BALANCE FOR PRIVACY, FREEDOM OF INFORMATION AND NATIONAL SECURITY

Agnes Zaure

Master Student, Department of Public Law, IT-Law Programme, University of Tartu (Estonia), Department of International Law
Naituse 20, 50090 Tartu, EE
Agnes.Zaure@gmail.com

Keywords: ***Cyber security, civil liberties, privacy, national security, freedom of information, surveillance***

Abstract: *This article examines how the continuous escalation of new emerging threats to national security has forced states to re-consider the balance of civil liberties and national security established in international human rights treaties. In the first section, the article reviews reasons for different interpretations of international treaties and implementations of legislation among states. In the second section, the article reveals divergent balances for the privacy, freedom of information and national security between European and American judges and politicians. And in the third section, author discusses on considerations on how to overcome contradicting approaches of balance in the future. In particular, the balance of civil liberties and national security established in international human rights treaties in practice has shifted among states significantly that produced polar dichotomy between judicial, legislative and executive powers and tend to crack existing understanding of democracy and the rule of law.*

«*They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety*.»[1]

Benjamin Franklin

1. Introduction

For the first time in history a democratic society is facing inevitable tension in finding a perfect compromise between the individual's rights online and national security purposes. Widely affirmed principles applicable to the web assume a well-established balance between the conflicting claims, such as the individual's rights and national security. The continuous escalation of new emerging threats to national security has forced states to re-consider the balance of civil liberties and national security established in international human rights treaties and implement number of new rules in order to legalise the increasing volume of security measures online. In international debates between politicians and lawyers a number of questions arise about how these measures adjust to the interpretation of the existing universal human rights treaties. Even though the United Nations (hereinafter UN) Human Rights Council[2] in 2012 affirmed that the human rights are applicable to the Internet as much as offline, the limits of the human rights constraints that favour national security interests were not clarified. As a result, different interpretations of international treaties and, therefore, implementations of legislation and security measures among states emerged with substantially divergent balances for the privacy, freedom of information and national security.

[1] Published in the «Memoirs of the Life and Writings of Benjamin Franklin» in 1818. Attributed to him around February 17, 1775 as he prepared for the Pennsylvania Assembly.

[2] The promotion, protection and enjoyment of human rights on the Internet, UN HRC A/HRC/20/L.13, 29 June 2012.

This article follows the balanced approach rather than the one-sided advocacy of libertarians and authoritarians focusing mainly on the interrelationship of privacy, freedom of information and national security concepts as a complex issue, suggesting that a balanced model for implementing rights and freedoms online is to be found in a systematic analysis of state practice, along with an examination of attitudes among the international community as well as the contingent conceptual integration of all three fields. The reader will be guided to current disputes in order to illustrate the difficulties in striking a fair balance between the conflicting claims related to the collection, storing, and analyzing the records of the private electronic communications from the following perspectives: the right to privacy, in particular, as a protection from extraction of information on individuals and contexts; the freedom of information, as in the right to receive and impart information; and national security, as in the security of nation states against man-made threats.

2. The Dynamics of the Balance

The dynamics of the balance point is affected by the volatile contextual framework of fundamental interests. The terminology of national cyber security entails non-definable nominators which are rapidly changing. The condition of a nation's security is changing in accordance with a government's current role and place, its national and contingent political values,[3] interests and goals, [4] as well as the means and methods preventing and reflecting internal and external threats. The basic organisation and principles of the systems that function to grant national security have additional mutual impact on the changes.[5] The nature of national security as well as nature of security in whole, is never measured, never certain and, always contains contradicting interests between individuals, society and state against external and internal threats.[6] Thus, national security does not have any static character,[7] especially in the cyber sphere. In a similar way, the concept of privacy[8] does not have an overarching definition but and is contained in plurality[9] of different things without a singular essence.[10] Therefore, position of scales favouring security and favouring liberty, that have variable characters, depends on the times[11] and the perception of threats.[12] These instances seem to coincide with times of war or conflict, when a direct threat to the state's political and social order can be readily identified.[13]

