belgium in an attempt to understand the impact of the Snowden Revelations across jurisdictions. Part 1 provides an overview of the post-Snowden public response in India and Belgium. Parts 2 and 3 give an overview of the post-Snowden inquiries and cybersecurity initiatives in India and Belgium. Part 4 refers to surveillance initiatives by India and Belgium, of which some have an obvious extraterritorial reach. Finally, we draw conclusions from the comparison obetween the post-Snowden response of India and Belgium, and point to the adoption of the International Principles on the Application of Human Rights to Communications Surveillance, as well as internal reviews of national surveillance legal regimes and practices as steps that both governments, despite contextual differences, could adopt.

Category: Articles
Field of law: Data Protection; Data Security
Region: Belgium; India

Citation: Gertjan Boulet / Elonnai Hickok, Post-Snowden reactions in India and Belgium: A snapshot, in: Jusletter IT 15 May 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1 Introduction

[Rz 1] Starting in June 2013, whistle blower Edward Snowden leaked multiple documents detailing the surveillance PRISM Programme of the United States National Security Agency (NSA).[1] The impact of the leaks has been both economical, political and legal, and has been felt by countries around the globe. In a post-Snowden world, countries are facing critical questions about appropriate limits to state surveillance – particularly extraterritorial surveillance, privacy rights of citizens and foreigners, cybersecurity, and internet governance. In that regard, the post-Snowden reactions of Belgium, as a Member State of the European Union (EU), will reflect EU developments, such a the recent annulment of the EU Data Retention Directive by the European Court of Justice. The position of Belgium may be further influenced by the alleged involvement of the intelligency agency of another EU Member State, the United Kingdom's Government Communications Headquarters (GCHQ).

[Rz 2] This article explores and analyzes reactions, policies, and projects that have emerged post-Snowden in India and Belgium. Though both India and Belgium have many legal tools addressing surveillance and cybercrime, including criminal law, internet related legislation, national level policies, and international agreements that have been established pre-Snowden, this article intentionally limits itself to post-Snowden developments, so as to highlight potential trends arising from the revelations. Part 1 gives an overview of the post-Snowden public response in India and Belgium. Parts 2 and 3 give an overview of the post-Snowden inquiries and cybersecurity initiatives in India and Belgium. Part 4 refers to surveillance initiatives by India and Belgium, of which some have an obvious extraterritorial reach. Finally, we draw some conclusions from the comparison between the post-Snowden response of India and Belgium. As information from whistleblower Edward Snowden is still coming into the public domain, this article necessarily

[1] For more information about the Snowden leaks see: Al Jazeera, «Gaurdian announces leak of classified NSA documents», 5 June 2013. Available at: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html(all Internet sources last visited on 9 May 2014).

draw upon opinions, statements and information reported in the press.

2 The post-Snowden public response

2.1 India

[Rz 3] India is the largest democracy in the world, housing a population of 1.2 billion people[2], and multiple languages and religions. India's political relationship with the United States has been characterized as friendly – though the two countries do not see eye to eye on a number of issues.[3] According to documents leaked by Edward Snowden, India is the fifth most important NSA target worldwide[4], with the NSA collecting approximately 13.5 billion pieces of data in one month[5], and planting bugs in India's foreign embassies and missions in Washington DC and New York.[6]

[Rz 4] The public and the governmental response to information arising out of the NSA leaks regarding the United States surveillance of Indian communications, including governmental communications, has been inconsistent. On one level, parts of the Indian Government have not reacted strongly to the intrusion – as India's foreign Minister, Salman Khurshid, has been quoted in the press stating that the surveillance conducted by the US was «*only computer analysis of patterns of calls and E-Mails that are being sent. It is not actually snooping specifically on content of anybody's message or conversation*».[7] Similarly, on the topic, a spokesperson for the Prime Minister of India, Manmohan Singh, has stated to the press that «*there are no concerns*».[8] On another level, the response from other parts of the Indian Government has been indignant – as a home ministry official commented to the press that «*It's not just violation of our sovereignty, it's a complete intrusion into our decision-making process*».[9]

[Rz 5] Post-Snowden, portions of the Indian Government have also displayed an evident mistrust for US internet companies. For example, in 2013 the Indian Election Commission cancelled plans to have Google implement programs to improve voter access to information due to concerns raised that the information would be shared with the US government.[10] While P. Rajeev, Member of

---

2 Indiaonlinepages.com. Available at: http://www.indiaonlinepages.com/population/india-current-population.html.

3 The Economist, «Less than allies, more than friends», 16 June 2012. Available at: http://www.economist.com/node/21556935.

