United Nations A/HRC/46/37/Add.8

General Assembly

Distr.: General
17 February 2021

English only

Human Rights Council
Forty-sixth session
22 February–19 March 2021
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the right to privacy on his visit to United States of America

Comments by the State*

* The present document is being issued without formal editing.

U.S. Recommendations to the Draft Report of the Special Rapporteur on the right to privacy on his visit to the United States of America

U.S. comments on the framework of the Special Rapporteur's analysis:

The United States notes that, throughout his report, the Special Rapporteur (UNSRP) assumes that "necessity and proportionality" and related European Union (EU) law data protection standards reflect current international law. In the view of the United States, this assumption is incorrect. Instead, the applicable international human rights law for evaluating U.S. privacy practices is the International Covenant on Civil and Political Rights (ICCPR). Article 17 of that instrument provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." This provision does not impose a requirement of proportionality or necessity on a State Party's interference with privacy; instead, it imposes an obligation to refrain from arbitrary or unlawful interference with privacy. That is the obligation that the United States implements through its domestic legal framework. While certain elements of U.S. domestic law may use the words "necessary" or "proportionate" in relation to privacy, the relevant inquiry here is how the United States implements its obligations under Article 17 of the ICCPR.

U.S. Recommendations on paragraphs in Annex:

II. Constitutional and other legal protections of privacy

12. Paragraph 12 of the report of the UNSRP contains two inaccurate statements.

(a) First, the paragraph misstates the United States' position regarding privacy safeguards applicable to U.S. persons and non-U.S. persons relating to surveillance for national security purposes. The paragraph describes the U.S. position only by reference to two grounds, relating to (1) the interpretation of the ICCPR and (2) the practice of other States. The United States' position includes a third ground, relating to concerns for protecting the integrity of the U.S. democratic system from the misuse of surveillance for domestic political purposes.[1]

(b) Second, while the report refers to the privacy protections the United States affords to all persons, regardless of nationality, under PPD-28, the text at paragraph 12 suggests that U.S. law and practice has departed from PPD-28 ("The US should further entrench and enforce the standards established under PPD28"). On the contrary, PPD-28 remains in force and continues to be enforced through implementing procedures at each U.S. intelligence agency.[2]

The United States respectfully requests that the UNSRP amend paragraph 12 accordingly.

13. All federal agencies have a Senior Agency Official for Privacy, whether this is specifically required by statutes creating Privacy and Civil Liberties Officers (PCLOs) or required by requirements issued by the Office of Management and Budget pursuant to its statutory authority. The United States recommends making a clear statement of this fact in the report, so the reader will understand this aspect of the U.S. legal privacy framework in the federal government.

Paragraph 13's assertion that the statutory PCLOs are "vulnerable to the whims of the Executive" appears to suggest that privacy officials should possess a kind of legal independence in order to be effective. However, privacy officials in the United States government are accountable to the democratically elected Executive, who, in turn, is accountable to the people. U.S. government privacy officials are also accountable to a democratically elected Congress, which both enacts the laws the officials are charged with

[1] *See* U.S. Narrative Response to UN Special Rapporteur Preliminary Report at 38–40.
[2] *See* U.S. Narrative Response to UN Special Rapporteur Preliminary Report at 49, 58.

enforcing and conducts oversight of these officials to make sure they are performing their jobs as required by the law. Congressional oversight places practical limits on the ability of the Executive to exercise power in an arbitrary and capricious manner. We respectfully request that the UNSRP delete the phrase "are vulnerable to the whims of the Executive," replacing it with the phrase "are appointed by and may be removed by the Executive." We also recommend amending the sentence to reflect the role that accountability to democratically elected officials plays in ensuring that U.S. privacy officials remain accountable while exercising their judgment on privacy matters.

18. The paragraph's assertion that "the U.S. has so far contented itself with a situation where it mostly takes a fragmentary approach to privacy protection" makes the assumption that a privacy legal framework that appears to create a seamless framework on the books necessarily corresponds to a seamless adherence to privacy practices on the ground. Laws on the books, however, are only effective insofar as they are enforced, and enforcement usually requires resources. Many jurisdictions that have enacted ostensibly comprehensive privacy laws fail to dedicate the resources necessary to enforce them comprehensively. As a result, the law on the ground is every bit as "fragmented" as the U.S. privacy framework may appear to be on the surface.

