Groningen Journal of International Law, vol 2(2): Privacy in International Law

USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining?

Joanna Kulesza*

DOI: 10.21827/5a86a837b18b9

Keywords
PRIVACY; HUMAN RIGHTS; INTERNET GOVERNANCE; DUE DILIGENCE; JURISDICTION

Abstract
The paper covers the political and legal consequences of US deployed extensive cyber surveillance program, usually referred to with the codename PRISM. The author identifies the significant transnational legal challenges for privacy protection originated by US cybersecurity policy and the steps taken by other states aimed at limiting its consequences harmful to individual privacy. The author covers varying reactions to US-imposed privacy intrusions, from Brazil's plans to withdraw from the global network to some states' suggestions of holding Washington internationally responsible for violating the International Covenant on Civil and Political Rights. The paper's focus however is on the European personal data protection thus far not providing effective transnational protection of privacy, primarily through the strongly criticised and ineffective EU-US Safe Harbor arrangement. The EU personal data reform, approved by the European Parliament in March of 2014, seems the most significant consequence of mass privacy violations committed by the US National Security Agency and its agents.

The 2012 proposed Data Protection Regulation, which, together with the new personal data Directive**,** are to replace the 1995 Data Protection Directive 95/46/EC put strong emphasis on the effectiveness of transboundary privacy protection, although cover also many other significant changes, such as introducing the right to be forgotten or centralising the personal data protection decisions thus-far distributed among national Data Protection Authorities, often varying in their interpretations of community law. The reform is to oblige all companies, regardless of their country of incorporation, to meet EU privacy laws as it introduces high financial responsibility for those who fail to do so, making it a trigger for a significant change in the way the online markets operate.

The European approach seems significant for the entire international community not only because European citizens are an important element of the online markets, but also because personal data protection as a tool for safeguarding individual privacy has been adopted in over 100 out of the roughly 190 world's countries. Including an element of transnational data protection in EU law is therefore certain to influence the approach to privacy in other continents.

I. Introduction

The paper covers the political and legal consequences of US-deployed extensive cyber surveillance, usually referred to as PRISM. The author identifies the significant transnational legal challenges to privacy protection originated by US national security

* Joanna Kulesza, Assistant Professor of Public International Law, University of Lodz, Poland.

policy and steps taken by other States aimed at limiting its consequences for individual privacy right. The paper discusses varying reactions to US-imposed privacy intrusions, from Brazil's plans to withdraw from the global network to suggestions of holding Washington internationally responsible for violating the International Covenant on Civil and Political Rights and the universal human right to individual privacy. The paper's focus is on the European personal data protection laws thus far not providing effective transnational privacy protection, primarily through the strongly criticised and ineffective EU-US Safe Harbor arrangement. The EU personal data reform, approved by the European Parliament in March 2014, seems the most significant consequence of mass privacy violations by the US National Security Agency (NSA) and its agents. Focal to the reform, the 2012 proposed General Data Protection Regulation (GDPR) puts strong emphasis on the effectiveness of transboundary privacy protection. The reform aims to oblige all companies operating on EU citizens' data, regardless of their country of incorporation, to meet EU privacy laws.

This paper is an attempt to verify how effective the new EU regime is in resisting US cyber surveillance attempts. The author covers the personal data protection derogations included in the GDPR and turns to existing international business law standards as catering for the need to enforce universal privacy safeguards.

II. US "Signals Intelligence" Laws—the Origins of the Problem

Sixth of June 2013 was the day that proved conspiracy theorists right. Simultaneous publications by the New York Times, The Guardian and Der Spiegel on secret US surveillance programs disclosed multiannual and versatile electronic espionage of domestic and foreign individuals by the NSA.[1] The publications were based on top secret information, revealed to the journals by an ex-NSA contractor, Edward Snowden and proved the validity of long-lasting suspicions of US running its unique Panopticon,[2] operating under the code name PRISM, an abbreviation originally used by the NSA for its Planning Tool for Resource Integration, Synchronization, and Management.[3] It describes the use of three key surveillance programs, all serving the same purpose of collecting and automatically synthesising information about users of telecommunication services, including those obtained from Internet service providers. While UPSTREAM

---

1 Washington Post, Gellman, B. and Poitras, L., *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, 7 June 2013, available online at <washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html> (accessed 28 October 2014); The Guardian, Greenwald, G. and MacAskill, E., *NSA Prism program taps in to user data of Apple, Google and others*, 7 June 2013, available online at at <theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (accessed 27 October 2014).

2 The term Panopticon was first used by 18th century English philosopher Jeremy Bentham to describe a prison building whose architecture would enable one-man surveillance of all inmates without them being aware of being watched at a given time. The very possibility of being watched resulted in inmates obeying the rules of the facility, not wanting to risk punishment. With time the term came to signify comprehensive, secret surveillance imposed by authorities.

3 The 2013 publications confirmed previous information on US cyber surveillance, provided by whistleblowers in 2005, see, e.g., New York Times, Risen, J. and Lichtblau E., *Bush Lets US Spy on Callers Without Courts*, 16 December 2005, available online at <nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0> (accessed 27 October 2014).

was the program used for collecting data from public and private networks through international fiber-optic connections and Internet Exchange Points, the XKeyscore was an analytic system for buffering and retaining data from hundreds of websites and servers around the world while combining it with data from other sources, such as diplomatic and intelligence resources at US's disposal.[4] Its key function was to index such information using IP or e-mail addresses, phone numbers, cookies, usernames, search terms or location data as well as metadata retained by websites.[5] Finally, BULLRUN was used to break encryption safeguarding data stored on resources reached by the two other programs through, for example, backdoors installed in software and hardware delivered by companies operating under NSA contracts.