4 Andrew North, «NSA leaks helping India become «Big Brother» state?», *BBC*, 31 October 2013. Available at: http://www.bbc.co.uk/news/world-asia-india-24753696.

5 Glenn Greenwald/Shobhan Saxena, «India among top targets of spying by NSA», *The Hindu*, 23 September 2013. Available at: http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece.

6 Shobhan Saxena, «NSA planted bugs at Indian mission in D.C, U.N.», *The Hindu*, 25 September 2013. Available at: http://www.thehindu.com/news/international/world/nsa-planted-bugs-at-indian-missions-in-dc-un/article5164944.ece.

7 BBC, «India plans to restrict E-Mail use after NSA leaks», 30 October 2013. Available at: http://www.bbc.com/news/technology-24744695.

8 Andrew North, «NSA leaks helping India become «Big Brother» state?», *BBC*, October 31st 2013. Available at: http://www.bbc.co.uk/news/world-asia-india-24753696.

9 Jason Burke, «NSA spied on Indian embassy and UN mission, Edward Snowden files reveal», *The Guardian*, 25 September 2013. Available at: http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission.

10 M. Rochan, «Snowden NSA Leaks: India's Election Commission Dumps Google», *International Business Times*, 10 January 2014. Available at: http://www.ibtimes.co.uk/snowden-nsa-leaks-indias-election-commission-dumps-

Parliament from Kerala, started a public petition asking Facebook, Google, Yahoo, and Microsoft to share information about the extent of disclosure by the company to the NSA.[11] Since the NSA leaks became public, the Indian press and public has speculated widely about the response of the Indian Government, pointing to the fact that India desires to have strong economic ties with the U.S[12], highlighting that the Indian public has not reacted strongly –thus not forcing the Indian Government to react[13], and surmising that the Indian Government is using the NSA scandal to offset and justify its own surveillance practices and upcoming schemes.[14]

2.2 Belgium

[Rz 6] Belgium is an important hub for the EU institutions, and for that reason also an interesting target for potential cyber-espionage. On several occasions, EU Officials have been reported as victims of spying activities, such as Herman Van Rompuy, President of the European Council.[15] Nevertheless, the post-Snowden public response in Belgium has been remarkably weak in comparison with the public response in India. The post-Snowden public voice in Belgium was triggered in September 2013, when the news headlines focused on the hacking of the internal systems of Belgacom, Belgium's largest telecom provider, and whose customers include the European institutions. The Belgian newspaper the Standaard referred to the alleged involvement of the NSA, and reported the targeting of a subsidiary of Belgacom, Bics, which offers telecom services in Africa and in the Middle East.[16] Newspaper Der Spiegel referred to documents leaked by Snowden indicating the involvement of the British GCHQ intelligency agency behind the hack.[17] The Belgian federal public prosecutors referred to the incident as «*state-sponsored cyber-espionage*'[18], while the Belgian Prime Minister, Elio di Rupo, categorized it as «*strategic information gathering*» with «*a high-level involvement by another country*».[19] Elio Di Rupo also noted that «*appropriate steps will be taken if the break-in turns out to be a case of cyber-espionage*».[20] In addition to the hacking of

google-1431822.

11 For access to the petition website see: https://www.change.org/en-IN/petitions/google-facebook-microsoft-yahoo-reveal-information-on-data-of-indian-citizens-given-to-us-security-agencies-2#.

12 Wasantha Rupasinghe, «New Delhi downplays evidence of extensive NSA spying targeting India,» *WSWS*, 14 November 2013. Available at: http://www.wsws.org/en/articles/2013/11/14/nsai-n14.html.

13 Sushil Aaron, «Waiting for Greenwald: why India cant» stay mute on NSA spying», *Hindustan Times*, 3 December 2013. Available at: http://www.hindustantimes.com/comment/analysis/waiting-for-greenwald-why-india-can-t-stay-mute-on-nsa-spying/article1-1158485.aspx.

14 Andrew North, «NSA leaks helping India become «Big Brother» state?», *BBC*, 31 October 2013. Available at: http://www.bbc.co.uk/news/world-asia-india-24753696.

15 Andrew Rettman, «Hackers stole Van Rompuy's E-Mails», *EU Observer*, 30 July 2012. Available at: http://euobserver.com/justice/117097.

16 Mark Eeckhaut/Peter De Lobel/Nikolas Vanhecke, «NSA verdacht van hacken Belgacom» (NSA suspected of the hacking of Belgacom), *De Standaard*, 19 September 2013. Available at: http://www.standaard.be/cnt/dmf20130915_00743233.

