Foreign Surveillance: Law and Practice in a Global Digital Environment

Professor Ian Brown

Associate Professor, Oxford Internet Institute, University of Oxford

Professor Douwe Korff

Emeritus Professor of International Law, London Metropolitan University

Electronic communications; Extraterritoriality; Interception of communications; International law; Privacy; Sovereignty; Surveillance; United States

Abstract

The reporting of leaks from whistleblower Edward Snowden has led to a global debate about privacy in the Internet era. This article reviews US and UK alleged practices related to surveillance of foreign Internet communications content and "metadata", and the international human rights law issues they raise. Often, these practices are based on vague laws that are applied on the basis of secret guidance or interpretations—which in international human rights terms is not "law" at all. To the extent that there are specific, published laws, their hallmarks are the sweeping, largely discretionary powers that they grant, a lack of effective oversight, and (often) discrimination between nationals or residents and non-nationals or non-residents. Spying on citizens, politicians and companies in another country, and obtaining data from servers in that other country, without the consent of the target country, furthermore violates the sovereignty of the latter country.

1. Surveillance in the digital environment

American and European intelligence agencies are carrying out surveillance of telephone and Internet use on a massive scale. Whistleblower Edward Snowden revealed in 2013 that the US National Security Agency (NSA) is gaining "bulk access" to records of all domestic telephone calls, using legal orders to telephony providers, and has at various points attempted to gain access to bulk records of Internet communications. Through its PRISM programme, the NSA is also able to compel the provision of large volumes of personal data held by US-based communications services, including Facebook, Microsoft, Apple, Yahoo! and Google.[1] The NSA and cooperating signals intelligence agencies (particularly in the other so-called "Five Eyes" nations: United Kingdom, Canada, Australia and New Zealand) have a global series of programmes to intercept and share data from fibre-optic cables carrying the majority of Internet traffic,[2] as well as satellite links,[3] radio communications (including mobile phone calls, most famously of

[1] See the overview of Snowden revelations and relevant documents on the Guardian website: *http://www.theguardian.com/world/the-nsa-files* [Accessed May 5, 2014].

[2] See the witness statement of Dr Ian Brown in the application submitted to the European Court of Human Rights under the ECHR, *Big Brother Watch, Open Rights Group, English PEN, and Dr Constanze Kurz v United Kingdom* (App. No.58170/13) (awaiting a decision on admissibility from the Court). The witness statements are available at: *https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-internet-surveillance* / [Accessed June 5, 2014].

[3] Steve Wright, "An Appraisal of Technologies of Political Control", *European Parliament PE* 166 499, January 6, 1998.

German Chancellor Angela Merkel),[4] and through "hacking" into sensitive systems (including the UN internal videoconferencing system,[5] EU embassies in New York and Washington DC,[6] and the European Commission and Parliament's telecommunications provider in Belgium[7]).

Governments are analysing and exchanging ever-greater quantities of information on their citizens, using data mining tools to identify individuals of interest in a digital tsunami of data about individuals produced by modern technologies.[8] Companies are required in many jurisdictions to provide law enforcement and intelligence agencies with access to this data—and in some cases explicitly to retain data for longer than otherwise required for business purposes.

1.1 Content and "metadata"

Internet surveillance clearly affects the privacy of electronic "correspondence" such as e-mails, instant messages, voice and video calls (through systems such as Skype), online forums, and other digital equivalents of the telephone and telegraph.

However, surveillance in this modern communications environment goes much further than crocodile clips attached to a targeted telephone line, or a bug installed in a telephone. In the online world almost every activity leaves behind detailed records, or "metadata", linked to individuals through the IP address of their computer or smartphone, and through digital "cookies" left on their browser by websites, as well as numerous other identifiers.