The United States takes a sectoral approach to privacy protections because democratically elected legislatures at the state and federal level have enacted privacy laws to address specific risks to privacy in specific situations. This tailored approach to privacy improves the fit for specific industries and communities, which increases buy-in and rates of compliance. The democratic accountability of the legislatures that enact the laws, in turn, improves the overall trust of the public in the legitimacy of the rules thus enacted. Enacting sectoral privacy laws that enjoy high levels of buy-in and compliance not only maintains public trust, but also addresses the specific risks to privacy in those unique contexts as opposed to applying a general "one-size-fits-all" rule. The sectoral approach may thus better serve the long-term goal of protecting privacy.

We respectfully disagree with the draft report's assertion that the U.S. approach is "more expensive to administer." While a sectoral approach may appear more difficult to understand at first glance, it is not difficult for those in the sectors who have to comply with the laws. Whether or not comprehensive privacy laws are easier to understand, they are far more expensive to administer because more data to protect means higher overall compliance costs. Privacy on the books is one thing, but privacy on the ground is a function of resources. If a comparison is made based on cost, we respectfully suggest that the UNSRP measure the costs of achieving meaningful compliance rates rather than the cost of enacting and comprehending the law. If U.S. companies devote more resources to protecting privacy, it is because they recognize the practical importance of complying with laws requiring them to protect their customers' privacy; it is the key to maintaining their customers' trust. If non-U.S. companies devote fewer resources to this purpose, it may be because they do not see the value of complying with their legal requirements, see no inherent business advantage in protecting the trust of their customers, and perhaps most importantly, do not risk enforcement of the law. In general, the more money is spent on compliance, the higher the compliance rates. Therefore, less money spent in jurisdictions with comprehensive frameworks does not mean those frameworks are cheaper; it is more likely to mean that the law in those jurisdictions results in little actual compliance on the ground.

We are unsure what the UNSRP means when he states that citizens should be "citizens first and consumers second," but assuming he intends to say that privacy laws should be based on a supposed universal human right of individuals to control data pertaining to them, we respectfully disagree. Article 17 of the ICCPR, which is the applicable international human rights law on privacy that is binding on the United States, requires States Parties to refrain from arbitrary or unlawful interference with privacy; it does not articulate a human right to control one's data. Moreover, the view we understand the UNSRP to be articulating treats data as if it were a kind of intellectual property, setting off a battle between businesses and consumers over the question of control. Personal data arises out of human activities that depend on relationships of trust. The goal of a data protection framework is to maintain these relationships of trust—and in connection with the use of personal data by businesses obtained from consumers, both businesses and consumers have a mutual interest in maintaining that

trust. Focusing on laws that protect that relationship of trust is the key to a functional privacy framework.

For this reason, the core of U.S. domestic privacy law is based on the model of consumer protection. The Federal Trade Commission and state attorneys general have been active and aggressive in enforcing privacy laws—bringing at least as many, if not more, actions as their counterparts in Europe, who, for exactly the same reasons, appear to be pursuing more or less the same kinds of cases. We respectfully suggest that the UNSRP include a paragraph taking into account the practical effectiveness of the U.S. privacy framework in addition to his overview of the law as written.

III. Conclusions and Recommendations

A. On intelligence oversight, security and surveillance

1. Background and Context

23-25. Parts of the text at paragraphs 23–25 of the report appear to be based on a mistaken premise. The text suggests that EU law regulates not only government surveillance for national security purposes within a country's territorial jurisdiction through the use of compulsory tools such as court-supervised search warrants or production orders, but also surveillance for national security purposes outside of a country's territorial jurisdiction through non-compulsory means of accessing data located in other countries or in transit between countries. This appears to be inconsistent with the current case law based on the following:

(a) The EU Court of Justice recently ruled that government measures to access data without imposing processing obligations on data holders are outside the scope of EU law on data protection. In its judgment in La Quadrature du Net and Others of October 6, 2020, the Court considered what scope of data access by Member State governments falls within the scope of Directive 2002/58, in light of Article 1(3) of that Directive, which excludes from its application activities that fall outside the scope of EU treaties.[3] Numerous Member States argued that the Directive did not apply to the national security data access at issue in the case because Article 4(2) TEU places such activities within the exclusive competence of the Member States.[4] The Court decided that Directive 2002/58, and likewise the EU General Data Protection Regulation, applies only to national measures requiring data holders to process data.[5] "By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only."[6]

(b) Separately, while the ECtHR has for decades reviewed national laws and programs for conducting surveillance for national security purposes, those judicial cases have involved only domestic surveillance programs—that is, government access to communications or other data within a State's territorial jurisdiction.[7] Indeed, in cases not

[3] *LQdN and others*, joined cases (C-511/18 and C-512/18, EU:C:2020:6), judgment ¶¶ 86–104.

[4] *Id.* 89.

[5] *Id.* 91–102; 102 ("It follows that the above interpretation of . . . Directive 2002/58 is consistent with the definition of the scope of [the GDPR], which is supplemented and specified by that directive").

[6] *Id.* ¶ 103. The Court stated that this form of data access is covered by national law only, subject to the application of the EU Law Enforcement Directive, but the Law Enforcement Directive expressly excludes from its application national security activities and thus does not apply to the national security data access under discussion here. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, art. 2(3)(a) & recital 14.

[7] E.g., Big Brother Watch and Others v. United Kingdom, Nos. 58170/13, 62322/14 & 24960/15 56–95

actually brought by residents of the respondent State, the ECtHR made clear that its review concerned only domestic surveillance within the respondent State's territorial jurisdiction.[8]

25. Paragraph 25 of the report contains what we believe is an overly broad description of the judicial remedies that citizens and residents of Europe enjoy for violations of national laws authorizing government access to their data for national security purposes. We encourage the UNSRP to revisit this statement in light of the implementation of the laws and policies in Europe, which, as in the United States, may limit individuals' access to courts, based on secrecy requirements for intelligence operations and admissibility requirements for judicial claims.

(a) For example, a German court in 2014 held inadmissible a claim of unlawful surveillance that did not show the claimant had been personally affected by the alleged surveillance activity.[9]

(b) As another example, the European Court of Human Rights ("ECtHR") in June 2018, in the case of Centrum För Rättvisa v. the Kingdom of Sweden,[10] determined that Sweden's intelligence surveillance program provides sufficient privacy protections under the European Convention on Human Rights, notwithstanding a lack of effective judicial remedies. The ECtHR found that "the Swedish remedies available for complaints relating to secret surveillance do not include the recourse to a court."[11] Although Sweden's legislation requires the Swedish government to "inform a natural person, if search terms directly related to him or her have been used, about when and why the collection took place," the ECtHR noted a secrecy-based exception to this notification requirement and observed that "in practice a notification has never been made, due to secrecy."[12] The ECtHR concluded that where secrecy precludes notifying targets and thereby limits their recourse to civil litigation, an aggregate of non-judicial safeguards and remedies is sufficient to protect privacy interests, especially safeguards such as prior judicial approval of surveillance followed by multiple layers of independent supervision.[13] The relevant inquiry is whether sufficient protections are in place taking the system as a whole, including, in that case, the supervisory roles of the

(13 Sept. 2018) (sixteen persons and organizations from different countries challenging the United Kingdom's Regulation of Investigatory Powers Act authorizing the interception of communications subject to the United Kingdom's territorial jurisdiction); Ben Faiza v. France, No. 31446/12 (8 Feb. 2018) (resident of France challenging France's Code of Criminal Procedure authorizing fixing of geolocation device onto vehicle and disclosure of telephone records); Szabó and Vissy v. Hungary, No. 37138/14 ¶¶ 6–17 (12 Jan. 2016) (residents of Hungary challenging Hungary's Police Act authorizing intelligence surveillance measures); Zakharov v. Russia, No. 47143/06 ECtHR ¶¶ 25–138 (4 Dec. 2015) (resident of Russia challenging Russia's Operational-Search Activities Act authorizing interception of telephone communications, and regulations issued thereunder); Kennedy v. United Kingdom, No. 26839/05 ECtHR ¶¶ 25–74 (18 May 2010) (resident of United Kingdom challenging United Kingdom's Regulation of Investigatory Powers Act authorizing interferences with telecommunications); Liberty and Others v. United Kingdom, 58243/00 ¶¶ 5, 15–17 (1 July 2008) (civil liberties organizations from United Kingdom and Ireland challenging the United Kingdom's Interception of Communications Act authorizing interception of communications at facility in United