3 Andrew Preston, Monsters Everywhere: A Genealogy of National Security, *Diplomatic History*, vol. 38, issue 3, 2014, p. 480.
4 Ibid. p. 484.
5 Strategija nacionalnoj bezopasnosti Rossijskoj Federaciji do 2020 goda ot 12 May 2009, no. 537, http://www.scrf.gov.ru/documents/1/99.html.
6 *Russia's National Security Concept*, 1 January 2000, https://www.armscontrol.org/act/2000_01-02/docjf00.
7 Alexander Klimburg (Ed.), *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE Publication, 2012), p. 9.
8 Ferdinand D. Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, London, New York: Cambridge University Press, 1984), p. 2.
9 Austin Sarat, *A world Without Privacy: What Law Can and Should Do?* (New York, NY: Cambridge University Press, 2015), p. 48.
10 Daniel J. Solove, *Understanding Privacy* (Cambridge, London: Harvard University Press, 2008), p. X.
11 Edward Snowden, Snowden: «The Balance of Power Is Beginning to Shift», 5 June 2015, http://truthinmedia.com/snowden-the-balance-of-power-is-beginning-to-shift/.
12 Megan Warshawsky, The Balance to be found between civil liberties and national security, *The RUSI Journal*, Vol. 158, issue 2, 2013 p. 94.
13 Ibid. p. 95.

Majority of discussions which are usually tilted towards either the state or the individual,[14] create a contest of weights on the scales of democratic society. Even if it seems that the interests of individuals and states are contradictory, both civil liberties and national security can co-exist when on both sides sacrifices of one value (either privacy, freedom of information, or national security) are made in order to create a satisfactory balance. The public must be willing to allow some intrusion by government in order to protect national security's interests when there is a threat present.[15] On the government side, individuals expect an effective model of data management that keeps agencies accountable and the establishment of structural technological changes to Internet architecture with a reducing number of anti-privacy laws. When social agreement on these interests is achieved, mutual beneficial results start to appear: security measures enhance the protection of user's interests, including protection of privacy, in cyberspace, strengthen defences in cyberspace, improve resilience and diminish the impact of cyber attacks.

3. The Contest of Powers

The balance point between privacy, freedom of information and restrictive interests of national security in the light of new emerging cyber threats, determines who has a hold over political, military, and economic power.[16] In 2013 Snowden wrote to Brazilian government that the National Security Agency's (hereinafter NSA) programs were never about terrorism: they were about economic spying, social control and diplomatic manipulation.[17] From an economic point of view, surveillance practices provide insight into other countries' economic policy or behaviour which could affect global markets. A complex and often relatively complete «digital dossier»[18] of individuals can be assembled by private companies as was evidenced in the Apple case when it was caught sharing a year's worth of location data on every user's iPhone with state officials.[19] From a military perspective, the possession of surveillance assets provides the confidence to adequately assess the capabilities of a potential partner over time.[20] And finally, spying on the UN, European Union (hereinafter EU), the European Parliament, the G20 summit, the Vatican, and world leaders is aimed at gaining advantage in diplomatic negotiations.[21] These considerations lead progressive states (United States (hereinafter US), United Kingdom (hereinafter UK), Canada) to admit that there are no better alternatives in the current digitized world to effectively protect country's sovereignty than by advancing defence capacities of information technology and corresponding national legislation.

---

[14] Eneken Tikk-Ringas, Norms for International Peace and Security: Privacy, Freedom of Information and National Security, *ICT4Peace Norms Project*, April 2015, p. 3.

[15] Megan Warshawsky, The Balance to be found between civil liberties and national security, *The RUSI Journal*, Vol. 158, issue 2, p. 94.

[16] Douglas M. McLeod, Dhavan V. Shah, *News Frames and National Security, Covering Big Brother* (New York: Cambridge University Press, 2015), p. 71. Shawn Powers, Michael Jablonski, *The real Cyber War, The Political Economy and Internet Freedom* (Urbana: University of Illinois Press, 2015), p. 75.

