Queen Mary University of London
School of Law

Queen Mary, University of London
Mile End Road, London E1 4NS
Department of Law
Tel: + 44 (0)20 7882 3936
Fax: + 44 (0)20 7882 7042
www.law.qmul.ac.uk

SciencesPo
CENTRE DE RECHERCHES INTERNATIONALES

CERI – UMR 7050
56, rue Jacob
75006 Paris
Tel: + 33 (0)158 71 70 00
Fax: + 33 (0)158 71 70 91
http://www.sciencespo.fr/ceri/fr

UNIVERSITÉ LYON III
JEAN MOULIN

UNIVERSITE JEAN MOULIN LYON 3
FACULTE DE DROIT
EQUIPE DE DROIT PUBLIC EA 666
15, Quai Claude Bernard
69239 LYON cedex 02
TEL: +33 (0)478 78 70 59
www.univ-lyon3.fr

Contribution to OHCHR Inquiry: Identifying and Clarifying Principles, Standards and Best Practices regarding the Promotion and Protection of the Right to Privacy in the Digital Age, including the Responsibility of Business Enterprises in this regard

Professors Elspeth Guild, Queen Mary University of London
Didier Bigo, Sciences-Po Paris
Marie-Laure Basilien-Gainche, University Jean Moulin Lyon III

Legal Framework

Article 12 of the Universal Declaration of Human Rights (UDHR): "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
Article 17 International Covenant on Civil and Political Rights (ICCPR) (ratified by 167 States) "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". "Everyone has the right to the protection of the law against such interference or attacks."
Article 26 of the International Covenant on Civil and Political Rights (ICCPR) provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law." "In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

Introduction

We have followed with interest the work of OHCHR on the right to privacy in a digital age. The Annual report of the UN High Commissioner for Human Rights of 30 June 2014[1] provides an excellent overview of the challenges which the digital age presents for the universality of the right to privacy. In this submission we take the opportunity to develop on three paragraphs of that report in particular: paragraph 32[2]; paragraph 35[3] and paragraph 36.[4] In particular, our concerns relate to the claim and in the case of some states, the assumption that the right to privacy can be differently articulated depending on the nationality of the person claiming it. This problem has arisen with the expansion of electronic technology which is based on technical capacities unrelated to national borders. As intelligence services seek to obtain information, including personal data, in the interests of their national security, the rules which they apply all too frequently are those relating to foreign intelligence. This has accentuated a tension regarding the human right to non-discrimination in the delivery of the right to privacy as it has required state authorities to provide some justification for the differential treatment of citizens and foreigners (as increasingly the personal

Many thanks for Dr Claude Cahn for his very useful additions on an early draft.

[1] A/HR/27/37.

[2] Article 2 of the International Covenant on Civil and Political Rights requires each State party to respect and ensure to all persons within its territory and subject to its jurisdiction the rights recognized in the Covenant without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. The Human Rights Committee, in its general comment No. 31, affirmed that 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."[2] This extends to persons within their "authority".

[3] This conclusion is equally important in the light of ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside,[3] or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

[4] International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks", as well as with article 2, paragraph 1. In this regard, the Human Rights Committee has underscored the importance of "measures 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."

data of citizens is mixed with that of foreigners, all data travelling around the world on the internet before arriving at its destination), something which they could previously avoid.

From a European perspective, we are particularly concerned by developments in the European Union where the right to privacy of non-EU nationals is currently subject to greater intrusions than that of EU citizens. This problem is particularly acute as regards the creation, use and access to EU databases of personal information of non-EU citizens (described as third country nationals by the EU institutions) such as the EU database of fingerprints of asylum seekers and third country nationals apprehended irregularly crossing an external border, EURODAC;[5] the database of personal information of all third country nationals who apply for a visa, the Visa Information System;[6] the database which includes personal data of third country nationals who are to be refused entry to the EU, the Schengen Information System II;[7] and the proposal that these databases should linked to permit police authorities to search all of them simultaneously.[8] The implicit assumption of these databases and the new proposal for interoperability among them is that the privacy of the foreigner is protected to a lesser extent than that of the (EU) citizen. This presumption is inherent in the fact that none of the EU databases containing information about EU citizens are available on such a wide basis to police authorities, nor are they interoperable. The problematic nature of the legal framework is reinforced when the European Criminal Records Information System (ECRIS)[9] is taken into account. It is proposed that this database be split into two – one containing criminal record information of EU citizens the other of information relating to the criminal records of third country nationals (including dual EU and third country national citizens). Only the latter database will be included in the interoperability project with the other databases containing personal data of foreigners.[10] We are deeply concerned that this action by a regional institution undermines the principle of equality in relation to the right to privacy and is inconsistent with the duty of the EU's Member States to comply with the UDHR and ICCPR.