Those three tools have technically enabled the NSA to obtain, store and analyse information on US nationals and foreigners. The legal basis for their operation was the Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008,[6] which enhanced the powers granted to the NSA by the 2001 USA PATRIOT Act.[7] When discussing the FISAA, two elements of the unique US perception of the right to privacy must be mentioned: lack of privacy protection for data provided to the government by third parties, such as banks or telecommunication companies (the so-called third party doctrine) and the varied approach to the protection of US citizens as compared with "non-US persons", whose data was unprotected by US law. The right to privacy is granted to all US citizens in the Fourth Amendment to the US Constitution and warrants them freedom from 'unreasonable searches and seizures' making any privacy invasion subject to a judicial warrant issued upon 'a probable cause, describing the place to be searched'.[8] As per 1970s US case law, this protection does not apply to private information about an individual obtained not directly from him, but from a third party, such as a bank or a telecommunication company (third party doctrine).[9] This derogation of privacy protection was extended by the already mentioned 2001 USA PATRIOT Act, which allowed security authorities to access companies' business records. After numerous protests from civil society and privacy activists USA PATRIOT Act was amended in 2006 to allegedly limit such privacy interferences, covering access to only "relevant" information. This broad interpretative clause however proved ineffective, especially with the introduction of the 2008 FISAA. Further derogations resulted from section 702 FISAA, allowing the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Court of Review (FISCR) the discretion in interpreting the Act, and deciding on what "relevant" information is. The scope of such information was set very broadly, as based on the "three hops" rule (more recently limited to "two

---

4 European Parliament, Bowden, C., The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and Their Impact on EU Citizens' Fundamental Rights, 2013, available online at <europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf> (accessed 27 October 2014) (EP 2013).

5 *Id.*, 14.

6 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304, United States of America, 10 July 2008, Chapter 36 Section 1801 *et seq*., available online at <congress.gov/110/plaws/publ261/PLAW-110publ261.pdf> (accessed 27 October 2014) (FISAA).

7 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law 107-56, 115 Stat. 277, United States of America, 26 October 2014, available online at <gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf> (accessed 27 October 2014) (USA PATRIOT Act)

8 The Constitution of the United States, Amendment IV, available online at <constitutioncenter.org/media/files/constitution.pdf> (accessed 27 October 2014).

9 See, e.g., the recent case of *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012).

hops").[10] As per an NSA representative's explanation, the decision on whether data relating to a certain individual is to be collected depends on the possibility to link his telephone number with other numbers connected with a terrorist activity within "three hops". This connection is made based upon the definition of "foreign intelligence information", subject to NSA's inspection. The FISAA definition of such information covers all information relating to, and if concerning a United States person, necessary for the United States to protect itself against foreign attacks or "hostile acts", sabotage, terrorism, proliferation of weapons of mass destruction or clandestine intelligence activities.[11] It also covers 'information with respect to a foreign power or foreign territory' relating to or, if concerning a US person, 'necessary for the purpose of' national defense, protecting US security or conducting foreign affairs of the US. Such a definition clearly indicates two groups of subjects regarding whom information may be processed, giving weaker protection to "non-US persons", while no definition of a "US person" is to be found within the FISAA. As per the explanations provided by the NSA, the constitutional privacy protection is understood to be granted only to US citizens.[12] While their information is to be collected only when "necessary" for the purposes of US security and foreign policy, data on non-citizens can be compiled and analysed when it only "relates to" those, very broadly designed, terms. The decisions on the relevance of such data are made by the NSA and require judicial oversight only when referring to "US persons". There is no judicial supervision requirement for accessing the information of non-US persons, since neither FISAA nor the US Constitution is applicable to them. As explained by NSA and confirmed by the FISC the national guarantees were applied only to those covered by US law, while none of its acts provide for any protection of foreign individuals.[13] As explained in detail below, the US does not recognise the direct applicability of international treaties, binding upon them and constituting such a right. Should the individual under surveillance be a US citizen, a court order for their surveillance would be issued. Such an order, directed at a service provider, required them to promptly provide to US authorities 'all information, facilities, or assistance', including not just traffic data or communication content, but also cryptographic tools used to safeguard individual communication.[14] A year after the PRISM revelation and despite some presidential actions, such as the Presidential Policy Directive/PPD-28, extending minimal safeguards onto non-US citizens, the protection granted to them is still nowhere near sufficient.[15] Effectively FISAA allows the NSA to intercept "non-US persons" communications without judicial oversight or a right to obtain information about their data being collected, even though the right to privacy, recognised within international human rights law, its treaties and customary practice, discussed in detail below, disallows for any blanket surveillance and unjustified invasions of privacy.

---

[10] The Guardian, Timm, T., *The House's NSA bill could allow more spying than ever. You call this reform?*, 25 March 2014, available online at <theguardian.com/commentisfree/2014/mar/25/house-nsa-bill-end-bulk-collection-act-reform> (accessed 27 October 2014).

[11] Section 702 FISAA.

[12] CBS News, Trowbridge, A., *NSA spying: Ally anger justified?*, 3 July 2013, available online at <cbsnews.com/news/nsa-spying-ally-anger-justified/> (accessed 27 October 2014).

[13] *Ibid*.

[14] Section 702 FISAA.

[15] The White House, *Presidential Policy Directive – Signals Intelligence Activities*, 17 January 2014, available online at <whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (accessed 27 October 2014).