[17] Josh Levs, Snowden's open letter offers to help Brazil investigate NSA surveillance, 18 December 2013, http://edition.cnn.com/2013/12/17/world/americas/snowden-nsa-brazil-letter/.

[18] Lauren Gelman, Privacy, Free Speech, and «Blurryedged» Social Networks, *Boston College Law Review*, vol. 50, issue 5, 2009, p. 1316.

[19] «Devices that betray you», *The TechPro Series*, 2014, p. 27.

[20] David W. Kearn, *Great Power Security Cooperation*, *Arms Control and the Challenge of Technological Change* (Lanham: Lexington Books, 2015), p. 27–28.

[21] «These Programs Were Never About Terrorism: They're About Economic Spying, Social Control, and Diplomatic Manipulation. They're About Power», 17 December 2013, http://www.washingtonsblog.com/2013/12/programs-never-terrorism-theyre-economic-spying-social-control-diplomatic-manipulation-theyre-power.html.

A number of technologically advanced countries have already adopted regulations to establish legal base for state practices in order to guarantee national security in a digital society. These laws have raised intense concerns among human rights watchers[22], journalists and academic representatives[23] that highlight internal state conflicts between civil and political individuals. One of the main concerns is about the power that public authorities gain through new technological means as well as their control of an individual's data. In 2001 the US signed the Patriot Act that bypasses the Foreign Intelligence Surveillance Court (hereinafter FISA Court)[24] and allows direct spying through a new NSA electronic surveillance program.[25] In 2014, Russia passed several amendments to its counterterrorism legislation that increased the penalties for, and broadened the definition of terrorist-related crimes.[26] In 2015 the UK adopted the Counter-Terrorism and Security Act with security measures through targeted and effective surveillance, criminal investigations and prosecution.[27] At the same time, the UK[28], like Australia,[29] lacks an impartial safeguards system to ensure against the abuse of such powers.[30] Thus, states have adopted number of counterterrorism legislative measures that focus on the protection of national security and allow states to take over control over personal data of every individual both inside and outside of a state's territory.

Much the same state practice can be seen in other cyber-territorially ambitious countries. In November 2014 France adopted the new counterterrorism law which legalised electronic surveillance by public bodies and increased the sentence to seven years if either offence is committed online. In January 2015 France doubled-down on an existing law that allows the shutdown of websites deemed to be «sympathizing with terror».[31] Many other countries, like Spain, Turkey, Nigeria, and Russia[32] continue to develop surveillance practices in spite of intensive social opposition by journalists[33] and other stakeholders.[34] And, for the complete picture must be mentioned, there are some exceptions in social attitude: 85percent of Chinese citizens support government control and restrictions of internet content.[35] These examples of recently adopted regulations show that counterterrorist laws already cover the European, American, Russian, Asian and Australian territories

22 «Human Rights Organisations Alarmed by Bill That Will Give Surveillance Agencies Dangerous New Powers», 25 March 2015, http://en.rsf.org/france-human-rights-organisations-alarmed-25-03-2015,47728.html.

23 Alan Travis, University professors decry Theresa May's campus anti-terrorism bill, 3 February 2015, http://www.theguardian.com/uk-news/2015/feb/03/professors-letter-protest-counter-terrorism-campuses.

24 David Cole, Reviving the Nixon Doctrine: NSA Spying, the Commander-In-Chief, and Executive Power in the War on Terror, *Georgetown University Law Center*, 2006, p. 3, http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1404&context=facpub.

25 «NSA inspector general report on email and internet data collection under Stellar Wind – full document», 27 June 2013, http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

26 «Country Reports on Terrorism 2014», *United States Department of State Publication* (Bureau of Counterterrorism, 2015), p. 136, http://www.state.gov/documents/organization/239631.pdf.

27 «Counter-Terrorism and Security Act 2015», http://services.parliament.uk/bills/2014-15/counterterrorismandsecurity.html.

28 Andrew Fishman, Glenn Greenwald, Spies Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law, *The Intercept_*, 22 June 2015, https://firstlook.org/theintercept/2015/06/22/gchq-reverse-engineering-warrants/.