Many jurisdictions provide lower levels of legal protection for such metadata than for the contents of communication, because it previously was thought to be much less revealing than the contents of telephone calls. Modern data analytics tools make this questionable—as Professor Edward Felten noted in an affidavit for the American Civil Liberties Union, "Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations."[9]

However, now that so much metadata is generated by online activities—as well as a constant location trail from individuals' mobile phones—it can be even more revealing of individual interests, activities and associations. For example, the NSA's CO-TRAVELLER programme monitors nearly five billion global phone location updates each day, allowing the agency to link individuals that spend time together in the same physical locations.[10]

As the UN and Inter-American rapporteurs have made clear, there is an interference with fundamental rights as soon as communication data are intercepted and collected. The protection of the right to privacy and the other rights affected does not just begin at the moment data are extracted from a bulk interception database and used in respect of the relevant person (as some governments have suggested). Individuals must also be protected against their data being "hoovered" up for the purpose of analysis and data mining. This was also explicitly stressed in terms of the ECHR by Judge Zapančič of the European Court of Human Rights at a hearing into mass surveillance of the European Parliament's civil liberties committee (LIBE).[11]

[4] "Embassy Espionage: The NSA's Secret Spy Hub in Berlin", *Der Spiegel*, October 27, 2013.

[5] Laura Poitras, Marcel Rosenbach and Holger Stark, "Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel*, August 26, 2013.

[6] Laura Poitras, Marcel Rosenbach, Fidelius Schmid and Holger Stark, "Attacks from America: NSA Spied on European Union Offices", *Der Spiegel*, June29, 2013.

[7] Gregor Peter Schmitz, "Cyber Attack: Belgians Angered by British Spying", *Der Spiegel*, September 20, 2013.

[8] Ian Brown, *The challenges to European data protection laws and principles*, Working Paper No.1 for a "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments", European Commission, 2010.

[9] Supplemental Declaration of Professor Edward W. Felten, Case No.13-cv-03994 (WHP), United States District Court, Southern District of New York, filed October 25, 2013.

[10] Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show", *Washington Post*, December 4, 2013.

[11] Boštjan Zupančič, *Oral statement to the European Parliament Committee on Civil Liberties, Justice and Home Affairs*, October 14, 2013.

1.2 Surveillance of foreigners

Many jurisdictions provide lower privacy protection to communications outside (or to or from) their own borders than they do to purely domestic communications, at least in relation to national security surveillance. This is significant, because the global infrastructure of the Internet and electronic communications has made surveillance of such extraterritorial communications much easier.

Fibre-optic cables are the main arteries of the Internet worldwide. If they can be successfully tapped, then they provide a "fast track" to international Internet surveillance, without the need to target an individual user with more specialised surveillance methods. Much of the rest of Europe's external Internet traffic is routed through the United Kingdom, as this is the landing point for the majority of transatlantic fibre-optic cables. GCHQ has reportedly placed data interceptors on fibre-optic cables conveying Internet data in and out of the United Kingdom, and are able to store a significant fraction of global Internet traffic for three days on a rolling basis while carrying out further automated analysis.[12]

Much Internet traffic is encrypted to protect it from interception, especially since large companies such as Google and Facebook enabled encryption for their services. However, GCHQ and the NSA have also reportedly succeeded in decrypting data protected using many of the commonly used encryption standards. They did this by covertly influencing encryption standards; liaising with technology companies selling products to government; through compromise of personnel at selected companies; and through massive investment in computing capacity. Snowden revealed that funding for this programme—$254.9 million for 2013—dwarfed that for the PRISM programme ($20 million per year).[13]

1.3 Social media, behavioural targeting and ubiquitous computing

New communications tools enable a new level of surveillance of online activities. Social media sites encourage individuals to share information about themselves with their "friends", along with the operators of those sites—and government agencies that have access. Facial recognition software is used by some social networking sites to enable the identification of individuals in uploaded photos. Mobile phones send location information to network providers to enable calls to be forwarded, and to enable location-based "value-added" services such as mapping and advertising. Social media apps running on these smartphones allow users to both explicitly and implicitly share information about themselves and those around them. Behavioural advertising companies track individuals across websites to show adverts targeted to their profiles. WPP already has built such profiles on 500 million individuals in North America, Europe and Australia.[14]

Very low-cost remotely readable Radio Frequency Identification (RFID) tags are increasingly attached to consumer goods and access control cards, the first wave of the "Internet of Things" that could make some aspects of the physical world as trackable as Internet activity. More sophisticated tags are included in many nations' passports, and are also being used for road toll payment systems, public transport ticketing, and in contactless payment cards such as MasterCard's *PayPass* and Visa's *Paywave*. Gadgets such as heart rate monitors already allow individuals to share sensor information about themselves and their environment through social media.[15]

This "ubiquitous computing" will become a pervasive phenomenon, with some individuals recording and sharing online detailed information about every aspect of their lives.[16] Privacy-sensitive individuals

[12] See the witness statement of Dr Ian Brown (fn.2 above), p.10.