III. PRISM and International Law—Has US Violated the Human Right to Privacy? And with What Consequences?

The first document of international human rights law is the 1948 Universal Declaration on Human Rights.[16] This non-binding compromise was easy to achieve just a few years after the greatest horrors in human history unfolded on the frontlines of World War II. Yet completing a binding treaty, expressing the very same ideals, took the international community almost twenty more years, as States agreeing on the notions of individual rights, such as privacy, free speech or property, saw differently the scope and implementation of each of them. The 1966 International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ICESCR) introduced hard law obligations for different categories of innate human liberties, leaving the detailing of each of them up to State practice and international jurisprudence.[17] Privacy holds a well-established place in the human rights catalogue, with Article 12 UDHR and Article 17 ICCPR granting every individual freedom from 'arbitrary interference' with their 'privacy, family, home or correspondence' as well as from any 'attacks upon his honor and reputation', placing privacy among the catalogue of personal rights known to every national legal system, yet perceived differently. While the very term "privacy" is not defined within the convention, the UN Human Rights Committee (HRC) provided detailed guidelines on the scope of privacy protected by international law, in particular when discussing the thin line with State sovereignty, security and surveillance.[18]

As per international law, confirmed by the interpretations and jurisprudence accompanying the ICCPR, privacy right must be safeguarded with national laws protecting individuals from 'arbitrary or unlawful' interferences or attacks upon it.[19] National authorities are therefore obliged to set limits on privacy invasions executed by themselves or third parties, although the two crucial human rights document differ by one significant element, defining it. The non-binding UDHR includes a limitative clause for all rights contained therein, in Article 29 paragraph 2 it surrenders the exercise of all rights and freedoms subject to limitations determined by law 'solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society'. The ICCPR includes no such general restraint, nor one aimed directly at privacy, even though it does contain explicit limitations on other freedoms, such as the one in Article 19 paragraph 2, referring to the freedom of expression. The latter

---

[16] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, UNGA Res 217 A (III), (UDHR).

[17] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, 999 UNTS 171 (ICCPR); UN General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, 993 UNTS 3 (ICESCR).

[18] The Human Rights Committee (HRC) ought to be distinguished from the United Nations Human Rights Council (UNHRC) and the Commission on Human Rights. According to Article 28 of the ICCPR, the HRC consists of eighteen members, nationals of the States parties with recognised competence in the field of human rights and legal experience, who monitor the implementation of the ICCPR by its State parties. On the other hand the UNHRC is an inter-governmental body subsidiary of the UN General Assembly. It collaborates with the Office of the High Commissioner for Human Rights and aides the United Nations' engagement in special procedures. In 2006 the UNHRC replaced the United Nations Commission on Human Rights which carried similar functions.

[19] Article 12 UDHR; Article 17 ICCPR.

introduced a standardised three-steps test, which, even though its wording might be considered vague, sets minimal standards required from State parties agreeing to grant its subjects freedom of thought and communication.[20] Despite the fact however that Article 17 ICCPR is not accompanied by a limitative clause, the right to privacy is not to be considered an absolute one. As per the ICCPR practice and the HRC interpretations privacy may be subject to legal limitations as long as those meet the general standards present in human rights law and similar international treaties, just to mention Article 8 of the European Convention on Human Rights (ECHR),[21] which allows to restrict individual privacy with laws necessary in a democratic society for the protection of rights and freedoms of others.

The HRC confirmed this interpretation on various occasions, among which the 1988 General Comment No. 16 is most significant, as it paved the way for further elucidations.[22] Back in 1988, before the peak of the communications revolution brought about by the Internet,[23] the HRC stated that as per existing human rights norms, '[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited'.[24] It also approved the applicability of the general three-step test, recognised by the UDHR, for the right to privacy, granted by Article 17 ICCPR.[25] And so, the three steps test, as per this general human rights standard means that any limitation upon an individual right must be based on an act of law,[26] which ought to describe in detail the precise circumstances when privacy may be limited by authorities or third parties. The HRC specified that a decision on whether private information about an individual may be obtained must be made on a 'case-by-case basis',[27] emphasising that 'even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and reasonable in the particular circumstances', where "reasonable" means justified by those particular circumstances.[28] Moreover, not only does international law lay upon States the obligation to refrain from unjustified invasions of privacy, but it also includes their positive duty to protect individuals within their

---

[20] The three steps test means that any limitation upon an individual right must be based on an act of law, needs to be necessary in a democratic society and justified by one of the reasons named in the ICCPR, which include the protection of public order or the rights and freedoms of others.

[21] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, CETS 005 (ECHR).

[22] UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available online at <tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en> (accessed 24 November 2014).

[23] In 1991 the US National Science Foundation, funding the "Internet" research project allowed for setting up of the Commercial Internet eXchange (CIX), making the up-till-then purely academic network open to commercial use. The very same year the European Organization for Nuclear Research (CERN) introduced its "world wide web" protocol, significantly enhancing the commercial value of the network by making its operation more user-friendly. See Office of the Inspector General, National Science Foundation, *Review of NSFNET,* 1993, available online at <nsf.gov/pubs/stis1993/oig9301/oig9301.txt> (accessed 27 October 2014).

[24] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 28 December 2009, UN Doc. A/HRC/13/37 (A/HRC/13/37), 2.

[25] See above nt. 20.

[26] Human Rights Council, *supra* nt. 24, pt. 3, 1.

[27] *Id.*, pt. 8, 2.

[28] *Id.*, pt. 4, 1.

jurisdiction from privacy invasions committed by third parties by taking active steps to identify and mitigates such threats. The HRC emphasises that 'Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it'.[29]