29 Nigel Waters, Responding to new challenges to privacy through law reform: a privacy advocate´s perspective, in Normann Witzleb, David Lindsay, Moira Paterson, Sharon Rodrick (eds.), *Emerging challenges in privacy law: comparative perspectives* (Cambridge, United Kingdom: Cambridge University Press, 2014), 2014, p. 54–55.

30 Anthony W. Bradley, Keith D. Ewing, Christopher J. Knight, *Constitutional and Administrative Law*, (16th ed.), (Harlow, England: Pearson, 2015), p. 429.

31 Alessandria Masi, France's Online War on Terror Sympathizers and Extremists Has A New Cyber Security Cell, *International Business Times,* 17 January 2015, http://www.ibtimes.com/frances-online-war-terror-sympathizers-extremists-has-new-cyber-security-cell-1786662.

32 Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, Tightening the Net: Governments Expand Online Controls, *Freedom House*, https://freedomhouse.org/report/freedom-net/2014/tightening-net-governments.

33 2015 World Press Freedom Index, *Reporters Without Borders, For Freedom of Information*, June 2015, http://index.rsf.org/#!/.

34 NSA Surveillance, *Center for Democracy and Technology*, https://cdt.org/campaign/nsa-surveillance/.

35 Shawn M. Powers, Michael Jablonski, *The Real Cyber War, The Political Economy and Internet Freedom* (Urbana: University of Illinois Press, 2015), p. 171.

with the power of control tilted towards public authorities. Therefore, while the legislative and executive state powers of these countries acknowledge the balance of privacy, freedom of information, and national security at the point of enhanced securitization needs, where individual's liberties and rights are forced to give priority to national security interests, they mainly serve the interests of states. The worldwide tendency of adopting surveillance laws is evident in the rapidly growing number of the state practices.[36] Consider these statistics,[37] during the year from May 2013 to May 2014, 41 countries worldwide passed or proposed legislation to penalize legitimate forms of speech online, increase government powers to control content, or expand government surveillance capabilities.[38] Therefore, in the light of the current technological arms race[39] and the growing number of countries,[40] such as Russia, Turkey, Uzbekistan,[41] Nigeria and Vietnam, that implement surveillance practices and adopt respective legislation, there is no reason to believe that states will refuse to employ new surveillance capabilities and practices in the near future.

It is important to mention that the balance between privacy, flow of information, and national security cannot be measured without the operation of secret intelligence agencies, such as M15, GCHQ, CIA, FSB etc., been hidden from public as much as possible and now exposed again to improvements. The fact, that democracies do not have the luxury of focusing all their attention on maximizing internal accountability, instead of safeguard their national security, where intelligence has provided critical support,[42] should be accepted. To assure balanced approach, it is generally accepted among liberal democracies that intelligence services should in theory be subject to law and officials should be accountable for their actions.[43] The relationship between secret intelligence services and democracy that has been addressed by assigning distinct agencies with the responsibility for intelligence collection, should be balanced especially in terms of the degree of public transparency that is appropriate in a world which demands scrutiny, assurances and accountability for organisations.[44] In the current absence of intelligence network agreements,[45] detailed regulation and potential meaningful democratic accountability in oversight within the individual nations' needs,[46] the model of intelligence services performance remains a prerogative of certain state. But one is for certain: the accountability and transparency of secret agencies shall be limited to degree inevitably necessary due to the interests of national security of a specific state.

---

36 See world map of countries under surveillance in 2015: http://en.rsf.org/surveillance-malaysia,36670.html.

37 Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, Tightening the Net: Governments Expand Online Controls, *Freedom House*, https://freedomhouse.org/report/freedom-net/2014/tightening-net-governments.

38 «Freedom on the Net 2014», https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VZ6TPV9Viko.

39 Alexander Nicoll, *Communications interception: UK report seeks legal reform. Strategic Comments* (London: IISS 2015), vol. 21, issue 18, 8 July 2015.

40 See world map of countries under surveillance in 2015: http://en.rsf.org/surveillance-malaysia,36670.html.

41 Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, Tightening the Net: Governments Expand Online Controls, *Freedom House*, https://freedomhouse.org/report/freedom-net/2014/tightening-net-governments.