17 Spiegel, «Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm», 20 September 2013. Available at: http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

18 Colin Clapson, «Who bugged Belgacom», *Flandersnews.be*, 16 September 2013. Available at: http://www.deredactie.be/cm/vrtnieuws.english/News/1.1730665.

19 New Europe «Belgium's telecoms firm Belgacom hacked; officials suspect state-sponsored cyber-espionage», 16 September 2013. Available at: http://www.neurope.eu/news/wire/belgiums-telecoms-firm-belgacom-hacked-officials-suspect-state-sponsored-cyber-espionage.

20 Alan Hope, «Belgacom computers hacked», *Flanders Today*, 18 September 2013. Available at: http://www.flanderstoday.eu/business/belgacom-computers-hacked.

Belgacom, news headlines also focussed on the alleged hacking of Elio di Rupo's private e-mail account,[21] the computer network of the Belgian diplomatic service[22] and the computer of Belgian professor Jean-Jacques Quisquater, expert in cryptography.[23] Furthermore, on 10 May 2014, the newspaper De Tijd reported the hacking by Russia of the computer network of the Belgian Ministry of Foreign Affairs, supposedly to get confidential files about the current crisis in Ukraine.[24] On 12 May 2014, De Tijd reported about the decision of the Belgian Ministry of Foreign Affairs to go offline by putting its computer networks in quarantine.[25]

3 Post-Snowden inquiries

[Rz 7] The Government of India has not officially called for an inquiry into the US spying, and has not publicly asked Indian security agencies about their knowledge of access by the NSA.

[Rz 8] In Belgium, the Flemish Human Rights Ligue[26] and Belgian Green parties[27] have unsuccesfully called for a parliamentary inquiry commission into Prism. However, in contract to India, Belgium has several ongoing inquiries on various levels.

[Rz 9] First, post-Snowden, Hugo Vandenberghe, former member of the Belgian Senate and member of the Flemish bar association in Brussels, put that either the Belgian intelligence services «*didn't know about it* [NSA spying] *and they failed or they were aware of these monstrous practices*». Subsequently, he called for an investigation by the Belgian Standing Intelligence Agencies Review Committee (so-called Comité I), in charge of the supervision of the Belgian intelligence services, into the role played by Belgian intelligence services in the NSA spying.[28] Subsequently, the Belgian Senate asked the Comité I to launch three investigations related to Prism, respectively about the involvement of the Belgian intelligence services, the applicable (privacy) laws for data exchanges, and the economic consequences of Prism.[29]The second investigation is carried out in cooperation with the Belgian Privacy Commission.

---

21 FlandersNews.be, « PM's personal E-Mail box hacked», 31 May 2013. Available at: http://www.deredactie.be/cm/vrtnieuws.english/Politics/1.1644174.

22 Simon Demeulemeester, «Parket onderzoekt hacking «gevoelige informatie» Buitenlandse Zaken» (Public Prosecutor investigates hacking of «sensitive information» Foreign Affairs), *Knack.be*, 19 September 2013. Available at:http://www.knack.be/nieuws/belgie/parket-onderzoekt-hacking-gevoelige-informatie-buitenlandse-zaken/article-normal-106557.html.

23 Mark Eeckhaut/Nikolas Vanhecke, «Belgian professor in cryptography hacked» (English summary), *De Standaard*, 1 February 2014. Available at: http://www.standaard.be/cnt/dmf20140201_011.

24 Lars Bové, «Moskou hackt Belgische staat. Spionage in volle Oekraïne-crisis» (Moscow hacks the Belgian state. Espionage in full-blown Ukraine crisis), De Tijd, 10 May 2014. Available at: http://www.tijd.be/nieuws/politiek_economie_belgie/Moskou_hackt_Belgische_staat.9499843-3136.art?ckc=1.

25 Lars Bové, «Diplomatie offlina na hacking» (Diplomatic service offline after hacking), De Tijd, 12 May 2014. Available at: http://www.tijd.be/nieuws/politiek_economie_belgie/Diplomatie_offline_na_hacking.9500343-3136.art.

26 Liga voor Mensenrechten, «Liga vraagt Parlementaire Onderzoekscommissie over NSA» (Liga asks for Parliamentary Inquiry Commission on the NSA), 24 January 2014. Available at: http://www.mensenrechten.be/index.php/site/nieuwsberichten/liga_vraagt_parlementaire_onderzoekscommissie_over_nsa.

27 Jos De Greef, «Groenen willen onderzoekscommissie naar spionage» (The Greens ask an inquiry commission for espionage), *Flandersnews.be*, 1 February 2014, http://www.deredactie.be/cm/vrtnieuws/buitenland/NSA-schandaal/140201_NSA_groenen.