[5] Regulation 603/2013 OJ [2013] L 180/1.
[6] Regulation 767/2008 OJ [2008] L …/1.
[7] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ [2007] L 205/63.
[8] Commission proposal for a regulation of the European Parliament and of the Council (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/22 26 (COM(2017)793) and Commission proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) (COM(2017) 794).
[9] Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA OJ [2009] L 93/33.
[10] COM (2017) 344.

The universality of the right to privacy

As the OHCHR makes clear in its 30 June 2014 report, the right to privacy is universal. It applies equally to everyone, whether they are citizens or foreigners of the state within the jurisdiction of which they find themselves. Differences in the protection of the right to privacy contained in the ICCPR on the basis of nationality are inconsistent with the right to equality contained in Article 27 ICCPR.

The Human Rights Committee in General Comments 15[11] and 31 has made it very clear that citizens and foreigners are equally entitled to rely on the ICCPR rights without distinction:

> "10. 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. As indicated in General Comment 15 adopted at the twenty-seventh session (1986), the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves in the territory or subject to the jurisdiction of the State Party. This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained, such as forces constituting a national contingent of a State Party assigned to an international peace-keeping or peace-enforcement operation."[12]

The position of the Treaty Body responsible for the correct interpretation of the ICCPR is clear – the right to privacy in Article 17 applies equally to all persons whatever their nationality or immigration status. Further, there is only one standard applicable to the right to privacy. The content of the right contained in Article 17 does not vary according to the nationality or immigration status of the individual entitled to it. States parties which have bound themselves voluntarily to comply with the ICCPR and to deliver its rights to everyone within their jurisdiction must, in so far as they are implementing their Article 17 obligations, provide a consistent level of protection of privacy to everyone which fulfils their ICCPR obligations as interpreted by the Human Rights Committee. Further, the

[11] "[Aliens] may not be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence." HRC General Comment 15 The Position of Aliens Under the Covenant 30 September 1986.

[12] Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004).

right to privacy must be protected by the state including in circumstances where at first instance the challenges arises by the actions of private sector actors (and only subsequently are accessed by intelligence authorities).[13]

The 2017 session of HRC Universal Periodic Review included a peer-to-peer review of the UK, one of the EU Member States which has been heavily involved in the collection, storage, manipulation and sharing of personal data according to the revelations of Edward Snowden, former US contractor with the National Security Agency, in 2013.[14] The question of the protection of the right to privacy was reviewed in that session and in the preparatory documents the following summary of concerns were raised by UN human rights institutions and bodies:

> "Right to privacy and family life[15]
>
> 43.The Human Rights Committee was concerned that the current legal regime in the United Kingdom allowed for mass interception of communications and lacked sufficient safeguards against arbitrary interference with the right to privacy. It recommended that the Data Retention and Investigatory Powers Act 2014 be revised, with a view to ensuring that access to communications data is limited to the extent strictly necessary for prosecution of the most serious crimes and is dependent upon prior judicial authorization.[16]
>
> 44. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism stated that current assessments of the threat posed by terrorism in the United Kingdom had changed significantly in profile over the past years and that there should be a debate on the extent to which the public was prepared to tolerate official access to metadata.[17] He urged the British authorities to review their operations to ensure that they comply fully with the obligations of the State under the Convention for the Protection of Human Rights and Fundamental Freedoms regarding the right to liberty and security and the right to respect for private and family life."[18]

---

[13] By extension, the reasoning of the Committee on Economic and Social Rights in Communication 5/2015 "If a State party does not take appropriate measures to protect a Covenant right, it has a responsibility even when the action that undermined the right in the first place was carried out by an individual or a private entity. Thus, although the Covenant primarily establishes rights and obligations between the State and individuals, the scope of the provisions of the Covenant extends to relations between individuals." 20 July 2017, E/C.12/61/D/5/2015.
[14] Bauman, Zygmunt, et al. "After Snowden: Rethinking the impact of surveillance." *International political sociology* 8.2 (2014): 121-144.
[15] A/HRC/WG.6/27/GBR/2.
[16] See CCPR/C/GBR/CO/7, para. 24.
[17] newsarchive.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=13678&LangID=E.
[18] newsarchive.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=13678&LangID=E.