[8] *Big Brother Watch and Others* ¶ 271 ("nor did [the applicants] suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom's territorial jurisdiction. The Court will therefore proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom"); *Liberty and Others* ¶¶ 42, 47 (applicants and United Kingdom both proceeding on basis that claimed interception of communications occurred at facility in England); *Weber and Saravia* ¶¶ 86–88 (rejecting claim by the Uruguayan applicants that the surveillance involved extraterritorial measures, noting that "[s]ignals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In light of this, the Court finds that the applicants failed to provide proof . . . that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.").

[9] EU Fundamental Rights Agency, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Mapping Member States Legal Frameworks* at 67 (2015).

[10] ***Centrum För Rättvisa v. the Kingdom of Sweden*, No. 35252/08 ECtHR.**

[11] *Id.* ¶ 177.

[12] *Id.* ¶ 165.

[13] *Id.* ¶¶ 177–78.

Swedish Foreign Intelligence Inspectorate, Parliamentary Ombudsmen, and the Chancellor of Justice.[14]

26. Paragraph 26 states that "evidence continues to pile up that" U.S. surveillance is unconstrained by standards of reasonableness. The United States does not believe this assertion is accurate and points the UNSRP to the circumstances of the instances cited in the accompanying footnote. First, the instance of overbroad access discussed in some detail in the footnote concerned not collection of data in the first instance, but rather searching or "querying" of data that had already been lawfully and properly collected via individually targeted collection decisions. (Similarly, to the extent the set of other instances that are referred to in that footnote involved querying and not surveillance, that distinction should be made clear.) Second, the United States believes that this instance provides an example of effective oversight rather than an example of unregulated data access. In that instance, the FBI had erroneously interpreted the restriction applicable to querying unminimized data already collected under FISA to permit a set of queries broader than permitted by the rules; this restriction is governed by the FBI's querying procedures that were found legally sufficient and hence reasonable by an independent Court, the Foreign Intelligence Surveillance Court (FISC). It was the FBI's erroneous interpretation that was the problem, not the reasonableness of the restrictions. That erroneous interpretation was discovered through regular program review by the oversight sections of the U.S. Department of Justice and duly reported to the FISC, leading to remedial measures. Furthermore, the erroneous interpretation was reported to Congressional oversight entities and also publicly reported.

27. Paragraph 27 contains several statements that appear to be erroneous or are confusing. The United States respectfully raises these for the UNSRP's attention.

(a) The first sentence refers to the FISC as "the" independent oversight authority for FISA surveillance. This language could be interpreted to mean that the FISC is the only independent oversight entity. In fact, there are multiple independent oversight authorities that ensure that FISA surveillance adheres to privacy safeguards set out in law and court-approved implementing procedures. They include Inspectors General, the PCLOB, and the intelligence committees of the Congress.

(b) The paragraph appears to conflate a general criticism of the constraints on collection of data as authorized by FISA and concerns about government investigators conducting overbroad searches or queries of data already collected. The text appears to refer to data collection standards, but footnote 19 refers to an instance of overbroad querying. We suggest this disparity between the discussion in the text of data collection and the references in the supporting footnote to querying of data already collected be reconciled.