28 Colin Clapson, «Did Belgium know about US snooping?», *Flandersnews.be*, 2 July 2013. Available at: http://www.deredactie.be/cm/vrtnieuws.english/News/1.1667342.

29 Kristof Clerix, «Controlecomité inlichtingendiensten start groot Prism-onderzoek» (Control committee for intelligence services starts a big Prism-investigation», *Mondiaal Nieuws*, 5 August 2013. Available at: http://www.mo.be/artikel/controlecomite-inlichtingendiensten-start-groot-prism-onderzoek.

[Rz 10] Second, the same Belgian Privacy Commission initiated an investigation in the hacking of Belgacom and a co-investigation with the Dutch Data Protection Authority into the security of the financial system of the «Society for Worldwide Interbank Financial Telecommunication» (SWIFT), following allegations of access by foreign intelligence services to the financial data traffic of SWIFT.[30]

[Rz 11] Third, the post-Snowden response of the Belgian public prosecutors has been quite strong. Pre-Snowden, in 2013, federal public prosecutor Frédéric Van Leeuw expressed his fear that a great disaster may be needed in order to convince the public of a general cyber security policy.[31] The abovementioned victims of hacking, Belgacom, Prime Minister Elio di Rupo and the Belgian Ministry of Foreign Affairs filed complaints with the federal prosecutor. Additionally, public prosecutors are investigating the hacking of the computer network of the Belgian diplomatic service and of the computer of Professor Jean-Jacques Quisquater, expert in cryptography (see above: 1.).

4 Post-Snowden cybersecurity initiatives

4.1 India

[Rz 12] Post-Snowden, the Government of India has contemplated and taken a number of steps towards strengthening the Indian cyber security regime at a policy level.

4.1.1 National Cyber Security Policy 2013 and E-Mail Policy by the Department of Electronics and Information Technology

[Rz 13] In July 2013, the Department of Electronics and Information Technology[32] published the «*National Cyber Security Policy 2013*» with the vision to «*build a secure and resilient cyberspace for citizens, organizations. and government*». The policy provides a «roadmap» of different cyber security initiatives that the Government of India will pursue. Among other things, the policy envisions increasing the number of trained cyber professionals in the country, creating a 24x7 National Critical Information Infrastructure Protection Centre, developing indigenous security technologies, ensuring certification and verification of IT products and software used by Government Departments, and protecting data while it is in transit or it is being processed, handled, or stored in order to safeguard the privacy of citizen's data. [33]

---

[30] Caroline Wilson, «Belgian and Dutch DPAs to investigate security of SWIFT system», blog of *Privacy International*, 15 November 2013. Available at: https://www.privacyinternational.org/blog/belgian-and-dutch-dpas-to-investigate-security-of-swift-system.

[31] Interview by Nikolas Vanhecke with Frédéric Van Leeuw, *De Standaard*, 5 April 2013. Available at: http://www.standaard.be/cnt/dmf20130404_00529905.

[32] The Department of Electronics and Information Technology is responsible for the creation and implementation of policies related to the internet and information technology – including cyber laws and cyber security. More information about the Department can be found at: http://deity.gov.in/content/functions-deit.

[33] Department of Electronics and Information Technology, National Cyber Security Policy 2013. July 2013. Available at: http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.

4.1.2 E-Mail Policy of the Government of India

[Rz 14] In addition to the «*National Cyber Security Policy 2013*» the Department of Electronics and Information Technology is in the process of developing the «*E-Mail Policy of the Government of India*», and as a supplement, the «*Acceptable Use of IT Resources of Government of India*». These policies will set norms and practices for the use of E-Mail, the internet by government officials. To this extent, post-Snowden, the Indian Government has been inward looking, indicating a concern about present governmental practices with regards to the use of the internet. On 21 October 2013, the Department of Electronics and Information Technology circulated the policies to Governmental Departments for comment and recommendations.[34] The policies have yet to be finalized, and draft components can currently be found on the website of Department of Electronics and Information Technology.[35] The policies enumerate a number technical measures to be adopted as well as best practice guidelines for use of internet services. For example, all government officials should use encryption when sending classified information, officials working abroad in embassies and missions should use static IP addresses and virtual private networks, and in case of a security breach, an SMS alert will be sent to the registered mobile number containing details of the action that is to be taken by the user. The policies also require best practices to be followed including logging out E-Mail accounts whenever the computer is left unattended for a considerable amount of time, employing the latest version of the Internet Browser, and disabling the «save password» and «auto complete» features in a browser. Most significantly, the policies call for government E-Mail to be restricted to only the National Informatics Centres (NIC) mail servers in order to help prevent cyber crimes targeted at the Government from occurring. Presently, many Indian Government Officials use G-Mail, Yahoo and Hotmail addresses.[36] This means that not only do their data pass through different jurisdictions, but for the government to access the data of their own officials, they must issue requests to service providers, domestic or foreign, depending on the service. This is particularly problematic for the Government of India if the service provider is foreign, as processes permitting access such as Mutual Legal Assistance Treaties (MLATs), are often slow and inefficient.