As international espionage increased with the rising popularity of online communications and expanding war on terrorism, the HRC followed the initial 1988 General Comment with documents identifying and describing the interception of privacy and State security. In a 2009 report on the promotion and protection of human rights and fundamental freedoms and terrorism, it discussed the complicated equilibrium of State security and individual privacy.[30] According to the report, Article 17 ICCPR ought to be understood as allowing for 'necessary, legitimate and proportionate restrictions to the right to privacy' subject to 'a permissible limitations test'.[31] This test requires State authorities to 'justify why a particular aim is a legitimate justification for restrictions upon Article 17',[32] while identifying seven criteria of any such derogation. Consequently, a State may restrict individual privacy if such a restriction is 1) based on a provision of law; 2) does not interfere with the essence of the right; 3) is necessary in a democratic society; 4) is not subject to unfettered discretion; 5) is necessary to reach (rather than just aim at) one of those legitimate aims; 6) is proportionate; and 7) consistent with other ICCPR rights.[33] The HRC points to 6 principles which ought to guide best practice of any State when enforcing privacy restrictions. Those principles include 1) the principle of minimal intrusiveness, requiring States to ensure they have 'exhausted less-intrusive techniques before resorting to others';[34] 2) a data-minimisation principle, opting to refrain from obtaining information not necessary to meet a legitimate aim, even if it is technically possible to do so;[35] 3) the principle of purpose specification restricting secondary use, which declares the need to legally ensure data usage solely for the purposes for which they were initially gathered;[36] 4) the principle of oversight and regulated authorisation of lawful access, requiring States to ensure effective safeguards for the supervision of entities collecting and processing data;[37] 5) the principle of transparency and integrity, opting for openness and communication among States on their surveillance practices, and granting individuals the right to access information about themselves which has been collected by private and public bodies;[38] and 6) the effective modernisation principle, which encourages enhancing legislative and technological measures aimed at securing privacy, which include privacy impact assessments.[39]

---

29 *Id.*, pt. 10, 2–3.
30 A/HRC/13/37, *supra* nt. 24.
31 *Id.*, 2.
32 *Id.*, 1.
33 *Id.*, para. 17.
34 *Id.*, para. 49.
35 *Ibid*.
36 *Id.*, para 50.
37 *Id.*, paras. 51–53.
38 *Id.*, paras. 54–55.
39 *Id.*, para. 57. Privacy impact assessments were recently introduced as an obligatory security measure ensuring privacy within the EU data protection reform, discussed below. For a detailed discussion on privacy and other human rights protection in the age of the information society see: The Jean Monet Center for International and Economic Law and Justice, Kulesza, J., *Protecting Human Rights Online - an Obligation of Due Diligence*, Jean Monnet Working Paper Series, 2014, available online at <jeanmonnetprogram.org/papers/papers14.html> (forthcoming).

The author of this 2009 HRC report, Martin Scheinin, given his expertise in the area, was asked to assess the US surveillance programs for the European Parliament once the Snowden revelations were published. In a 2013 statement for the European Parliament, he repeated his arguments on the validity of a universal human right to privacy subject to strict limitations, arguing that the US violated its international obligations and the right to individual privacy granted by Article 17 ICCPR of all those whose communications were intercepted by the NSA without judicial supervision.[40] He claims that

> the United States … have been involved, and continue to be involved, in activities that are in violation of their legally binding obligations under the International Covenant on Civil and Political Rights of 1966. … It includes a specific provision that prohibits unlawful or arbitrary interference with anyone's privacy[41]

emphasising the use of the term in the very text of the Covenant. He argues for an international complaint to be filed against the USA by other ICCPR member States as per Article 41 ICCPR (discussed in more detail in the following paragraph).

Martin Scheinin's interpretation, reflecting the European understanding of privacy, and strongly rooted in the HRC interpretation of Article 17 ICCPR, is, however, opposed by the US and international lawyers that support the US understanding of privacy. Eric A. Posner argues that no right to privacy can be identified in contemporary international law, hence no State or authority may be required to respect it, as the term is too ambiguous to carry any legal obligation. On the other hand national sovereignty carries with it an inherent "right to surveillance" granted to each State and exercised by authorities in European, American or Asian States alike.[42]

As much as the latter opinion seems unjustified in the light of the HRC body of work, it is a good reflection of the US perspective on privacy and its limits. Hence, it must be assessed that, while in Europe the right to privacy (as a universal standard defined by the HRC) raises no controversy, other legal cultures, as represented by the US, view the issue differently, regardless of whether their motivation is dogmatic, academic or a purely political one.

IV. Enforcing International Privacy Standards—Is International Human Rights Law Binding to the US?

Assuming that the HRC work serves as a litmus test on the existence of a human right to privacy, its scope and limits, one could credibly state that, through the implementation of the PRISM program, the US has violated international law. Such an assessment was confirmed by the HCR in its 2014 observations to US periodic review report.[43] Since the

---

[40] European Parliament, Scheinin, M., *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens*, 14 October 2013, available online at <europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf> (accessed 24 September 2014) (LIBE Committee Inquiry statement).

[41] *Ibid*.

[42] Privacy & Civil Liberties Oversight Board, Posner, E. A., *Statement to the Privacy & Civil Liberties Oversight Board*, 14 March 2014, available online at <pclob.gov/Library/20140319-Testimony-Posner.pdf> (accessed 24 September 2014).

[43] OHCHR, Human Rights Committee, *Concluding observations on the fourth periodic report of the United States of America (HRC Observations)*, 23 April 2014, available online at

ICCPR is an international treaty, for its effectiveness, it requires ratification by a sovereign State, stating its willingness to give up parts of its sovereignty for the good of international cooperation. The US consented to such compromise when, in 1992, it ratified the ICCPR, adhering to the obligations and goals set in the treaty, yet having made significant reservations, limiting its effectiveness. The reservations, presented upon the ratification of the ICCPR, include, for example: denying the ICCPR a self-executing character, which effectively deprives all individuals under US jurisdiction of the possibility to demand protection for the rights named in the ICCPR directly from US authorities, unless such rights are reflected in national law.[44] The only obligation that the US did take upon itself, when it comes to meeting the ICCPR goals, is to implement the treaty through federal government, as well as State and local governments, making it their best efforts obligation to 'take appropriate measures for the fulfilment of the Covenant'.[45] Effectively, a right granted by the ICCPR and detailed by international jurisprudence and State practice, such as the right to privacy, named in Article 17 ICCPR, is not executable in the US, unless provided for by national law.