[13] James Ball, Julian Borger and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian*, September 6, 2013.

[14] Emily Steel, "WPP's digital ad arm pushes into China", *Financial Times*, October 9, 2012.

[15] Ian Brown, *The challenges to European data protection laws and principles* (fn.8 above).

[16] I. Askoxylakis and I. Brown, "To log or not to log?—Risks and benefits of emerging life-logging applications", *European Network and Information Security Agency*, 2011.

will have a limited ability to opt-out of such environmental sensing by others, as users of prototype Google Glass are discovering. In the next decade these sensors and tags are likely to become ubiquitous, dramatically smaller, and much more capable. They will fade further into the background of everyday life, with little to remind people of the data trails they are generating.[17]

These technology-mediated activities are open to surveillance in ways that are not present in face-to-face interactions, and this makes individual control more difficult. Digital data is usually persistent (saved by default, perhaps indefinitely), searchable (much easier to find), replicable (easily shareable in convincing form), and as a result "lacks a specific audience", as boyd put it.[18] None of these qualities is obvious to less experienced users. Real-world gossip is deniable, usually geographically limited and fades over time. Digital information about an individual—however partial and unrepresentative—can persist as a digital scarlet letter.

Before the Snowden revelations, many experts thought that the continued dramatic growth in levels of Internet traffic would outstrip the capacity of signals intelligence agencies to monitor this data flood. We now know that NSA and GCHQ have developed technology that is able to record and filter through very large volumes of traffic; there is no technological reason why they should not be able to continue to do so.

2. The applicability of international human rights treaty obligations to extraterritorial acts of states that are parties to these treaties

Under the international human rights treaties, states must ensure (or secure) the rights guaranteed in these treaties without distinction or discrimination to "everyone within their territory or jurisdiction" or simply "within their jurisdiction" or "subject to their jurisdiction" (art.2(1) of the ICCPR; art.1 of the ECHR; art.1(1) of the IACHR).[19] Although the concept of "jurisdiction" as used here is perhaps "primarily territorial", it is applied in a more "functional" way, at least in special cases, such as when agents of a state are acting outside the state and exercise control outside the state.

This has consistently been the position of the UN Human Rights Committee, as expressed in its views in the cases of *Lopez Burgos v Uruguay* and *Celiberti de Casariego v Uruguay*,[20] and as summed up in its General Comment on "the Nature of the General Legal Obligation Imposed on States Parties to the Covenant"[21]:

> "States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."

In the words of the European Court of Human Rights (which adopted the same view somewhat later)[22]:

[17] D. Korff and I. Brown, "New Challenges to Data Protection—Final report", *European Commission: DG Justice, Freedom and Security*, 2010. See also the forthcoming Council of Europe Commissioner for Human Rights Issue Paper on "The Rule of Law on the Internet and in the wider digital world".

[18] d. boyd, "Why Youth ♥ Social Network Sites: The Role of Networked Publics in Teenage Social Life", in David Buckingham (ed.), *Youth, Identity, and Digital Media* (Cambridge, USA: MIT Press, 2008), pp.119–142.

[19] The ACH&PR instead stipulates that "The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Chapter and shall undertake to adopt legislative or other measures to give effect to them" (art.1).

[20] *Lopez Burgos v Uruguay* and *Celiberti de Casariego v Uruguay*, Case Nos 52/1979 and 56/1979, both of July 29, 1981, at §§ 12.3 and 10.3 respectively. See also the Committee's Concluding Observations on the reports by Israel in 1998 and 2003.

[21] General Comment 31, para.10.

[22] *Issa v Turkey* (2005) 41 E.H.R.R. 27 at [68].