4.1.3 Report on Cyber Crime, Cyber Security, and Right to Privacyby the Parliamentary Standing Committee on Information Technology

[Rz 15] In February 2014, the Parliamentary Standing Committee on Information Technology (2013–2014), comprised of members from the Lok Sabha and the Rajya Sabha

[Rz 16] Who are they? , presented the «*52nd Report on Cyber Crime, Cyber Security, and Right to Privacy*». The Report is a compilation of briefings and evidence from the Department of Electronics and Information Technology on the state of cyber security in India, as well as recommendations from the Standing Committee. Despite the objectives defined in the National Cyber Security Policy, the Report demonstrates that there are still a number of steps that must be taken for these

34 Notification from the Department of Information Technology Government of Himachal Pradesh, to all the Administrative Secretaries to the Government of Himachal Pradesh. Consideration of «E-Mail policy of GoI and Policy on acceptable use of IT Resources of GiO, formulated by DeitY, by the Committee of Secretaries. Available at: http://himachaldit.gov.in/file.axd?file=2013%2F11%2FGoI+Mail+policy.pdf.

35 For access to the policies comprising the «E-Mail Policy» see: http://deity.gov.in/content/E-Mail-policy.

36 New Delhi Television (NDTV), Indian Government wakes up to risk of Hotmail, Gmail, 8 December 2013. Available at: http://www.ndtv.com/article/india/indian-government-wakes-up-to-risk-of-hotmail-gmail-455999.

goals to be realized. For example, according to the Report, India presently has only 44 empanelled auditors for carrying out cyber security audit related activities, 65,000 trained personnel in issues related to cyber security, and only 546 critical sector organizations under Central Government Departments have obtained the required ISO 27001 certification.[37] In the Report, the Department of Electronics and Information Technology also emphasized the importance of domestic servers – stating in evidence provided to the Standing Committee «*our policy is to encourage the hosting of servers in India ... so our efforts are there that the Indian data should remain in the country and the servers should be in the country, and the citizens should be able to access services in India*».[38] The Report also points to the importation of electronics and IT products and the hosting of servers outside of India as a threat to India's security and to the security and privacy of Indian citizens, and stresses the need for more Memoranda of Understanding (MoUs) and International Treaties for the facilitation of international cooperation on cyber security matters. On the topic of the NSA Spying, the Standing Committee stated «*the Committee are of the strong opinion that the Department should have exercised enough caution so that such a situation was not allowed to occur at the first instance. Further, the Committee feel that the Department should be extremely vigilant and cautious in terms of safety as well as in terms of policy with different countries so as to avoid such leakage and interception of sensitive data in the name of surveillance*».[39] The Report is significant as in its recommendations, the Standing Committee emphasizes the need for a privacy legislation in the context of cyber security to be passed in India.

4.1.4 Domestic Servers

[Rz 17] As highlighted by the Department of Electronics and Information Technology in the «*52nd Report on Cyber Crime, Cyber Security, and the Right to Privacy*», many stakeholders in India have been voicing the need for domestic servers as an important steps towards enhancing Indian cyber security post-Snowden. For example, in 2013, news reports indicated that on request of the Deputy National Security Advisor of India, the Department of Telecommunications[40] is exploring the possibility of requiring all Internet Services Providers (ISPs) and Telecommunication Service Providers (TSPs) to route local data through the National Internet Exchange of India (NIXI).[41] Many industry bodies – though not all – have echoed this standpoint.[42]

---

37 Standing Committee on Information Technology, «The 52nd Report on Cyber Crime, Cyber Security, and Right to Privacy», February 2014 p. 14. Available at: http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf.

38 Ibid., p. 21.

39 Ibid., p. 70.

40 The Department of Telecommunications is responsible for policies relating to the telecom sector, licensing of telecommunication companies, and coordination of matters relating to telecommunications. More information about the Department can be found at: http://www.dot.gov.in/about-us/objectives-dot.

41 Thomas K. Thomas, «Route domestic Net traffic via India servers, NSA tells operators», *The Hindu Business Line*, 14 August 2013. Available at: http://www.thehindubusinessline.com/industry-and-economy/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article5022791.ece.