Moreover, although in its jurisdiction, the US denies the applicability of the ICCPR rights to individuals outside its territory, as noted by the HRC, such practice is contrary to the interpretation of Article 2 paragraph 1 ICCPR 'supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and State practice'.[46] The practice of affording also foreign individuals active privacy protection confirmed by the HRC serves as evidence for customary human rights law and is binding upon the US, despite the ICCPR reservations. The lack of recognition of individual rights granted by the ICCPR to non-US residents, whether those detained in Guantanamo or those under surveillance in Europe, is clearly in breach of well-established international law and practice.[47] The HRC's observations cover therefore the need for the US to 'interpret the Covenant in good faith, in accordance with the ordinary meaning to be given to its terms in their context, including subsequent practice, and in the light of the object and purpose of the Covenant, and review its legal position'.[48]

The HRC also addresses the non-self-executing reservation, calling upon the US to ensure 'effective remedies' against violations of the Covenant,

> including those that do not, at the same time, constitute violations of the domestic law of the United States of America, and undertake a review of such areas with a view to proposing to Congress implementing legislation to fill any legislative gaps,

eventually recommending the US to withdraw its reservations.[49] It is therefore clear that, according to the HRC, the US remains in violation of its international obligations as set within the ICCPR to which the US acceded in 1992. Moreover, the reservations might be

---

<tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en> (24 September 2014) (HRC Observations).

44 University of Minnesota, *US reservations, declarations and understandings, International Covenant on Civil and Political Rights*, 2 April 1992, pt. III(1), available online at <umn.edu/humanrts/usdocs/usres.html> (accessed 23 September 2014)

45 *Id.*, pt. II(5).

46 HRC Observations, *supra* nt. 43, pt. C.4, 2.

47 *Id.*, pt. C.4(a)–(c), 2.

48 *Id.*, pt. C.4(a), 2.

49 *Id.*, pt. C.4(c)–(d), 2.

considered as contrary to the very aim and scope of the convention and therefore inadmissible as per the law of treaties.[50]

In its observations on the US periodic report, the HRC directly addressed the privacy concerns raised by NSA.[51] Referring to the implementation of Section 215 of the USA PATRIOT Act and, 'in particular, surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act' it addressed their 'adverse impact on individuals' right to privacy'.[52] According to the HRC, the 'current oversight system of the activities of the NSA fails to effectively protect the rights of the persons affected' and the overall US practice grants persons affected by it 'no access to effective remedies in case of abuse'—a right well recognised by the ICCPR in Articles 2, 5(1) and 17.[53] The HRC therefore recommends that the US 'take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17'.[54] It refers directly to its body of work on Article 17 ICCPR, naming the need to introduce measures ensuring legality, proportionality and necessity of any privacy limitation, 'regardless of the nationality or location of the individuals whose communications are under direct surveillance'.[55] To meet that requirement, the US is directly obliged to ensure that any interference with the right to privacy or correspondence

> is authorised by laws that are
>
> (i) are publicly accessible;
>
> (ii) contain provisions that ensure that collection of, access to and use of communication s data are tailored to specific legitimate aims;
>
> (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorisation, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and
>
> (iv) provide for effective safeguards against abuse.[56]

Moreover, the HRC requires the US to reform its current oversight of the surveillance programs, ensuring its effectiveness. The US should therefore provide for 'strong and independent' judicial oversight over the authorising or monitoring of surveillance measures, to prevent abuses.[57] The 2014 Presidential Policy Directive PPD-28 fails to

---

[50] See Vienna Convention on the Law of Treaties, 1969, 1155 UNTS 331, Article 19, indicating that a State may formulate a reservation to a treaty unless 'the reservation is incompatible with the object and purpose of the treaty'. The convention does not however foresee a procedure of assessing which reservations are to be considered contrary thereto, leaving it up to the contracting States to hold other State parties to their obligations set per each treaty, as provided for by general international law norms.

[51] HRC Observations, *supra* nt. 40, pt. 22, 9.

[52] *Ibid*.

[53] *Id.*, pt. 22, 9–10.

[54] *Id.*, pt. 22, 10.

[55] *Ibid*.

[56] *Ibid*.

[57] *Ibid*.

meet that goal as it lacks judicial supervision over individual decisions on engaging bulk data collection.

Despite the fact that the US is in violation of its international law obligations, enshrined in the ICCPR and present in customary international law, the HRC recommendations remain by their very nature non-binding—the US is not legally obliged to introduce them, suffering only moral responsibility for the faults identified within the document, should they remained unattended to. This is not to mean, however, that there is no effective legal remedy against the US violations of international law.

V. PRISM Reactions—How Should States Protect Individuals from Privacy Invasions by Foreign Authorities?

The ICCPR provides for two complaint mechanisms, significant to the issue discussed herein.

The first is the procedure of individual complaints against State parties who fail to meet the treaty protection standards. As per the Optional Protocol, each individual within the jurisdiction, either territorial or effective, of a State party whose treaty rights have been violated has the right to address the HRC with a claim for assessing the potential violation and granting them an effective remedy against such infringement. Despite the limited success of the individual procedure, it is a direct remedy against human rights violations committed by ICCPR parties. The US never adopted the Optional Protocol, despite HRC recommendations.[58] The HRC disapproved of the way the US has implemented the ICCPR, emphasising the 'considerable limits' of its 'legal reach and practical relevance' in the US, as directly required by Article 2 ICCPR, demanding State parties to provide for domestic implementations of the guarantees provided for in the treaty.[59] With the US clearly failing to make the necessary changes, it stays in breach of international law by the deficient implementation of the ICCPR as well as international human rights law, created by the State practice and jurisprudence accompanying the treaty.

Since the US has not acceded to the Optional Protocol, nor does it indicate any plans to do so, individuals, whose privacy has been violated by the NSA, seeking compensation would need to base their claims on national US law and direct them at national courts with little chance of success, as the versatile privacy derogations in the USA PATRIOT Act and FISAA ensure extensive NSA freedom in limiting individual privacy.