> "… In exceptional circumstances the acts of Contracting States performed outside their territory or which produce effects there (extra-territorial act) may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention."

According to the Committee and Court, states must act in accordance with their human rights treaty obligations whenever they "exercise effective control" over an area outside their borders, or when they bring persons who are in the territory of another state under their "authority or control". This is because (to again refer to the Court):[23]

> "Accountability in such situations stems from the fact that Article 1 of the [ECHR] cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory […]."

The same view is taken by the Inter-American Commission of Human Rights, *Coard v the United States*.[24] This shows that this "functional" approach to the obligations of states has broad support in the international human rights fora.

This approach was emphatically endorsed by the International Court of Justice in its Advisory Opinion on the Israeli Wall, in which it expressly agreed with the views of the Human Rights Committee and held:[25]

> "In conclusion, the Court considers that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory."

If a state intercepts, extracts copies of, and analyses communications of individuals and organisations outside that state, that of course "produces effects" on those concerned, even if they are "foreigners" and not physically on the territory of the state concerned. It would therefore seem to be difficult to maintain that if a state explicitly legislates to authorise such surveillance, it is not exercising its "jurisdiction" in that respect: bringing something within the legal rules of a country, making that something subject to the legal order of a country, is perhaps the most conspicuous way to exercise a country's jurisdiction. It is strongly arguable that in international-legal terms, such a country is exercising both "legislative" and "enforcement jurisdiction" over the data.

This would be the case, even if the exercise of that jurisdiction would violate the sovereignty of another state, e.g. because it concerned data physically located in another country (cf. the discussion under the heading "*Transnational collecting of data and state sovereignty*", below). The fact that the act was contrary to international law of course does not mean that the state perpetrating the act is not bound by its human rights obligations.

In sum: it is strongly arguable that a state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state, e.g. by using the physical infrastructure of the Internet and the global communications system to extract those data from servers, personal computers or mobile devices in the other state, or by requiring private entities that have access to such data abroad to extract those data from the servers or devices in another country and hand them over to the state, is bringing those data, and in respect of those data, the data subjects, within its "jurisdiction" in the sense in which that term is interpreted by the treaty bodies and courts implementing the ICCPR, the ECHR and the IACHR. In the view of these bodies, such a state must, in this extraterritorial activity, comply with its obligations under those treaties.

Specifically, in this view, states must limit any such extraterritorial surveillance in the same way as they must limit their domestic surveillance. Both must be in accordance with the fundamental requirements

[23] *Issa* (2005) 41 E.H.R.R. 27 at 71, with reference to earlier case-law.
[24] *Coard v United States* , Decision of September 29, 1999, Report No.109/99, Case No.10.951, §§ 37, 39, 41 and 43.
[25] ICJ, *Construction of a Wall (Advisory Opinion)*, July 9, 2004, para.111 (see also para.109 on the HRC).

of "law", "necessity", "proportionality", absence of excessive discretion/arbitrariness, "effective remedies" and oversight, etc. As noted by Stratford and Johnston in an Opinion for the UK All-Party Parliamentary Group on Drones,[26] and argued in the prioritised application to the Strasbourg court *Big Brother Watch v United Kingdom*,[27] this has been a serious problem with the UK legal framework. Nor may the state discriminate on the basis of either the nationality or the geographical location of the individuals whose data are caught.[28]

However, certain states, most notably the United States and Israel, do not accept any extraterritorial effect of their international human rights treaty obligations, in particular in relation to the ICCPR. In its most recent (2011) report to the Human Rights Committee, consideration of which was delayed until March 2014, the United States reiterated its earlier position that the ICCPR "appl[ies] only to individuals who were both within the territory of a State Party and within that State Party's jurisdiction", even though it acknowledged the Committee's contrary views and the jurisprudence of the ICJ.[29] One commentator has argued that this position has been "expertly dismantled" and "fatally compromised" by the leak of two internal reviews concluding the opposite, undertaken by Professor Harold Koh while chief legal adviser at the US State Department.[30]

In its 2014 Concluding Observations on the US report under the ICCPR, the Human Rights Committee:[31]

> "regret[ted] that the State party continues to maintain its position that the Covenant does not apply with respect to individuals under its jurisdiction but outside its territory, despite the contrary interpretation of article 2(1) supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and state practice[,]"

and urged the United States 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 its object and purpose and review its legal position so as to acknowledge the extraterritorial application of the Covenant under certain circumstances, as outlined inter alia in the Committee's general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant."