It is clear that, in the UPR, the HRC was not satisfied that the UK government's attempts to codify in law generalised power to intercept electronic communications were consistent with the right to privacy. While the specific issue of the differential treatment of citizens and foreigners was not directly addressed, the problem arises because of the capacity of the state to access the personal communications of both citizens and foreigners within a general framework of protection of privacy which was considered inadequate.
On the issue of jurisdiction and extraterritorial effect of Article 17 ICCPR, we endorse the position of the High Commissioner in the report on the Right to Privacy in the Digital Age.[19] This position has been widely adopted by the UN Treaty Bodies as evidenced in the UPR of the UK in 2017.

The Right to Privacy and National Constitutional Protections for Citizens

What is the situation where a state's constitution provides a higher level of protection of privacy than that which has been established by the HRC as required by Article 17 ICCPR but that constitutional protection is limited to citizens of the state? This situation appears to be ever more common, as the HRC noted in the concluding observations on the 4th periodic report of the USA in 2014.[20] This position also exists in EU law regarding access and the grounds for access to the EU databases which contain only information about third country nationals as described above in the introduction. In the European Commission's proposal for interoperability of the databases, dispositions permit Member States to provide access to the interoperable databases to their police authorities for purposes of identification without the necessity of any suspicion of crime.[21]

[19] A/HRC/27/37 para 33.
[20] CCPR/C/USA/CO/4 para 22, as noted in the High Commissioner's report of 30 June 2014: "22. The Committee is concerned about the surveillance of communications in the interest of protecting national security, conducted by the National Security Agency (NSA) both within and outside the United States, through the bulk phone metadata surveillance programme (Section 215 of the USA PATRIOT Act) and, in particular, surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act, conducted through PRISM (collection of communications content from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic) and the adverse impact on individuals' right to privacy. The Committee is concerned that, until recently, judicial interpretations of FISA and rulings of the Foreign Intelligence Surveillance Court (FISC) had largely been kept secret, thus not allowing affected persons to know the law with sufficient precision. The Committee is concerned that the current oversight system of the activities of the NSA fails to effectively protect the rights of the persons affected. While welcoming the recent Presidential Policy Directive/PPD-28, which now extends some safeguards to non-United States citizens "to the maximum extent feasible consistent with the national security", the Committee remains concerned that such persons enjoy only limited protection against excessive surveillance. Finally, the Committee is concerned that the persons affected have no access to effective remedies in case of abuse (arts. 2, 5 (1) and 17).
[21] COM(2017)793. Article 20 "Access to the common identity repository for identification.

Further, the prohibition on discrimination in the proposal does not include nationality.[22]

We note that the General Assembly, in the New York Declaration of 19 September 2016, stated: "We recall that our obligations under international law prohibit discrimination of any kind on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Yet in many parts of the world we are witnessing, with great concern, increasingly xenophobic and racist responses to refugees and migrants." (para 13 A/71/L.1). We are concerned that the actions of the EU in respect of the privacy of third country nationals is a further demonstration of a response to refugees and migrants inconsistent with both Articles 17 and 26 ICCPR.

Further the UN Committee on Economic, Social and Cultural Rights has set out the relationship to rights and discrimination in the following terms, noting the consistency with the HRC General Comment 18:

> "…discrimination constitutes any distinction, exclusion, restriction or preference or other differential treatment that is directly or indirectly based on the prohibited grounds of discrimination and which has the intention or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of Covenant rights."[23]

In order to fulfil their obligations under these Articles 17 and 26 ICCPR, states must ensure that there is no discrimination in the protection of privacy of citizens and foreigners. The single fact of failing to be a citizen of a state cannot justify differential treatment in the protection of privacy. We are dismayed that the justification for an EU separate database of third country nationals who have

---

1.Where a Member State police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.
Where the query indicates that data on that person is stored in the CIR, the Member States authority shall have access to consult the data referred to in Article 18(1).
Where the biometric data of the person cannot be used or where the query with that data fails, the query shall be carried out with identity data of the person in combination with travel document data, or with the identity data provided by that person.
2.Member States wishing to avail themselves of the possibility provided for in this Article shall adopt national legislative measures. Such legislative measures shall specify the precise purposes of identity checks within the purposes referred to in Article 2(1)(b) and (c). They shall designate the police authorities competent and lay down the procedures, conditions and criteria of such checks."

[22] COM(2017)793 Article 5 "Non-discrimination" Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. Particular attention shall be paid to children, the elderly and persons with a disability."