42 Hindustantimes, «US Fallout: Indian ISPs seek local servers for global firms», 10 June 2013. Available at: http://www.hindustantimes.com/business-news/us-fallout-indian-isps-seek-local-servers-for-global-firms/article1-1073789.aspx.

4.2 Belgium

[Rz 18] Pre-Snowden, in 2011, the Belgian Standing Intelligence Agencies Review Committee published an investigation report with «Conclusions and recommendations of the investigation into the way in which the Belgian intelligence services consider the necessity of protecting the information systems against foreign interceptions and cyberattacks».[43]

[Rz 19] The Belgian «cyber security»-strategy of 21 December 2012[44] further addresses the threat of economic and political cyber-espionage,[45] and identifies 3 strategic objectives: 1) a safe and reliable cyberspace, 2) an optimal security and protection of critical infrastructures and governmental information systems, and 3) the development of national cyber security capabilities.[46]

[Rz 20] In October 2013, Prime Minister Elio Di Rupo announced that the Belgian federal government would reserve ten million euro for strengthening Belgium's cybersecurity in 2014.[47] However, on 9 May 2014, the Belgian media reported that the budget would not have been invested.[48]

[Rz 21] In November 2013, one year after the publication of the Belgian «cyber security»-strategy, the Belgian cyber security guide was launched,[49] It lists ten key security principles and ten elementary security actions. Our attention goes to the ten security actions: 1) Implement user education & awareness; 2) keep systems up to date; 3) Protect information; 4) Apply mobile device security; 5: Only give access to information on a «need to know» basis; 6) Enforce safe surfing rules; 7) Use strong passwords and keep them safe; 8) Make and check backup copies of business data and information; 9) Apply a layered approach against viruses and other malware; 10) Prevent, detect and act.

[Rz 22] In December 2013, the Belgian Federal Cabinet of Prime Minister Elio Di Rupo announced the set up of a Belgian cyber security centre in 2014, responsible for monitoring internet security and «*advising the general public on issues related to online security and cybercrime*».[50] As regards the protection of governmental information systems, the Belgian cyber security centre will be responsible for «*drawing up the standards and security norms that will be applicable to IT systems*

---

43 Belgian Standing Intelligence Agencies Review Committee, «Conclusions and recommendations of the investigation into the way in which the Belgian intelligence services consider the necessity of protecting the information systems against foreign interceptions and cyberattacks», Enquête de contrôle 2007.181. The French version is available at: http://www.comiteri.be/images/pdf/eigen_publicaties/rapport_181_%20fr.pdf.

44 Cyber Security Strategy, 21 November 2012, p. 1. The Dutch version is available at: https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_nl.pdf. The French version is available at: https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_fr.pdf.

45 For an overview of national cybersecurity policies and strategies, see NATO Cooperative Cyber Defence Centre of Excellence. Available at: http://ccdcoe.org/328.html.

46 Cyber Security Strategy, 21 November 2012, p. 9.

47 Telecompaper, « Belgium reserves EUR 10 mln in 2014 budget for cybersecurity», 10 October 2013. Available at: http://www.telecompaper.com/news/belgium-reserves-eur-10-mln-in-2014-budget-for-cybersecurity--972139.

48 Lars Bové, «Di Rupo vergeet miljoenen voor cyberbeveiliging» (Di Rupo forgets millions for cybersecurity), *De Tijd*, 8 May 2014. Available at: http://www.tijd.be/nieuws/politiek_economie_belgie/Di_Rupo_vergeet_miljoenen_voor_cyberbeveiliging.9498802-3136.art?ckc=1.

49 International Chamber of Commerce (ICC) Belgium, FEB, EY, Microsoft, L-SEC, B-CCENTRE & ISASA Belgium, *Belgian cyber security guide. Protect your information*, November 2013. Available at:http://www.penal.org/IMG/pdf/RIDP_2013_1_2_CD_Annexe.pdfhttp://www.iccbelgium.be/images/uploadedfiles/BCSG.pdf.