In the context of the discussions on the Draft UN General Assembly Resolution on *Privacy in the Digital Age*, submitted in response to the Snowden revelations, a briefing note was leaked that confirmed that the United States continues to take the position that it is not under any legal duty to comply with art.17 of the ICCPR (privacy) outside its own geographical territory. Indeed, it considered this to be a "red line" which it will not cross. Its very first instruction was that the US negotiators should:[32]

> "Clarify that references to privacy rights are referring explicitly to States' obligations under ICCPR and *remove suggestion that such obligations apply extra-territorially"(emphasis added)*.

2.1 Transnational collecting of data and state sovereignty

Quite separate from the duty of states to comply with their international human rights obligations when acting extraterritorially, there is the question of when transnational collection of data by one state from

[26] J. Stratford and T. Johnston, "The Snowden 'revelations': is GCHQ breaking the law?" [2014] 2 E.H.R.L.R. 129–141.
[27] *Big Brother Watch v United Kingdom* App. no.58170/13, communicated to the parties on 16 January 16, 2014 (see fn.2 above).
[28] See again General Comment 31, para.10.
[29] CCPR/C/USA/4, para.505. See also Testimony of John B. Bellinger III (chief Legal Adviser for the US Department of State 2005–2009) to the Privacy and Civil Liberties Oversight Board, March 19, 2014.
[30] M. Milanovic, "Harold Koh's Legal Opinions on the US Position on the Extraterritorial Application of Human Rights Treaties", *EJIL: Talk!* March 7, 2014.
[31] HRC 2014 *Concluding Observations CCPR/C/USA/4*, para.4.
[32] *Right to Privacy in the Digital Age—U.S. Redlines*, *http://columlynch.tumblr.com/post/67588682409/right-to-privacy-in-the-digital-age-u-s* [Accessed June 5, 2014].

servers or routers or other devices in another state, as part of a general surveillance programme by the first state, is compatible with general public international law and in particular with the principles of respect for other states' sovereignty and non-interference in the internal affairs of another state. We are talking here of data being actively "pulled" from a server in the latter country, by—or at the demand of—an agency of the first country.[33] There are separate issues related to the transnational sharing of communications and "metadata" by intelligence agencies.[34]

We know from the Snowden revelations that, for instance, corporations established in the United States, or indeed even controlled from the United States, or even just active in the United States, can be ordered by the US authorities to produce such data from servers they own or operate in other countries; and can be ordered by the US authorities to not inform either the authorities in the countries from which they pull the data, or the entities whose data they are handing over, or indeed the data subjects, of such compulsory data disclosures.

Leaving the broader, complex issues aside,[35] we should note that:[36]

> "The governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter."

More specifically, as the International Law Commission said:[37]

> "With regard to the jurisdiction to enforce, a State may not enforce its criminal law, that is, *investigate* crimes or arrest suspects, in the territory of another State without that other State's consent" (emphasis added).

In fact, rather than consenting to extraterritorial investigations by foreign agents on the territory of other states, in international law enforcement cooperation, the norm is to provide mutual legal assistance through so-called Mutual Legal Assistance Treaties or MLATs. These can be bi- or multi-lateral. A provision in the Council of Europe Cybercrime Convention that suggests that transnational collecting of data by law enforcement agencies might be possible with the consent, not of the target state, but with "the lawful and voluntary consent of the person who has the lawful authority to disclose the data to [the requesting LEA]" (art.32(b)) is highly contentious. At the *Octopus Conference on Cooperation against Cybercrime* (Strasbourg, December 4–6, 2013), it was agreed to explore drafting a new protocol to either the Cybercrime Convention or the Council of Europe Data Protection Convention (or an entirely new, separate treaty) to address this issue.[38] This confirms that transnational access to data, and the "pulling"

[33] We are not discussing other scenarios here, such as access by a state national security or law enforcement agency to data held on the territory of the state in question, but when the data are owned by a foreign company or by a foreign public body (e.g. by a company or public body using a cloud service in the country where the data are accessed); or access by a state agency to data flowing through cables running through the territory of the state (even if the data relate to communications between entities that are both, or all, outside the state); or interception of radio or Wi-Fi communications data in one state by interception stations or satellites operated by another state. These scenarios too raise serious questions, also as concerns the different levels of control exercised by different countries over the global Internet and e-communications infrastructure. However, they fall outside the scope of the present article.