42 Mike Rettig, Democracy and Intelligence: An Uneasy Working Partnership, *Fair Observer: Make Sense of the World*, 12 March 2013, http://www.fairobserver.com/region/north_america/democracy-intelligence-uneasy-working-partnership/#sthash.kPMckhes.dpuf.

43 Simon Chesterman, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford, New York: Oxford University Press, 2011), p. 57.

44 David Anderson, A Question of Trust, Report of the Investigatory Powers Review, Presented to the Prime Minister on June 2015, p. 190–191.

45 Elizabeth Sepper, Democracy, Human Rights, and Intelligence Sharing, *Texas International Law Journal*, 2010, vol. 46, p. 194, http://www.tilj.org/content/journal/46/num1/Sepper151.pdf.

46 Lars Schall, Intelligence services and democracy, *Asia Times*, 27 November 2013, http://www.atimes.com/atimes/World/WOR-02-271113.html.

4. Global imbalance

While states are striving toward securitizing,[47] courts have pointed, in several decisions, to balanced solutions for states to follow.[48] The regions of case-law examination will be the EU, the US, the UK, and Australia, as territories which are upheld as democracies and are generally lauded for maintaining a commitment to the protection of human rights.[49] They are also countries that have each experienced challenges to their national security as a result of both foreign and domestic terrorism.

For the European region, the European Court of Human Rights (hereinafter ECtHR) case-law emphasizes: both the collection of communications data and the interception of content interfere with art 8 of the European Convention of Human Rights (hereinafter ECHR).[50] In some cases, there are hints in the ECtHR jurisprudence that they may legitimately be treated differently. This way the case-law of the ECtHR suggests that bulk data collection and analysis, in the absence of suspicion, is not in itself a disproportionate interference with the right to respect for private life, but is assessed against a higher standard than individual interferences with the right to privacy.[51] The decisions of the ECtHR illustrate that the EU courts have given priority to national security interests only in those cases where interference with human rights was justified by passing a control «triple» test of necessity, legitimacy and proportionality by means of lawful limitations.[52] The research from 2012 on examination of the data privacy laws revealed, that the «European standard» has exerted an influence in a majority of the world's countries[53], although, it originated from the universal legal standards established in the Universal Declaration of Human Rights (hereinafter UDHR) and in the International Covenant on Civil and Political Rights (hereinafter ICCPR) which follows the same logic of subordination for rights and restrictions, legally binding on all UN Member States. In European case-law, we see that an unlimited mass communication interception is strictly prohibited. Where the judicial balance gives an advantage to human rights with proportional, legitimate and necessary restrictions, the balance established in national counterterrorism laws tends to hold in favour of state interests. Thus, the gap between balances for the legislative, executive and judicial powers emerges, as the political and judicial concepts for the balance of the privacy, freedom of information and national security in Europe differ substantially.

---

47 Jef Huysmans, *Security Unbound, Enacting Democratic Limits* (London; New York: Routledge, Taylor & Francis Group, 2014), p. 126.

48 See also: ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, 28 June 2007; ECtHR, *Shimovolos v. Russia*, no. 30194/09, 21 June 2011; and ECtHR, *Vetter v. France*, no. 59842/00, 31 May 2005.

49 Megan Warshawsky, The Balance to be found between civil liberties and national security, *The RUSI Journal*, Vol. 158, issue 2, pp. 94–99.

50 ECtHR, *Malone v. UK*, no. 8691/79, 26 April 1985, para 84; ECtHR, *Copland v. United Kingdom*, no. 62617/00, 3 April 2007, paras 39–47.

51 David Anderson, A Question of Trust, Report of the Investigatory Powers Review, Presented to the Prime Minister on June 2015, p. 79.

52 ECtHR, *Chauvy and Others v. France*, no.64915/01, 29 September 2004, para. 70; ECtHR, *Pfeifer v. Austria*, no. 12556/03, 15 November 2007, para. 35; and ECtHR, *Polanco Torres and Movilla Polanco v. Spain*, no. 34147/06, 21 September 2010, para. 40.