50 MB, «A cyber security centre for Belgium», *Flandersnews.be*, 20 December 2013. Available at:http://www.deredactie.be/cm/vrtnieuws.english/News/1.1810978http://www.deredactie.be/cm/vrtnieuws.english/News/1.1810978.

used by government bodies»[51] In our views, a Belgian private governmental cloud would provide a solution for unjustified threats to national security and economy posed by the processing and storage of communication outside national territory.[52]

5 Post-Snowden surveillance initiatives

5.1 India

[Rz 23] Post-Snowden, India introduced and continued multiple projects and policies that are focused on cyber security and seek to expand governmental surveillance powers. Indeed, as noted previously, it has been hypothesized that the Snowden revelations has started a «race to the bottom», with the Indian Government seeking to match the surveillance capabilities of the US and implement similar surveillance techniques.[53] Much of this criticism has been directed at the implementation of the Centralized Monitoring System (CMS), a project that started in 2009, and that seeks to automate the process of interception by allowing security agencies, when authorized, to bypass the service provider and directly intercept communications.[54] To enable this, the Department of Telecommunications has amended service providers licensing agreements to provide for the technical capabilities of the project[55], and is also in the process of amending the legal regime through a proposed amendment – section 419B – to the Indian Telegraph Rules 1951, which are rooted in the Indian Telegraph Act 1885.[56]

[Rz 24] In additional moves to expand and centralize surveillance powers for cybersecurity purposes, in June 2013, the Government of India began plans to establish a National Cyber Coordination Centre (NCCC) under the Department of Electronics and Information Technology. News articles have reported on the NCCC's envisioned capabilities stating that «*The NCCC will collect, integrate and scan [Internet] traffic data from different gateway routers of major ISPs at a centralised location for analysis, international gateway traffic and domestic traffic will be aggregated separately ... The NCCC will facilitate real-time assessment of cyber security threats in the country and generate actionable reports/alerts for proactive actions by the concerned agencies*».[57] And in March 2014, according to news items the Department of Telecommunications was seeking a separate security policy for the telecom sector to adequately address the security issues and technical needs that

---

51 Ibid.

52 Gertjan Boulet/Koen Gorissen, «De bescherming van persoonsgegevens in de cloud» (the protection of personal data in the cloud), in *Handboek informatiemanagement*(Manual on Information management), 2013, issue 6, Politeia, pp. 30–31.

53 Andrew North, «NSA Leaks helping India become «Big Brother» State», *BBC*, 31 October 2013. Available at: http://www.bbc.com/news/world-asia-india-24753696.

54 Press Information Bureau, «Government of India. Centralised System to Monitor Communications. Ministry of Communications and Information Technology», 26 November 2009. Available at: http://pib.nic.in/newsite/erelease.aspx?relid=54679.

55 Department of Telecommunications, «Amendment to the UAS License agreement regarding Central Monitoring System», 11 October 2013. Available at: http://www.dot.gov.in/sites/default/files/DOC231013-004.pdf.

56 Kalyan Parbat, «Prepare yourself to be snooped in the interest of national security», 17 December 2013. Available at: http://articles.economictimes.indiatimes.com/2013-12-27/news/45626736_1_indian-telegraph-act-national-security-telecom-department.

57 Sandeep Joshi, «India gets ready to roll out cyber snooping agency», *The Hindu*, 10 June 2013. Available at: http://www.thehindu.com/news/national/india-gets-ready-to-roll-out-cyber-snooping-agency/articl98049.ece.

the telecom sectoris faced with and requires to adequately ensure security.[58]

5.2 Belgium

[Rz 25] The Belgian Law of 13 July 2013[59] and a Royal Decree of 19 September 2013[60] complete the transposition of the EU Data Retention Directive 2006/24/EC[61] into Belgian national law.[62] However, on 8 April 2014, the European Court of Justice declared the Data Retention Directive to be invalid.[63] The judgment will be a key argument for the Flemish and French Human Rights Ligues and other NGOs, which on 25 February 2014 lodged a complaint before the Belgian Constitutional Court to obtain the cancellation of the new Belgian law.[64] Furthermore, the judgement may also be reflected in the current evaluation by the Belgian Privacy Commission on the compatibility of the new Belgian law with its advice of 2009 on the legislative proposals on data retention.[65]

[Rz 26] Noteworthy also is the uncertainty about the application of the Belgian law to foreign based companies. The law firm Lorenz was asked the following question: «*What entities do the data retention requirements apply to? What is the impact on foreign based organisations who provide such services in Belgium?*» Lorenz replied that «*[n]either the Act nor the Royal Decree clearly determine to what extent the data retention requirements apply to companies established abroad. We assume that the obligation is triggered when companies established abroad offer services on the Belgian territory. However, it remains unclear when a company, established abroad, is considered to provide services on*

---

58 Gulveen Aulakh, «Government plans to access your mobile data», *Times of India*,3 March 2014. Available at: http://timesofindia.indiatimes.com/tech/tech-news/telecom/Government-plans-to-access-your-mobile-data/articleshow/31323329.cms.