[34] See again Stratford and Johnston (fn.26 above).

[35] For a detailed discussion, see the 2006 Report of the International Law Commission (58th session), *Annex E—extraterritorial jurisdiction*, pp.516ff.

[36] Ian Brownlie, *Principles of Public International Law*, 6th edn (2006), p.306. The classic expression of the principle can be found in the award of the sole arbitrator in the *Palmas Island* case, Max Huber: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organization of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations." *Island of Palmas Case (Netherlands/United States of America)* , Award of April 4, 1928, UNRIAA, vol.II (1928), pp.829–871 at p.838. See also the Lotus *judgment* of the Permanent Court of International Justice (the forerunner of the International Court of Justice), September 7, 1927, pp.18–19.

[37] 2006 Report of the International Law Commission, *Annex E*, p.526, para.22, emphasis added.

[38] On the conference, see *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp* [Accessed June 5, 2014]. The need for a new protocol was broadly agreed at the concluding session, even though the nature of this protocol was still very unclear, other than the "consent" options in an earlier 2013 paper were insufficient (they referred to consent by the data subject/suspect, which it was agreed could not be assumed to have been given voluntarily; and to consent to others with "lawful authority" to disclose data (read: Internet and e-communications

of data from other countries, without the consent of such other countries, is still seen as clearly contrary to public international law; and that the contentious Cybercrime Convention article, by itself, does not express such consent.

Similarly, the post-World War II treaties between Western states on international cooperation in relation to national security also start from the premise that—outside of times of war—spying by one nation on the activities of citizens of another nation is, in principle, a violation of the sovereignty of the latter nation. That the states in question felt the need for treaties in this regard confirms that they believe that without such treaties transnational surveillance (outside of times of war) is unlawful under public international law. This is reinforced by the fact that, reportedly, under the main 1946 UKUSA treaty, since amended and extended to the other three mainly white and English-speaking countries, Australia, Canada and New Zealand (now jointly known as "5EYES"), the parties agreed to limit surveillance of each other's citizens or officials.[39] The Western Allies equally felt obliged to enter into formal (treaty) agreements on intelligence with the Federal Republic of Germany at the end of the World War II occupation period.[40]

Crucially, it is *not* enough to argue that just because many states in practice collect data held in other countries even in the absence of a treaty, either in a law enforcement or a national security operations context, the requirement of consent from the target country has somehow gone away, or even that transnational access to data without such consent from the target country is now allowed under customary international law.[41] The creation of new customary law requires not just wide state practice (and it is even doubtful whether the practice really is that widespread), but also, crucially, *opinio iuris*: acceptance by states that the practice takes place under a legal rule.

It is quite clear from the strong protests against transnational surveillance, as expressed both by individual states in Europe, South America and elsewhere, and by major intergovernmental bodies and fora such as the UN General Assembly, the Council of Europe, the European Parliament and Commission that *opinio iuris*, if anything, is on the opposite side: that it is a principle of public international law, confirmed in international customary law, that transnational collection of data from a country without that country's consent, for either law enforcement or national security purposes, is unlawful.

3. Conclusion

Following the Snowden revelations, the US government has begun the process of significant reform of its intelligence agencies' surveillance activities. In a speech setting out the reforms,[42] President Obama acknowledged: "America's capabilities are unique. And the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do."

Importantly, significant decisions of the Foreign Intelligence Surveillance Court that oversees surveillance orders to US companies will be annually reviewed by the Administration for potential declassification. Limited constraints will be placed on the use (but not the collection) of communications

service providers), who it was agreed were not in a position to make the relevant judgment on disclosure). The matter is therefore to be addressed in further study.