Non-US persons aware of being under surveillance by the NSA,[60] however, might resort to national law in order to request protection against privacy violations they have suffered. Such claims may be directed not at the US but at local authorities who have failed to protect their residents, as international law requires State authorities not only to refrain from committing human rights violations, but also to take 'all necessary measures' to protect individuals under their jurisdiction from violations by third parties. Acting with

---

[58] *Id.*, C.4(c), 2.

[59] *Id.*, C.4, 2.

[60] US laws do not provide for a right to information on the fact of being under surveillance, in line with many other national criminal procedure codes.

due diligence, State authorities are not obliged to effectively prevent all such violations, only to take all necessary steps to identify and mitigate such risks.[61]

Hence in the case of States whose residents have been under surveillance by the NSA, two different cases are to be analysed. As per the information available through official statements and media coverage, some States, such as the UK, have actively helped the US to gather and process information about individuals within their jurisdiction, or at least allowed for such information to be gathered by US agents. Other State authorities, such as those in Brazil, had little or no information on the private data of their subjects being stored. In the case of the UK and other US allies, their obligation to remedy the damages suffered by individuals is apparent. Individual claims against State authorities allowing for foreign surveillance without national, judicial supervision as well as against those who have failed to take all appropriate measures to identify and mitigate risks of such violations, may be based on national laws granting the right to privacy, meeting the international standards of legality and proportionality. Any national law reflecting the broad US derogations fails to meet the international standard discussed above and makes the State enforcing it liable under the ICCPR. Such States may be targeted with individual complaints under the ICCPR Optional Protocol by those individuals whose rights have been infringed. Yet should US allies in anti-terrorism surveillance not be party to the Optional Protocol or any other international human rights treaty enabling individual complaints (such as the ECHR) individuals whose rights have been infringed by the NSA are deprived of a direct, effective remedy against the violations they have suffered.

In the case of States which despite best efforts have been unable to identify US surveillance activities and have failed in protecting their subjects, no individual remedy against the violators may be deployed. Those States however, wishing to seek protection and remedies for the individuals under their jurisdiction, may file an international claim against the US for the violation of individual privacy rights, constituting a breach of Article 17 ICCPR. As per Article 41 ICCPR any State party to the convention may address the HRC with a claim against another State party not adhering to the treaty. The US has recognised the HRC competence for inter-State complaints and hence may be targeted with such a claim. Even though the procedure of inter-State complaints has not been exercised so far, primarily for diplomatic reasons, the gravity of the NSA surveillance affair might prove a good occasion for a precedent.[62]

Despite this legal possibility, provided for in Article 41 ICCPR, no State has so far confirmed its plans to address the HRC with a privacy violation claim against the US. States have limited themselves to cutting down on their use of US-based telecommunications services. Brazil led the way with President Dilma Rouseff announcing plans for a "Brazilian Internet", one based on infrastructure and services independent from the US.[63] Seeking ways to free the international network from its

---

[61] For more on the due diligence principle in international law, see generally: Kulesza, J., *Due diligence in International Law*, Brill, Leiden, 2015 (forthcoming).

[62] Such a recommendation was included in the statement of Martin Scheinin in his opinion for the European Parliament on the NSA surveillance scheme. See, Scheinin, LIBE Committee Inquiry statement, *supra* nt. 40.

[63] See e.g., The Independent, Charlton, J., *Brazil plans national Internet redesign in order to avoid US web surveillance*, 18 September 2013, available online at <independent.co.uk/news/world/americas/brazil-plans-national-internet-redesign-in-order-to-avoid-us-web-surveillance-8823515.html> (accessed 24 September 2014); The Guardian, Holpuch, A., *Brazil's controversial plan to extricate the internet from US control*, 20 September 2013, available online at <theguardian.com/world/2013/sep/20/brazil-dilma-rousseff-internet-us-control> (accessed 24 September 2014).

strong technical and economic US dependency, President Rouseff invited national diplomats, international business and community activists from all over the world to a first ever NetMundial—an event offering a unique, multistakeholder platform for Internet governance discussions, with its inaugural meeting focused on plans to limit US dominance of the network. NetMundial was viewed as providing strong support for the UN-led Internet Governance Forum, whose political impact has so far been only limited. The PRISM affair enhanced governmental interest in Internet governance, motivating State authorities to increase their involvement in seeking effective ways for multistakeholder decision making.[64] Other States have also taken steps to limit their US dependency, with, for example, the EU States proposing an EU cloud for storing data of EU citizens according to local privacy laws.[65] Also the recent EU data protection reform has a strong international angle, with Chapter V of the proposed Regulation devoted entirely to protecting EU personal data stored or processed outside the Union.[66] Russia recently adopted laws requiring personal data collected by Internet companies operating in that country to be kept on local servers.[67] Surprisingly, both the EU and Russia might be considered to be following the so-far much criticised Chinese example—it is the Great Firewall of China combined with heavily State-funded local infrastructure that allows China for considerable independence from the US in its Internet-based services.[68] Ironically, the BRIC nations,[69] thus far strongly criticised for their drive towards an internationally controlled and US-independent Internet, seem to lead the way in the fight against universal US cyber surveillance.[70]

Summarising the legal claims provided for in international law for privacy violations by foreign authorities, it must be emphasised that States take primarily diplomatic steps to limit the massive US surveillance and mitigate its results. They act less through international law treaties, and more through diplomacy and soft law forums, often resorting to international business practices, rather than international courts, to influence US security and privacy policies.

---

64 On the role of "multistakeholderism" in Internet governance and international law, see Kulesza, J., *International Internet Law*, Routledge, London, 2012, 125-156.

65 See, European Commission, *European Cloud Computing Strategy*, September 2012, available online at <ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy> (accessed 24 September 2014).

66 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, available online at <ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> (accessed 24 September 2014) (GDPR).