(c) The paragraph understates the role of the FISC in overseeing the FISA 702 program. The paragraph indicates that FISA 702 collection is subject only to annual review and approval by the FISC. Suggesting that the FISC's oversight role ends with a single annual review is inaccurate. In fact, the FISC has a comprehensive and continual role in actively overseeing both government decisions to target specific individuals under FISA 702 and the government's handling of data after it is acquired. For reference, certain aspects of this oversight were described in a White Paper recently published by the U.S. government that the UNSRP may find useful.[15]

(d) The paragraph also presents what may be a confusing representation of the U.S. explanation for why FISA 702 was instituted. The quotation and accompanying text at footnote 20 indicate that the United States instituted FISA 702 only to save resources. The UNSRP's quotation from the ODNI report, however, overlooks critical text from that same report explaining that the U.S. Congress enacted FISA 702 to "address a collection gap" resulting from a change in communication technology that resulted in "many terrorists and other foreign adversaries . . . using email accounts serviced by U.S. companies." For many such terrorists and other national security threats located abroad, it was not feasible to satisfy

[14] *Id.* ¶¶ 141, 150, 153–161, 168–181.

[15] *See, e.g.*, U.S. government white paper, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II* at 6–11 (Sept. 2020), available at link.

the "probable cause" standard applicable for traditional FISA, which was designed for surveillance against domestic threats against whom basic investigative techniques could feasibly be used to gather evidence to demonstrate probable cause. FISA 702 was instituted not to save resources while sacrificing privacy, but to authorize regulated access to data in the United States, with robust oversight safeguards, to protect effectively against threats to citizens of the United States and our allies. We recommend that the text be revised to represent these facts.

30 and 32. The concepts of "necessity and proportionality" do not constitute internationally accepted rules. These are primarily terms from EU law, where they have been the subject of vigorous debate and various interpretations by European courts and policy makers. Since the concepts do not appear in Article 17 of the ICCPR, which is the applicable law with respect to the United States, we believe it is inappropriate to apply them in connection with assessing the protections provided by the United States to individuals.

35. Paragraph 35 of the report recommends certain new amicus curiae functions before the FISC. However, in fact the current FISA statue already establishes a role for amici before the FISC, and amici have appeared in numerous cases before the FISC.

B. Further modernisation of USA's privacy and data protection laws

45. We respectfully suggest that the recommendation that the U.S. Privacy Act, which governs how federal government agencies collect, use, maintain, and disseminate information, be revised "in the direction" of the CCPA misunderstands the Privacy Act as well as the CCPA. The goals of the two laws are quite different, their legal structures operate on different assumptions, and the suggestion that one should be more like the other is not helpful in furthering the goal of protecting privacy.

D. Gender and privacy

47. The recommendation that the "principles outlined [in the UNSRP's findings and recommendations on gender and privacy] should be closely respected and implemented in any forthcoming reform of USA's contribution to the debate about review and reform of its applicable data protection law(s), in this case, the GDPR" inaccurately indicates that the GDPR is an applicable internationally accepted data protection law or domestic regulation in the United States; it is not. We recommend revising the GDPR reference to replace it with laws applicable to the United States "for example, the Privacy Act, HIPAA, and the Federal Trade Commission Act."

F. Harmonising federal and state legislation, policy and practice

49. We respectfully disagree with the paragraph's assertion that "there is huge reliance on the ordinary courts to issue wiretap orders at state level and some NGOs claim that these are not subjected to sufficient scrutiny," as we are unaware of evidence to support this statement. Further, such a general statement without examining each state and its system could be misleading because each state has its own courts and the situation may differ to some extent by state. At the same time, the assertion does not take into account that the U.S. Constitution, Fourth Amendment, and case law govern how all states may collect and use information in the criminal context. Notably, the level of scrutiny required by American jurisprudence, — the reasonable suspicion and probable cause standards — in the criminal context is higher than in most modern democracies, including those to which the GDPR and Criminal Justice Directive apply.

G. The USA's role on the international stage

53. **The paragraph states:**

> If the US were to go beyond reform of surveillance law and gradually also reform the Privacy Act 1974 into something more closely resembling California's Consumer Privacy Act, then the way would be open to joining the world's largest Privacy and Data Protection Law club. The Special Rapporteur strongly recommends that the Government of the USA follows up reform of US laws on surveillance with reform of the Privacy Act 1974 and then ratification of Convention 108+ without delay.

While we commend the UNSRP for recognizing the importance of the Privacy Act as an effective structure for implementing privacy protections, comparisons with the CCPA are inapposite for the reasons set forth above.