39 For the original text, see *http://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf* [Accessed June 5, 2014]. For the background and extensive further documentation, see *http://www.nsa.gov/public_info/declass/ukusa.shtml* [Accessed June 5, 2014]. But note that this is still not complete; some (many?) documents relating to the 5EYES arrangements, including in particular subsidiary agreements or guidelines, remain secret. The principle that 5EYES countries (or rather, initially, the United States and the United Kingdom) would not spy on each other may be derived from the clarification in fn.3 to the March 5, 1946 text, which says that "the U.S., the British Commonwealth of Nations, and the British Empire" shall not be regarded as "foreign countries"; and that their communications therefore do not constitute "foreign communications". Note the deletion of one word from the de-classified text: the word may well be "diplomatic". If so, that would suggest that diplomatic communications of countries outside the 5EYES were (and still are?) specifically targeted under the treaty.

40 Joseph Foschepoth, *Überwachtes Deutschland*, 3rd edn (2013), Ch.2. The (German) text of the "Memorandum of Understanding" between the Western allies and the young FRG (full title in English: "Agreements affecting the Intelligence Situation in Germany after the Termination of the Occupation", May 11, 1955, ref. NACP, RG 84) can be found at pp.291–292. It was only declassified in the last few years.

41 This was argued by some representatives at the Octopus Cybercrime Conference in Strasbourg.

42 Remarks of President Barack Obama, *Results of our Signals Intelligence Review*, January 17, 2014 in Washington DC.

gathered between Americans and foreign citizens. "Bulk" intercepted data will only be used for the purposes of "counter-intelligence; counter-terrorism; counter-proliferation; cyber-security; force protection for our troops and allies; and combating transnational crime, including sanctions evasion". And communications companies will be allowed to make public more information on the level of accesses to their systems by government agencies for national security purposes.

However, as the Human Rights Committee noted in its review, the United States still needs to "review its legal position so as to acknowledge the extraterritorial application of the Covenant under certain circumstances" and "ensure that effective remedies are available for violations".[43] The Committee "remains concerned that [non-US] persons enjoy only limited protection against excessive surveillance", and concluded that the United States should[44]:

(a) 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 art.17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance;

(b) ensure that any interference with the right to privacy, family, home or correspondence be authorized by laws that (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise specifying in detail the precise circumstances in which any such interference may be permitted; the procedures for authorizing; the categories of persons who may be placed under surveillance; limits on the duration of surveillance; procedures for the use and storage of the data collected; and (iv) provide for effective safeguards against abuse.

There has been much less public debate of the Snowden revelations in the United Kingdom; cursory investigations by the parliamentary Intelligence and Security Committee; and as yet no government plans for reform—although the Labour and Liberal Democrat parties have both called for changes.[45]

The United Kingdom's Investigatory Powers Tribunal is hearing five complaints from non-governmental organisations,[46] but on past form is unlikely to find in their favour (having previously found for the complainant in only 0.75 per cent of cases).[47] If the Strasbourg Court decides this Tribunal cannot provide an "effective remedy",[48] it may hear the *Big Brother Watch* case directly. It may additionally or instead hear appeals from the Tribunal. Either way, it seems judicial intervention will be required to bring the United Kingdom's legal framework back into compliance with the Human Rights Convention.

[43] CCPR/C/USA/4 para.4 (note 31).
[44] CCPR/C/USA/4 para.22, CCPR/C/USA/4.
[45] I. Brown, "Finally, some high-level UK debate on Internet surveillance", March 4, 2014, *http://doooooom.blogspot.co.uk/2014/03/finally-some-high-level-uk-debate-on.html* [Accessed June 5, 2014].
[46] *Liberty v GCHQ*, Investigatory Powers Tribunal. Directions hearing report by Naomi Colvin at *https://auerfeld.wordpress.com/2014/02/14/liberty-and-others-v-gchq/* [Accessed June 5, 2014].
[47] *Big Brother Watch* , App No.58170/13, para.84 (see fn.2 above).
[48] *Big Brother Watch* , App No.58170/13, paras 179–190 (see fn.2 above).