59 Wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van strafvordering (Law of 30 July 2013 amending Articles 2, 126 and 145 of the Law of 13 June 2005 on electronic communications), *Belgian Official Journal* 23 August 2013. The Dutch version of the law is available at: http://www.bipt.be/public/files/nl/21054/2013_07_30_Loi%20modifiant%20LCE.pdf. The French version of the law is available at: http://www.bipt.be/public/files/fr/21054/2013_07_30_Loi%20modifiant%20LCE.pdf.

60 Koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (Royal Decree of 19 September 2013 executing Article 126 of the Law of 13 June 2005 on electronic communications), *Belgian Official Journal*8 October 2013. The Dutch version of the Royal Decree is available at: http://www.bipt.be/public/files/nl/21058/2013_09_19_Art%20126%20LCE.pdf. The French verson of the Royal Decree is available at: http://www.bipt.be/public/files/fr/21058/2013_09_19_Art%20126%20LCE.pdf.

61 European Parliament and Council of the European Union (2006), Directive 2006/24/ECof the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13 April 2006.

62 DataGuidance, «Belgium: Decree fully transposes Data Retention Directive», 31 October 2013. Available at: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2128; For an overview of the new Belgian Law, see Jan Dhont/David Dumont, «Belgium Introduces Broad Data Retention Obligations». Available at: http://www.lorenz-law.com/wp-content/uploads/Belgium-Introduces-Broad-Data-Retention-Obligations.pdf.

63 European Court of Justice (Grand Chamber), Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12and C-594/12, 8 April 2014. The press release is available here: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

64 Heini Järvinen, «Belgian NGO's challenging the data retention law», EDRi 12 March 2014. Available at: http://edri.org/belgian-ngos-challenging-data-retention-law/.

65 Belgian Privacy Commission, «Adviesaanvraag inzake het voorontwerp van wet en het ontwerp van koninklijk besluit inzake dataretentie, en het ontwerp van koninklijk besluit inzake de medewerkingsplicht (A/09/012)» (Request for advice concerning the proposals for a Law and Royal Decree on data retention, and concerning the proposal for a Royal Decree on the duty to cooperate), Advice nr 20/2009 of 1 July 2009. Available at: http://www.privacycommission.be/sites/privacycommission/files/documents/advies_20_2009_1.pdf.

the Belgian territory».[66]

6 Reflections and conclusions

[Rz 27] Belgium and India are two very distinct contexts politically, legally, and culturally. As such, the two countries have taken different actions post-Snowden – Belgium through a series of inquiries, while India is reforming governmental practices around E-Mail and internet use. Both Indian and Belgium have recognized the significance of having in place robust and comprehensive cyber security policies and practices for its citizens and government. In this context, both countries have indicated (though perhaps to different degrees) that keeping governmental data within its respective jurisdiction is important towards enhancing cybersecurity and protecting the government against cybercrimes. At the same time both countries are considering and implementing surveillance policies and projects that seem to stem from the rationale that greater access to individual's data leads to greater security, similar to the NSA's programs. Furthermore, though both countries have expressed varying of degrees of displeasure in response to the spying conducted by the US Government, neither has taken the information revealed by the Revelations as a cue to review their own state surveillance practices and the impact on citizens and foreigners.

[Rz 28] This is unfortunate as, despite contextual differences, the two jurisdictions should be drawn together by the common goal of ensuring that the rights of citizens are upheld in the context of State surveillance – foreign and domestic. One way to achieve commonality would be to subscribe to the International Principles on the Application of Human Rights to Communications Surveillance. The Principles, developed in 2012–2013, seek to explain how international human rights law applies in the present digital and global environment, and define principles that State led surveillance regimes necessarily need to incorporate to ensure that practices are consistent with human rights.[67]

Gertjan Boulet is a PhD Candidate at the Vrije Universiteit Brussel (Brussels, Belgium). Elonnai Hickok is Programme Manager (Internet Governance) at the Centre for Internet and Society (Bangalore, India).

[66] Jan Dhont/David Dumont, «New Belgian Royal Decree Introducing Broad Data Retention Obligations», interview with Nymity, January 2014, p. 2. Available at: http://www.nymity.com/~/media/Nymity/Files/Interviews/2014/2014-01-dhontdumont.aspx%E2%80%9D.

[67] The Principles are: Legality, Legitimate Aim, Necessity, Adequacy, Proportionality, Competent Judicial Authority, Due Process, User Notification, Transparency, Public Oversight, Integrity of Communications and Systems, Safeguards for International Cooperation, and Safeguards against illegitimate access. The principles can be accessed at: https://en.necessaryandproportionate.org/text.