UN Special Rapporteur on Contemporary Forms of Racism, Xenophobia, and Related Intolerances, Call for Submissions Thematic Report on Race, Borders and Digital Technologies

15 May 2020

Introduction

Access Now welcomes this opportunity to provide relevant information to the United Nations (UN) Special Rapporteur on Contemporary Forms of Racism, Xenophobia, and Related Intolerances (Special Rapporteur) on race, borders and digital technologies to inform the Special Rapporteur's 2020 report to the UN General Assembly.[1] As an ECOSOC accredited organisation, Access Now routinely engages with UN Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world.[2]

Through representation in 15 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. We engage with an action-focused global community, convene stakeholders through the RightsCon Summit Series, lead the Digital Rights Litigators Network, and operate a 24/7 Digital Security Helpline that provides real-time direct technical assistance to at-risk individuals and communities worldwide.

Call for Submissions

Access Now is pleased to provide input on (1) discriminatory impacts arising from use of digital technologies in the context of border enforcement and administration and (2) state and corporate governance, including protection gaps and good practices for the Special Rapporteur's information.

Domestic and regional laws aimed to increase the use of digital technologies in the context of border enforcement and administration worldwide have, in practice, disproportionate and discriminatory impacts. Access Now takes the opportunity to highlight regulations and laws implemented in the United States (US) and European Union (EU) that are particularly troublesome.

1. Discriminatory impacts arising from use of digital technologies in the context of border enforcement and administration

a. Experimental use of new technologies, surveillance methods, and data gathering tools on vulnerable groups

[1] OHCHR, Call for Submissions: Thematic report on Race, Borders and Digital Technologies, 2020.
[2] Access Now, Access Now About Us

European Union (EU)

Over the past few years, the EU has adopted a series of laws and international agreements that require the travel industry and authorities to collect, store, and retain the personal travel records of everyone entering, travelling within, or leaving the EU, indiscriminately and in the absence of suspicion. While these legislation apply to any travellers, it reflects a wider context of deploying digital technologies geared at tracking people temporarily or permanently entering EU member states. With the so-called "Smart Borders" legislation, the European Passenger Name Record (PNR) law, and international PNR agreements, **the mass collection and retention of sensitive data and biometrics at the borders has become a dangerous new norm.**[3]

Governments typically cite "security" as a justification for mass data collection and profiling. Yet neither the EU nor its member-state governments have shown evidence to demonstrate that these measures actually improve security. In fact, creating massive databases of information on everyone who travels may instead bury the needle ever more deeply in the surveillance haystack.[4]

i. "Smart Borders" Package

In 2013, the EU Commission first proposed the "Smart Borders" package. The Smart Border package follows the EU Commission's 2008 Communication suggesting (1) the establishment of an Entry/Exit System (EES) to help EU Countries to flag so-called overstayers; (2) a Registered Traveller Programme (RTP) — a fast lane for frequent visitors willing to pay a fee and digital "toll" in private information; and (3) amendments to the Schengen Information System.[5]

The Smart Borders proposal is part of the EU Agenda on Migration.[6] European Parliament and EU member states eventually dismissed the initial 2013 Smart Borders proposal because of its technical complexity, cost, and negative civil liberties implications.[7] Nonetheless, soon after, the EU Commission conducted a consultation to collect views to help prepare a revised proposal, which was introduced in 2016, and adopted in July 2017.

In November 2016, Access Now released a report on the EU Commission's 2016 Smart Borders Package.[8]The report provides an analysis of the EU Commission's 2016 Smart Borders package proposal in relation to (1) use of data for border management purposes, and (2) use of data for law enforcement purposes. The Report therefore assesses the overall impact on the fundamental rights to data protection and privacy. We would like to draw the Special Rapporteur's attention to a main finding.

---

[3] Access Now, We (still) Know Where You'll Be Next Summer, 19 July 2017.
[4] *Id.*
[5] Access Now, Smart Borders - The Little Package that couldn't protect your rights, 5 November 2015; *See also* European Commission, Smart borders - background accessed on 8 May 2020.
[6] European Commission, European Agenda on Migration 2015 - four pillars to better manage migration
[7] Access Now, EU's 'Smart Borders 2.0' increases risks of surveillance and privacy abuses, 20 December 2016; Chris Jones, Analysis smart borders: fait accompli? Statewatch, August 2014.
[8] Access Now, Smart Borders Policy Analysis, November 2016.