[23] UN Committee on Economic, Socual and Cultural Rights General Comment 20 E/C.12/GC/20

been convicted of offences appears to rest on unsupported claims about the threat of terrorism[24] and the effectiveness of border controls.[25] Yet, the ICCPR standard requires the same protection of privacy to be apply to both citizens and foreigners. Where states are able to provide higher standards of privacy protection to their citizens than are considered the threshold required by Article 17 ICCPR, the same standard must also be applied to everyone irrespective of nationality or immigration status in order to comply with Article 26 ICCPR. Where states seek to interfere with the right to privacy, as the High Commissioner has clearly set out in section A.1 of the note of 30 June 2014, there are finite grounds on which this can be done, the interferences must not be arbitrary and it is for states to justify on those grounds, in accordance with the law, the compatibility of the interference.

We would highlight one final point, there are a number of state efforts regarding the lack of relevant data on convictions for criminal offences of foreigners as opposed to nationals of the state. It seems that some states are starting projects to separate out data of criminality and foreigners from that of citizens. The new reporting requirements contained in the Trump Travel Ban(s)[26] on US law

[24] COM(2017) 344 "Firstly, further horrific terrorist attacks in European cities have led to security issues becoming even more prominent. The political stance regarding systematic use of fingerprints for secure identification and generally the attitude towards data sharing and security has changed, [footnote on impact assessment] focussing on effectiveness and efficiency and the need to exploit synergies between different European information exchange systems. The creation of a centralised ECRIS-TCN system containing both fingerprints and other identity information can support this approach, since it would make it possible to create a shared biometric matching service and a common identity repository for the interoperability of information systems, if so decided by the legislators in the future. A decentralised solution would not create the same opportunities for future synergies."

[25] COM(2017) 344 "Secondly, the Communication "Stronger and Smarter Information Systems for Borders and Security" [footnote] contains concrete and practical suggestions to further develop existing tools, but also concrete suggestions and ideas on new forms of interoperability. The Commission calls for more efficiency and interoperability of existing European databases and electronic information exchange systems, including an ECRIS-TCN system. The work to follow up on the Communication was led by the High Level Expert Group on Interoperability8, and the ECRIS-TCN system proposed here is one of the systems that is part of this interoperability initiative. Such interoperability would not be possible if a decentralised solution as proposed in January 2016 would have been pursued."

[26] US Executive Order 13780 Sec. 11. Transparency and Data Collection. (a) To be more transparent with the American people and to implement more effectively policies and practices that serve the national interest, the Secretary of Homeland Security, in consultation with the Attorney General, shall, consistent with applicable law and national security, collect and make publicly available the following information:

(i) information regarding the number of foreign nationals in the United States who have been charged with terrorism-related offenses while in the United States; convicted of terrorism-related offenses while in the United States; or removed from the United States based on terrorism-related activity, affiliation with or provision of material support to a terrorism-related organization, or any other national-security-related reasons;

(ii) (ii) information regarding the number of foreign nationals in the United States who have been radicalized after entry into the United States and who have engaged in

enforcement bodies to provide data on convictions of foreigners in the US is one example of this move.[27] This also seems to be the logic of the EU proposal for a special database of third country nationals who have been convicted of offences in any EU Member State discussed above.[28] No attention is given to the discriminatory effect of such databases and their prejudicial affects, in particular the challenges to equal treatment in the protection of privacy or the rights of third country nationals to the protection of their personal data.

Conclusions

In this contribution to the work of the OHCHR, we have addressed only the issue of discrimination between citizens and foreigners in exercise of the right to privacy. We have made three propositions:

1. Articles 17 and 26 ICCPR protect the right to privacy of everyone. There must be no discrimination between the right to privacy of citizens and foreigners.
2. Interferences with the right to privacy of people on the basis of their nationality is a suspect ground of discrimination which states must justify in accordance with the limited grounds applicable to the ICCPR right.
3. In so far as states provide more extensive protections of privacy to their own nationals they must also extend these protections to foreigners within their jurisdiction to comply with Article 26 ICCPR.

We warmly welcome this Inquiry which is both timely and of profound importance to the protection of privacy in a digital age.

31 March 2018

---

terrorism-related acts, or who have provided material support to terrorism-related organizations in countries that pose a threat to the United States;

(iii) (iii) information regarding the number and types of acts of gender-based violence against women, including so-called "honor killings," in the United States by foreign nationals; and

(iv) (iv) any other information relevant to public safety and security as determined by the Secretary of Homeland Security or the Attorney General, including information on the immigration status of foreign nationals charged with major offenses.

[27] Chacón, Jennifer M. "Immigration and the Bully Pulpit." *Harv. L. Rev. F.* 130 (2016): 243.

[28] COM (2017) 344.