67 Deutsche Welle, Maynes, Ch., *Russia tightens Internet screws with 'server law'*, 11 July 2014, available online at <dw.de/russia-tightens-internet-screws-with-server-law/a-17779072> (accessed 24 September 2014).

68 IT World, Patrizio, A., *BRIC Nations Plan Their own "Independent Internet",* 4 October 2013, available online at <itworld.com/internet/377182/bric-nations-plan-their-own-independent-internet> (accessed 24 September 2014).

69 The abbreviation signifies complementing international policies of Brazil, Russia, India, China, and South Africa.

70 IGF Watch news, Malcolm, J., *India's proposal for a UN Committee for Internet-Related Policies (CIRP)*, 29 October 2011, available online at <igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp> (accessed 24 September 2014)).

VI. EU Personal Data Reform—How Efficient Is the New Regulation?

The PRISM revelations were one of the key catalysts for the EU personal data reform. In Europe, that is in the European Union States as well as the 48 Council of Europe States bound by the ECHR, privacy is protected through laws on gathering, storing and processing personal data. Personal data is to be understood broadly as any information on an identified or identifiable individual. This intentionally flexible definition is to allow for legal protection over forever new categories of data, including not only names, addresses, health or employment information, but also data provided by geolocation services or social media. The basic requirement for gathering, storing or processing personal data is the consent of the person whom the data concerns, the data subject, which is to be explicitly granted to the controller of such data unless a particular legal provision states otherwise. A controller is understood to be the entity which 'alone or jointly with others determines the purposes, conditions and means of the processing of personal data', while a processor means any person or other body which 'processes personal data on behalf of the controller'.[71] As per those definitions, the controller decides on the gathering, storage and use of the data, while the processor simply follows the controller's instructions. The obligations instituted by the personal data protection laws are directed at both categories of entities.[72] Another general rule present in European data protection law since its inception is that no international transfer of personal data outside the EU is permissible unless the third country offers 'an adequate' level of protection. As per EU law, assessing the adequacy of the protection granted by foreign authorities is left to the European Commission and only upon its decision may a transfer to a third country be performed. When the third country provides no adequate protection, EU States are obliged to prevent data transfers to such countries. The US approach to privacy has been a challenge to EU data protection law since the early 1990s. Since the US does not grant privacy protection to foreigners, an individual compromise between Brussels and Washington needed to be reached. Such was the character of the much controversial Safe Harbor arrangement, an international compromise between the European Commission and US Department of Trade.[73] Limited to a basic compromise on the key guarantees present in the Directive,[74] it proved insufficient, as adherence to the Safe Harbor program led by the Department of Trade was voluntary for US companies and US authorities failed to verify whether those

---

71 GDPR, *supra* nt. 66, Article 4(5).

72 *Id.*, Article 43.

73 For more information on the "Safe Harbor" agreement visit official EU website devoted to this cooperation, European Commission, *How will the "safe harbor" arrangement for personal data transfers to the US work?* available online at <ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm> (accessed 1 December 2014).

74 These guarantees include the following seven principles: 1) notice (requiring individuals to be informed of their data being collected and ways of its use); 2) choice (possibility of an individual to decide against their data being gathered or processed); 3) onward transfer (further transfer of one's data may be executed only when the third party provides for adequate protection); 4) security (requiring the processor to prevent the data from being lost or misused); 5) data integrity (requiring the processor to ensure the data reliability and use according to the purpose declared); 6) access (enabling the data subject to obtain information on the information about them in the disposal of the processor, as well as to have that information corrected or deleted); 7) enforcement (granting the data subject effective remedy against any infringement of the rights named above).

declaring their compliance with the program actually met its objectives. As a consequence European citizens' data was not protected in the US, even though gathered, stored and processed by US companies in bulk.

The popularity of cloud-based services enhanced the threats to European personal data stored and processed by foreign companies outside the EU. Increasingly, less data was stored in Europe, not allowing local authorities to effectively enforce EU and national privacy laws. It was one of the reasons the comprehensive data protection reform was adopted in Europe in 2014. Aiming to make up for the shortcomings of the 1995 designed framework, the European Commission decided to propose a Regulation, which is directly applicable throughout the Union, rather than a Directive (the Data Protection Directive, DPD), which demanded adoption within national legal systems, often leading to their discrepancies.[75] The primary aim of the reform is to secure personal data originating from the European Union on the global market, moving the current heavy reliance on cloud computing services offered by US companies, and storing Europeans' personal data in the US or off-shoring it to Asia or Africa. It was in 2013 that the elaborate European legal framework for personal data protection proved blatantly ineffective when confronted with the cloud computing design and US national security laws. Differing approaches to individual privacy, discussed above in the context of the contradicting opinion of international law scholars on the universal right to privacy, well known before the PRISM revelations, became the bone of contention between Washington and Brussels, leading to a tight political and economic situation. PRISM was a crucial incentive for the adoption of new, enhanced personal data protection laws as set within the GDPR, whose Chapter V is devoted to transfers of personal data to third countries.[76] As already discussed, one of the principles of EU data protection laws is the prohibition of data transfers outside the Union to countries or territories not grating an 'appropriate' level of protection. The GDPR aims to maintain and elaborate this basic standard, however, following a strong political debate its Article 44 on derogations to this rule is not as strict as one might imagine it to be. Article 44 enumerates cases where controllers, processors and their subcontractors are exempted from data protection obligations. Article 44, paragraph 1(d) allows transfers of personal data to a third country when it is 'necessary for important grounds of public interest'. Recital 87 GDPR lists examples of such public interest, including cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, exchanges between services competent for social security matters, and authorities responsible for prevention, investigation, detection and prosecution of criminal offences.[77] Moreover, as per Recital 56, where personal data might lawfully be processed

---

[75] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD), available online at <eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (accessed 24 September 2014).