As part of the Smart Borders package, the EU extends **biometric identity checks** — previously reserved for travellers from countries requiring visas — to all non-EU nationals entering or leaving the EU. Biometric identity checks involve collecting four fingerprints and a facial image, which is retained in a centralised system, together with a plethora of other personal information, for five years. This excessive and unjustified retention contradicts the jurisprudence of the EU Court of Justice. In April 2014, the court ruled that blanket retention of telecommunication data is not compatible with the EU. While the data retained in the case of the Smart Borders package is different, its massive retention is nonetheless not less intrusive, on the contrary, as it includes unique genetic identifiers of people.[9] [10]

The alleged objective of this system is to help the authorities identify travellers who have stayed longer than permitted in the EU, so-called overstayers. However, having a single, centralised database opens up **significant risks for the fundamental rights to privacy and data protection, due to the amount of data stored, the risk of unauthorised access to the data, and the lack of robust data protection safeguards in the proposal.** Moreover, biometric identifiers, including fingerprints, iris scans, and facial geometry, have become increasingly popular as a means of enrolling individuals into systems and then authenticating users. Biometric data is vulnerable to hacking just like other authentication methods. However, unlike a password, **biometric indicators cannot simply be reset or changed as needed.** This poses a higher security risk, since it becomes increasingly difficult to repair the damage done by leaks or hacks of biometric data, and thus restore sanctity to biometric-based systems.[11] This system, which has now been adopted, therefore enables profiling and increases risk of surveillance of travellers on a massive scale.[12]

Profiling is when authorities analyse personal information — often employing the use of automated decision-making tools, predictive analytics and algorithms — in order to make assumptions about those crossing their borders. The analysis could range from guessing a holiday itinerary to weighing on the likelihood that a person is a terrorist. In practice, profiling can mean that if someone is part of — or connected to — a religious, ethnic, or other type of targeted community, authorities are more likely to violate their privacy without cause. The realities of these practices leave such individuals and communities to reconsider how their personal choices will be interpreted by agents at the border.[13]

The implications go well beyond tracking travellers' movements. Creating a detailed dossier on individuals simply because they choose to travel is not only privacy-invasive and inherently disproportionate, it increases the risk of human rights abuses for the most vulnerable people and communities. **History shows us that when data are collected and profiling techniques are used, they tend to be discriminatory.[14]** In 2019, Access Now contributed to an official pilot project from the European Union which found that the EU "Smart Borders" legislation lack "specific provisions that

[9] Access Now, EU's 'Smart Borders 2.0' increases risks of surveillance and privacy abuses, 20 December 2016.
[10] Court of Justice of the European Union, Digital Rights Ireland ruling, 8 April 2014.
[11] Access Now, #WhyId, November 2019; Access Now, National Digital Identity Programmes: What's Next? May 2018.
[12] Access Now, EU's 'Smart Borders 2.0' increases risks of surveillance and privacy abuses, 20 December 2016.
[13] Access Now, We (still) Know Where You'll Be Next Summer, 19 July 2017.
[14] Access Now, We (still) Know Where You'll Be Next Summer, 19 July 2017.

would ensure the implementation of the non-discrimination safeguards foreseen" under the EU Charter.[15] **A number of PNR laws were found to be in violation of the right to non-discrimination by failing for instance to prevent the collection of sensitive data related to race or political views.** [16] Moreover, in the context of the implementation of PNR checks, research conducted by the EU Fundamental Rights Agency pointed out that several passengers felt they were being checked unfairly because of their ethnic or national background or their gender.[17] No matter how much legal safeguards a law may include, border agents may interpret PNR data in a discriminatory manner. However, the addition of specific provisions requiring statistics on border controls could help detect discriminatory patterns and trends in the application of specific rules, criterion or practices which can then help mitigate the risk of indirect discrimination.

ii. Passenger Name Records (PNR)