53 Except for Japan, Bahamas, Vietnam and Chile. See more: Graham Greenleaf, A World Data Privacy Treaty? «Globalisation» and «Modernisation» of Council of Europe Convention 108, in Normann Witzleb, David Lindsay, Moira Paterson, Sharon Rodrick (eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge, United Kingdom: Cambridge University Press, 2014), p. 94–95.

Compared with the European contradictions, the United States current case-law achieved cohesion in its state practice, regulations and judicial overview after the 9/11 accidents[54]. Before that in 1971 the US courts concluded that the threat level did not justify an infringement of the core values of society, such as privacy or freedom of speech[55]. For example, in the *New York Times Co. v. United States*[56] the court ruled that, in attempting to suppress the Pentagon Papers, the government failed to meet the «*heavy burden of showing justification for the imposition of prior judicial restraint*». However, the 9/11 terrorist attacks caused a crucial shift in the balance of privacy, freedom of information, and national security in the US finding, for the first time, full agreement about that balance between the courts, the US Congress and the President. The US judicial concept made a radical shift both in state practice and judicial decisions after terrorist incidents in 2001.[57] These incidents brought the longstanding tension between civil liberties and national security into sharp focus which resulted in the provisions of the USA Patriot Act on 24 October 2001,[58] which was previously turned down by Congress because it eroded civil liberties.[59] The record search provision made it possible for the FBI to secure client records without judicial oversight, and without notification of the person under surveillance. Each of these provisions removes important layers of oversight and accountability for government law enforcement activities.[60] Thus, the US judicial concept of balance moved to the completely opposite side from the previous position and now contradicted the judicial balance set in the EU.

Going even deeper in the analysis, the fact should be mentioned that an apparently coherent US model does not mean that there is an internal consensus between judicial and legislative powers: after a federal appellate court' decision in May 2015 that declared illegal the collection of metadata from every call in and out of the United States, and despite Congress voting to terminate the NSA' bulk telephone metadata surveillance program due to its illegality, the FISA Court, being urged by the government, ruled in June 2015 that the NSA was free to continue with the program.[61]

A similar paradigm shift in the conceptualisation of privacy and national security after 9/11 in 2001 in the US may have resulted for the UK after 7/7 in 2005. Before the terror incidents the case-law of the UK courts (for example, 2001 *R v. Khan*[62] and *Rehman*[63]) was designed to ensure that practices in surveillance were brought into line with the ECHR requirement that the different kinds of surveillance be authorised in advance, the authorisation in some cases requiring judicial approval. The adoption of the new Counter-Terrorism and Security Act 2015 intended to give Britain some of the «toughest powers in the world»[64] against terrorism. Thus, the principle allowing the interception of connection only when it is properly justified within the law, are intensely challenged in the UK. In November 2014 this premise was affirmed by the UK home secretary who addressed her strong view to the courts that the provisions of the Counter-Terrorism and Security Bill

54 Douglas M. McLeod, Dhavan V. Shah, *News Frames and National Security: Covering Big Brother* (New York: Cambridge University Press, 2015), p. 1, 2.

55 Jef Huysmans, *Security Unbound: Enacting Democratic Limits* (London; New York: Routledge, Taylor & Francis Group, 2014), p. 46.

56 US Supreme Court, *New York Times Co. v. United States*, no. 403 U.S. 713, 30 June 1971.

57 Douglas M. McLeod, Dhavan V. Shah, *News Frames and National Security: Covering Big Brother* (New York: Cambridge University Press, 2015), p. 1 and 2.

58 Ibid. p. 44.

59 Ibid. p. 45.

60 Ibid. p. 45.

61 David Kravets, Secret US court allows resumption of bulk phone metadata spying, *ArsTechnica*, 30 June 2015, http://arstechnica.com/tech-policy/2015/06/secret-us-court-allows-resumption-of-bulk-phone-metadata-spying/.