[76] GDPR, *supra* nt. 63, Recital 98, Article 43. According to Recital 98, the authority providing such a one-stop shop should be located where the controller or processor has 'its main establishment'.

[77] European Parliament, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available online at <europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> (accessed 24 September 2014). As per the EP proposed amendment this prerogative is to go to the European Data Protection Board. EP proposed amendment 102 to Article 8.

on grounds of public interest, the data subject should be entitled to object to the processing, while the burden of proof rests on the controller who is to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject. A significant vice of the proposed regulation is therefore the lack of reference to the validity of a foreign court order, requesting EU personal data from a subject within its jurisdiction. The proposed regulation, although claiming to fend against third-party intrusions, lacks reference to, for example, a foreign court order approval issued by a European court or a requirement for the issuance of such an order under an international agreement, which would significantly enhance local supervision over foreign processing of personal data of EU citizens. Obliging the addressee of such an order—an EU operating company—to inform local European authorities of a request for data from a foreign court or a requirement for local authorisation prior to delivering the requested data by such a company would also seem an efficient measure to ensure the protection of European data against third party interference. No such stipulations are to be found in the GDPR however, although they were originally present in the 2011 draft version of the Regulation.[78] The threat of an unjustified foreign inspection is not effectively mitigated by the moderate phrasing in Recital 90 GDPR allowing for international transfers only 'where the conditions of this Regulation' are met.

In effect, the proposed personal data reform in the EU, although incited by the Snowden revelations, fails to provide effective protection against FISAA. With that in mind, reference to other international law mechanisms is needed.

VII. Human Rights Due Diligence

As discussed above, international law offers certain tools to protect individuals against foreign privacy intrusions. As per the ICCPR national authorities are under an obligation to actively seek ways to protect their subjects from human rights violations inflicted by third parties. Within this category, next to foreign governments, also international corporations are to be identified. States are under an obligation to ensure that companies operating within their jurisdiction also refrain from violating the rights of State residents. Such an obligation was confirmed in 2008 by the UN Special Representative John Ruggie, who produced a report on the interrelationship of business and human rights.[79] The report, although controversial, is recognised as legal justification of certain human rights obligations resting directly on private companies. Ruggie's argument on "human rights due diligence" obligations relies on three assessments, derived from contemporary international law jurisprudence and State practice. The Special Rapporteur non-controversially claims that active human rights protection is one of a State's duties, originating from international human rights law—an argument discussed in detail above. This duty obliges authorities to refrain from human rights violations as well as to protect individuals from human rights infringements by third parties. States are therefore under a direct obligation to identify and prosecute human rights violations of the latter. Ruggie's

---

[78] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 29 November 2011, Article 42, available online at <statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf> (accessed 24 September 2014)

[79] UN Human Rights Council, Protect, Respect and Remedy: a Framework for Business and Human Rights, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, 7 April 2008,A/HRC/8/5.

second argument is more controversial in nature suggesting corporate responsibility for human rights violations by binding international business to universal human rights standards. Ultimately the report contains a postulate for victims' greater access to effective legal and financial remedies. In 2011, the Report resulted in a set of Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (PRR Framework), detailing human rights obligations of international business.[80] This document may be used as a reference for identifying and executing certain human rights obligations of international companies, regardless of their place of incorporation, seat or the market they target. Without the need to engage in confusing debate on limits of State jurisdiction of international companies and international private law, the Ruggie principles and the PRR Framework allow identification of which measures need to be taken by international corporations with respect to individual privacy rights of their users.

As per the PRR Framework, it is a State's duty to guide business on respecting human rights by advising on appropriate methods, including 'human rights due diligence',[81] yet the norms of international human rights law may be applied to business directly. Companies must represent a certain "human rights due diligence" when an individual right is under threat created by their activities.[82] The lack of State action preventing businesses from certain actions or allowing for a certain violation is no excuse for a company's infringement. Principle 17 of the PRR Framework defines a human rights impact assessment as 'assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed'[83] and encourages companies to introduce human rights standards for their customers regardless of the legal requirements effective in their jurisdiction. As a matter of fact, forever more companies, seeking to best cater for their clients' needs, such as Google, Facebook, IBM or Intel have introduced internal privacy policies, seeking to ensure their clients' comfort and trust. The PRR Framework offers a human rights standard for international business, regardless of national laws and differing regional perceptions of individual liberties. Together with the rich body of work on privacy by the HRC, it serves as a good basis for setting privacy policy standards and formulating reasonable expectations for companies processing and trading personal data. The growing consumer awareness of the value of their data requires international companies to cater for their customers' needs also on the level of privacy protection. While international law offers certain solutions against States infringing human rights, as discussed above, it is the PRR Framework that allows direct enforcement of these rights against the companies.

VIII. Summary

While a US company denying an NSA request would likely face sanctions just as much as the employees of its Chinese operating branch could face prison for denying police access to data stored on their machines, there is no doubt that any bulk collection of personal information without legal basis and court supervision is against international

---

[80] Human Rights Council, The Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (Guiding Principles), 21 March 2011, A/HRC/17/31.

[81] *Id.*, 12.

[82] *Ibid.*

[83] *Id.*, 21.

law. The options discussed above all aim to limit this undesired state of affairs. Be it an inter-State complaint under the ICCPR, enhanced diplomatic activity, such as the NetMundial or direct consumer pressure on companies betraying clients' trust, the easily-identifiable international privacy standard seems possible to achieve, despite states or private entities claiming no such standard exists. Consequently, denying corporate responsibility for privacy violations deliberately departs from the truth. It is not the legal notion of privacy that proves troublesome in the global information society, it is the political approach and interests that disallow the existing universal standard to be enforced. The PRISM affair proved the existence and universal recognition of such a right and one is left to hope that the rising awareness of telecommunication service users will lead to a significant change in State surveillance policies.

*