The EU Passenger Name Record (PNR) Directive, which entered into force in May 2016, created national databases storing personal information about everyone flying into or out of the EU. It also allows EU member states to additionally store data from anyone travelling across the EU.[18] PNRs contain information about a passenger's flight details, including itinerary, contact details, forms of payment, accompanying guests, and more. All this information is stored in airlines' databases for commercial purposes. This is indiscriminate and disproportionate storage of massive amounts of personal information, and it creates a risk to the right to privacy.[19] The database that this law implements could be abused or misused, resulting in personal harms ranging from credit card fraud to government profiling.[20]

History shows that this **type of profiling disproportionately affects vulnerable people and communities, such as religious, ethnic, or other minority groups.** Yet this profiling is enabled and authorised under the EU PNR Directive.[21] Proponents of the EU PNR try to minimise the risks of this measure, claiming that it will increase security in the EU, at a time when the political context is creating intense pressure to "do something" about terrorism. France, which has suffered three terrorist attacks in 2015, was one of the main proponents of this law.

The EU has also adopted several international PNR agreements which includes measures that are far more sweeping that the EU PNR Directive. The EU-US PNR agreement for instance practically does not establish time- limitation for the retention of the data collected. The EU study conducting a Fundamental rights review of EU data collection instruments and programmes **found that all PNR**

[15] Fondazione Giacomo Brodolini, Fundamental rights review of EU data collection instruments and programmes, 2019, page 39.
[16] Fondazione Giacomo Brodolini, Fundamental rights review of EU data collection instruments and programmes, 2019, page 69.
[17] Fundamental Rights Agency, Fundamental rights at airports: border checks at five international airports in the European Union, November 2014, page 47.
[18] Access Now,We (probably) Know Where You'll Be Next Summer, 26 January 2016.
[19] EDPS, EDPS supports EU legislator on security but recommends re-thinking on EU PNR, 10 December 2015.
[20] Access Now, We (probably) Know Where You'll Be Next Summer, 26 January 2016; EDRi, EU secret profiling of air passengers nominated for "big brother awards", 15 October 2015.
[21] Access Now, We (probably) Know Where You'll Be Next Summer, 26 January 2016.

instruments in place in the EU, including all international instruments, contravene EU law, in particular because they create unjustified intereferece with the rights to privacy, data protection, and in some case, the right to non-discrimination.[22] The validity of PNR frameworks is routinely under legal scrutiny in the EU. In 2017, a new draft PNR Agreement between the EU and Canada was struck down for violating the rights to privacy, data protection, and non-discrimination.[23] Currently, the national implementation of the EU PNR Directive is facing similar scrutiny in courts in Belgium, Austria, and Germany.[24]

United States (US)

Similar to the EU, over the past few years, the US has proposed rules and regulations regarding the collection and monitoring of social media information of migrants, visitors, and travelers, at the border and beyond. Such rules enable authorities to tap into social media accounts to collect, store, and retain data of everyone intending to enter, travel within, or leave the US, indiscriminately and in the absence of suspicion. Various government agencies operate under opaque policies and unclear and overbroad jurisdictional claims, compounding risks of rights infringement.[25]

i. Collecting Social Media Information and Smartphone Data

In 2017 then US Secretary of Homeland Security John Kelly told members of the US Congress that the Trump administration wants back-end access to social media accounts of visitors to the US as a condition for entry.[26]This proposal floated around since the earliest days of the new Trump administration and broadened to reportedly require visitors to turn over passwords not just to social media accounts, but also to their personal devices like smartphones, a policy Access Now strongly opposes.[27] A password-for-entry rule harms a wide range of human rights: the rights to privacy, freedom of expression, freedom of association, of thought, of religion, and of movement and has a disproportionate and discriminatory impact on vulnerable and marginalized individuals and groups.