62 ECtHR, *Khan v. UK*, no. 35394/97, 12 May 2001.

63 United Kingdom: House of Lords (Judicial Committee), *Secretary of State for the Home Department v. Rehman (AP)*, [2001] UKHL 47, 11 October 2001.

64 Matthew Holehouse, Counter-terrorism Bill: What it contains, *The Telegraph*, 26 November 2014, http://www.telegraph.co.uk/news/worldnews/islamic-state/11254950/Counter-terrorism-Bill-What-it-contains.html.

were compatible with the ECHR and should be implemented.[65] On 5th December 2014 the Investigatory Powers Tribunal (hereinafter IPT) in *Liberty & Others v. the Security Service, SIS, GCHQ*[66] has ruled that Britain's legal regime governing mass surveillance of the internet by intelligence agencies does not violate human rights.[67] The case was appealed to the ECtHR and is awaiting judgment.[68] Another pending case before the ECtHR is the case of *Big Brother Watch v. UK*[69] that concerns bulk data collection and data sharing. The ECtHR will be called upon to determine the issue that collection is of itself an intrusion into privacy which requires careful justification and, in law, a proportionality analysis and provide the final word on the matter.[70] These recent applications represent the view that the balance of privacy, freedom of information and national security that is, present in US, has already taken place in UK case-law. Therefore, the upcoming decisions of the ECtHR will show the results of the cross-continental battle between legislative and executive powers with judicial ones.

Thus, the present dichotomy of concepts for the balance between executive and judicial powers in Europe cracks the existing framework of the European democracy. The justification by states for receding from the universal treaty requirements is the idea that, apart from its questionable ability to adjust to modern-day threats to national security, the UDHR is not legally binding and that the signatories of the ICCPR who had an «unprecedented number of reservations, understanding, and declarations» rendered the treaty powerless under domestic law.[71] Another reason is, that for states as rational egoists, the «costs of strict adherence to the UN Charter in a world of new security threats» has just become too great.[72] This way, the grave differences between state practices and the international human rights treaties, which sustained at least surface peace, reflect the enormous imbalance between national executive, legislative and judicial powers, and jeopardize the present rule of law.

5. Solution Perspectives

The way the technologies and data flows are shaped will have far-reaching effects for the social structures of the digital societies of the future. It is noticeable that the limits of obligations taken by states with international human rights instruments in the context of the new massive technological developments are undetermined. In 2013 the UN General Assembly filled the gap by issuing a resolution[73] that called upon states to end privacy violations and prevent further privacy incursions. Still, in the absence of formal guidelines, the British report «A Question of Trust» on interception of communications[74] by David Anderson is aimed at convinc-

65 Home Secretary Theresa May on counter-terrorism, 24 November 2014, *Royal United Services Institute*, https://www.gov.uk/government/speeches/home-secretary-theresa-may-on-counter-terrorism.

66 Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, [2014] UKIPTrib 13_77-H, 5 December 2014.

67 GCHQ does not breach human rights, judges rule, *BBC News*, 5 December 2014, http://www.bbc.co.uk/news/uk-30345801.

68 ECtHR, *10 Human Rights Organisations v. United Kingdom*, an application filed on 10 April 2015.

69 ECtHR, *Big Brother Watch and others v. United Kingdom*, no. 58170/13, lodged on 4 September 2013.

70 David Anderson, A Question of Trust, Report of the Investigatory Powers Review, Presented to the Prime Minister on June 2015, p. 224, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

71 Amitai Etzioni, *The New Normal: Finding a Balance Between Individual Rights and the Common Good* (New Brunswick (U.S.A.): Transaction Publishers, 2015), p. 62. See also: William A. Schabas, Invalid Reservations to the International Covenant on Civil and Political Rights: Is the United States Still a Party?, *Brooklyn Journal of International Law,* no. 21, 1995, p. 277, 280. Kristina Ash, U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence, *Northwestern Journal of International Human Rights*, 2005.

72 Martti Koskenniemi, Formalism, Fragmentation, Freedom: Kantian Themes in Today's International Law, *No Foundations. Journal of Extreme Legal Positivism*, 2007, p. 17.