In 2019, the US Department of Homeland Security (DHS) proposed a rule to require disclosure of social media accounts from certain people seeking to travel, be admitted to the US, or are applying for

---

[22] Fondazione Giacomo Brodolini, Fundamental rights review of EU data collection instruments and programmes, 2019, page 69.
[23] Access Now, Border Surveillance: What Europe's "PNR" Ruling Means for your Privacy, 17 September 2017.
[24] Epicenterworks, We're going to overturn the PNR directive, 14 May 2019.
[25] *See, e.g.*, ACLU, US Customs and Border Protection asserting the power to conduct warrantless searches anywhere within 100 miles of the border, 2020.
[26] Access Now, Give us your Twitter, your Facebook, your passwords guarding your free expression, 14 February 2017.
[27] Access Now, Give us your Twitter, your Facebook, your passwords guarding your free expression, 14 February 2017; Access Now, We (still) Know Where You'll Be Next Summer, 19 July 2017; Alexander Smith, U.S. Visitors May Have to Hand Over Social Media Passwords: DHS, NBC News, 8 February 2017; Jake Tapper, White House discussing asking foreign visitors for social media info and cell phone contacts, CNN, 30 January 2017. In 2017, more than two dozen human rights and civil liberties groups, including Access Now, wrote to United Nations experts requesting a broad investigation into reports that U.S. border agents are "demanding visitors provide access to their electronic devices as well as passcodes to those devices and online accounts." *See* Access Now, Human rights groups ask United Nations to investigate U.S. border policies, 16 February 2017.

immigration-related benefits.[28] Fields collecting information regarding social media identifiers were added to visa application forms.[29] This year marked an expansion of the US Department of State (State Department) collection of social media information "collecting from some 15 million people per year." [30] The information collected by the State Department is "shared within the US government, [including the DHS], and also disseminated, in some circumstances, to other other governments."[31] Unfortunately, many questions remain as to "how the State Department will use the millions of identifiers that it is collecting."[32] Nonetheless, according to the Brennan Center for Justice, "DHS has reportedly used its social media monitoring programs to **surveil Black Lives Matter activists, individuals involved in anti-Trump protests in New York City, and lawyers and journalists at the southern border."[33]**

Asking or requiring people to hand over social media information at the border or for immigration purposes is neither secure nor rights-respecting. The existence of – and information found on – one's social media accounts is deeply personal and highly susceptible to misinterpretation. Asking customs agents to make decisions based on their interpretation of a traveller's conversations, posts, and relationships is dangerous. **There is no guarantee that an agent would understand the context, or have any knowledge of an individual's language or culture.**[34]

2. State and corporate governance, including protection gaps and good practices for the Special Rapporteur's consideration

a. Corporate Governance

In November 2019, the Investor Alliance for Human Rights released a *Human Rights Risks Briefing on Palantir Technologies* to inform investors of the human rights risks associated with the US software company through its contracts with the US federal government.[35] Palantir contracted with the US Immigration and Customs Enforcement (ICE) to provide software that is used to gather and search for data on undocumented immigrants and to faciliate workplace raids. ICE has drawn international criticism for violating human rights in its enforcement of immigration policies. **Responsible investors called on the private equity funds that directly invest in Palantir and on Palantir itself to**

[28] Federal Register, 84 Fed. Reg. 46557 - 46561 Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms, (posted 4 September 2019).
[29] U.S. Department of State, Collection of Social Media Identifiers from U.S. Visa Applicants, 4 June 2019.
[30] Brennan Center for Justice, Social Media Monitoring, March 2020; Faiza Patel and Harsha Panduranga, Snooping on Foreigners' Facebook Feeds Is Ineffective and Creepy,The Atlantic, 14 June 2019; *See also* Brennan Center for Justice, Doc Society v Pompeo, 5 December 2019.
[31] *Doc Society v. Pompeo*, No. 1:19-cv-03632 (D.D.C.) § 1 available at Brennan Center for Justice, Doc Society v Pompeo, 5 December 2019.
[32] Faiza Patel and Harsha Panduranga, Snooping on Foreigners' Facebook Feeds Is Ineffective and Creepy, The Atlantic, 14 June 2019.
[33] Brennan Center for Justice, Government: Social Media Surveillance
[34] Access Now, We (still) Know Where You'll Be Next Summer, 19 July 2017.
[35] Investor Alliance for Human Rights, Human Rights Risks Briefing: Palantir Technologies, November 2019.

reconsider partnering with an agency that has perpetuated human rights abuses against undocumented immigrants.[36]

The Investor Alliance has previously warned technology companies of the US government's "zero tolerance" immigration policy, sending guidance on human rights due diligence to "technology companies with active contracts with federal immigration agencies to provide a range of hardware and other infrastructure, including cloud services, risk assessment tools, artificial intelligence, face scanning technology, network operations management, and military technology."[37]

b. EU-Canada PNR Case at the Court of Justice of the European Union

In November 2014, the EU Parliament brought the EU-Canada PNR agreement case before the Court of Justice of the European Union so the court could assess whether the agreement is compatible with rights guaranteed under EU Treaties and the Charter of Fundamental Rights.[38] On 26 July 2017, the CJEU issued an opinion in a case challenging the validity of the EU-Canada PNR agreement.[39] The Court found that the data-sharing arrangement does not comport with Europeans' fundamental rights to privacy, data protection, and non-discrimination. The Court therefore concluded that the European Union cannot sign the agreement in its current form and provided a list of safeguards that must be incorporated into the text.[40] No new text has been formally put to debate in the European Parliament since then.

The ruling is a **huge victory for the fundamental rights to privacy and data protection.** It has **implications well beyond Europe and Canada**, since disproportionate government agreements for collecting and retaining passenger travel records impact the privacy of everyone travelling across borders, and the ruling provides grounds for invalidating rights-harming frameworks for the EU, Australia, and the United States.[41]

c. Assessment of Other EU-PNR Agreements

The landmark decision of the court provides clear guidance and criteria that PNR schemes must comply with in order to be compatible with EU law. Access Now created a table and we have taken a close look at the EU-Australia and EU-US agreements as well as the EU-PNR Directive to see if they

---

[36] Investor Alliance for Human Rights, Direct and Indirect Investors Engaging Palantir Technologies on Human Rights Risks, November 2019.
[37] Investor Alliance for Human Rights, Investors Warn Corporations of Human Rights Risks Related to "Zero Tolerance" Immigration Policies, 26 July 2018.
[38] InfoCuria, Case-Law, Request for an opinion submitted by the European Parliament pursuant to Article 218(11) TFEU
[39] Court of Justice of the European Union, The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form 26 July 2017.
[40] Access Now, In win for privacy, European court rejects EU-Canada "PNR" agreement , 26 July 2017; Access Now, Border Surveillance: What Europe's "PNR" Ruling Means for your Privacy, 7 September 2017.
[41] Access Now, Border Surveillance: What Europe's "PNR" Ruling Means for your Privacy, 7 September 2017.

would pass that test.[42] The result is clear: all three of them fail to comply with all or a large number of criteria set by the court and should therefore be suspended immediately.[43] Access Now participated in an EU study conducting a Fundamental rights review of EU data collection instruments and programmes and was tasked with reviewing the legality of all PNR instruments. We found that all PNR laws and agreements in place in the EU contravene EU law, in particular because they create unjustified intereferece with the rights to privacy, data protection, and in some case, the right to non-discrimination.[44] In the study, we call on the European Commission to recast these legislations, and at minimum, to significantly reform these legislative instruments to strengthen their safeguards.

Conclusion

Law enforcement and border agencies around the world continue to operate complex new surveillance systems under the ambit of providing security. Digital security matters even more as individuals cross borders, hop onto airport wifi, and use their devices around the world. Prior to the 2016 Summer Olympics, Access Now released a series of tips to help individuals travel more securely in light of increased surveillance measures.[45] In addition to these tips, Access Now's Digital Security Helpline is available 24/7 for all civil society groups and activists, media organizations, journalists and bloggers, and human rights defenders to provide comprehensive, real time direct technical assistance. The Digital Security Helpline can be reached at help@accessnow.org.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

[42] *See table* at Access Now, Border Surveillance: What Europe's "PNR" Ruling Means for your Privacy, 7 September 2017.
[43] *Id.*
[44] Fundamental rights review of EU data collection instruments and programmes, 2019, Page 69.
[45] Access Now, Best Practices Digital Security Traveling 2016 RIO Olympics,4 August 2016.