73 The right to privacy in the digital age, Brazil and Germany: draft resolution, UNGA A/C.3/68/L.45. See also The right to privacy in the digital age, UNGA A/RES/68/167.

74 Alexander Nicoll, *Communications interception: UK report seeks legal reform. Strategic Comments* (London: IISS 2015), vol. 21, issue 18, 8 July 2015.

ing that the UK practice does not appear to contravene to the ECHR. To promote his argument he expressed that balance must be found between retaining the secrecy of operational tools and methods on the one hand, and, on the other, having a law that is «sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions under which public authorities will access their communications».[75] However, the onus is on governments to demonstrate a practical and effective standard for the future.

It appears more probable that the one and only global model of balance cannot be achieved and constructed due to conceptual contradictions for states that fragment parts of the world, such as, for example, US, China, Iraq, and Germany, who's political aims and technical capabilities are not coherent. In 2011 between contradicting approaches of the US and Russia, Germany took a mediating role on the idea of a universal cyber convention, that codifies reasonable standards of state behaviour, and expressed support for formulating a codex that would guide government actions in cyberspace.[76] On the other hand, in 2013 as a response to the NSA spying revelations, Brazil adopted the *marco civil* with provisions for net neutrality, privacy protection, open government, data storage guidelines and guarantees that platform providers should not be held liable for user content.[77] So far, Brazil has been an example of state who was willing to save its political autonomy and protect human rights according to the human rights treaties in digital sphere as well. Therefore, states group into territorial collective unities with homogeneous solutions to handle new threats.

6. Conclusion

The balance point between privacy, freedom of information and national security is under reconsideration by international society which is reviewing the legal grounds for protecting national security and human rights agreed globally after the World War II. Partners of international agreements stand at the cross-road of decision whether it is possible to continue with the balance model according to the existing universal treaties or the «new normal» standard is to be introduced.

After an inclusive and multi-pronged analysis of the matter, it is revealed that terrorist attacks during last decade have intensified implementation of security measures online and escalated adopting surveillance laws by states in order to guarantee national security in a digital society. The absence of a shared vision on the future of legitimate limitations of the human rights produced polar dichotomy between judicial, legislative and executive powers among states. The balance for privacy, freedom of information and national security in US has shifted after changes of state's practice and judicial concepts. Similar tendencies are followed for the rest digitally advanced states in Europe, Asia, Canada, Russia and Australia. Intensified implementation of security measures online and laws crack existing understanding of democracy and the rule of law.

Applications has been put before international courts to give interpretation of the existing universal human rights treaties for countries to implement international treaties and provided with balanced guidance on security measures. Deep continental controversy on fundamental concepts of legitimate justifications on limitation of human rights and national security protection demands prevent states agree on one global working model for balance, instead they would rather continue to cooperate through international fragmented unities to be able to handle new threats in even more efficient manner.

---

[75] David Anderson, A Question of Trust, Report of the Investigatory Powers Review, Presented to the Prime Minister on June 2015, p. 75.

[76] Annegret Bendiek, *European Cyber Security Policy* (Berlin: SWP Research Paper, October 2012), p. 15.

[77] Jonathan Watts, Brazil to legislate on online civil rights following Snowden revelations, *The Guardian*, 1 November 2013, http://www.theguardian.com/world/2013/nov/01/brazil-legislate-online-civil-rights-snowden.

7. Acknowledgements

This research was granted by ICT4Peace Norms Project. The author is grateful to the International Institute for Strategic Studies in London for interviews and remarks on the draft text. The author deeply appreciates the substantive and financial support provided by Dr. iur. Eneken Tikk-Ringas and Dr. Mika Kerttunen. The model for approach of the article originates from research papers[78] issued by ICT4Peace Norms Project for Hague Global Conference on Cyberspace.

[78] Eneken Tikk-Ringas, Norms for International Peace and Security: Privacy, Freedom of Information and National Security, *ICT4Peace Norms Project*, April 2015, p. 3. See also: Eneken Tikk-Ringas, Comprehensive Normative Approach to Cyber Security, *ICT4Peace Norms Project*, April 2015.